

Developing a Contextual Framework for Establishing a
Cybersecurity Culture in the Public E-Health Institutions: A
Case Study of South Africa

by

NWANNEKA EMILIA MWIM

Submitted in accordance with the requirements for
the degree of

DOCTOR OF PHILOSOPHY

in the subject

INFORMATION SYSTEMS

at the

University of South Africa

SUPERVISOR: Dr. J Mtsweni

CO-SUPERVISOR: Prof. B Chimbo

July 2025

DECLARATION

Name: Nwanneka Emilia Mwim

Student Number: 3382-561-0

Degree: Doctor of Philosophy in Information Systems

I Nwanneka Emilia Mwim hereby declare that this thesis titled **Developing a contextual framework for establishing a cybersecurity culture in the public E-Health institutions: a case study of South Africa** is my own work that all the sources used and/or quoted in this study have been indicated and acknowledged by means of references.

Signature: 

Date: July 2025

ACKNOWLEDGEMENT

I would like to recognise the almighty God for his goodness and mercy towards me in this journey. He has been my ultimate strength. Without His Mercy, I would not be here today.

My sincere appreciation and thanks go to my supervisors, Dr Jabu Mtsweni and Prof Chimbo, who have been with me on this journey. Dr Jabu Mtsweni (Dr J), thank you for believing in me when I approached you to be my supervisor. Your human heart, insight and fear of God were characteristics that made me approach you when you left Unisa to go to the CSIR. Working with you has really changed the way I approach things. Your work ethic, knowledge of cybersecurity and approachable attitude are highly valued. Thank you for making the difficult journey easier for me. I never for one day regretted working with you. To Prof Chimbo (Mother I often call you) thank you for stepping in for me and filling the gap when Unisa introduced changes regarding external supervisors. Your attention to detail and knowledge of grammar added great value to the work. You work so well with people, you and Jabu complimented each other and made the journey smooth. Thank you for working with me during this chapter of my life. I appreciate you, Mother.

My heartfelt gratitude goes to my husband Odirachukwu S. Mwim and children, Chidera, Chidalu and Ekene Mwim. Thank you, my love, for all your support, particularly your emotional support. You were the shoulder I could lean on when the going was tough. The value of your presence in my life cannot be overestimated. To my children, thank you for your prayers and follow up questions with regards to my work. Juju, thank you for your mathematical insight. It was helpful.

To my Mum, sisters and brother, thank you for your prayers and care. I love and appreciate you all.

Finally, to Dr Chiyangwa, a heartfelt message of appreciation for your assistance in the analysis of my data. Thank you for your patience and willingness to make yourself available even while busy with a busy teaching schedule. A special thank you.

DEDICATION

This thesis is dedicated to two special people in my life. To my mum, Theresa, for not giving up on me at a tender age. Your unconditional love made it possible for me to be here. To my husband Odirachukwu for giving me hope in life. I am here because God brought someone like you in my life.

ABSTRACT

The adoption and use of information and communication technology has transformed the way healthcare institutions perform administrative and clinical operations. The everyday use of this technology in the health sector requires an E-Health information system and this, when combined with telecommunication, is commonly known as E-Health. E-Health systems have many benefits for the wide variety of stakeholders in healthcare institutions. However, these systems are beset by a variety of risks, including challenges related to cybercrime, security, privacy and integrity. Healthcare institutions find it difficult to keep up with existing and evolving cybersecurity threats, making them very vulnerable. Coordinated and unified cybersecurity strategies must be implemented to counter these cyber threats and risks in E-Health institutions. However, a technological cybersecurity solution on its own is not sufficient as factors, such as a lack of security awareness, need for training, and irresponsible or careless digital behaviour, point to the need to create a cybersecurity culture as well.

Studies related to cybersecurity culture form an emerging research area and this has not been thoroughly investigated in the E-Health sector. The main objective of this research was to develop a contextual framework for establishing a cybersecurity culture in public E-Health institutions.

The study adopted a pragmatic world view supported by a case study strategy. Mixed-method research (quantitative and qualitative) accommodated both deductive and inductive research approaches in the collection and analysis of data. The data collection took place in three cycles using four data collection techniques (a systematic literature review, questionnaires, interviews and an expert review). Data were collected from one tertiary hospital as well as district hospitals in Mpumalanga province of South Africa.

The proposed contextual framework was developed by following the conceptual framework analysis phases and was evaluated through a defined use case, comparative analysis and expert reviews. Hence, the methodological contribution of the study is to demonstrate the design and development of the contextual framework using the conceptual framework analysis phases. Practically, the framework of the study will be able to guide the establishment of a cybersecurity culture in healthcare institutions. The study contributed by providing a step-by-step guideline as implementation support for the framework.

A limitation of this research was that data collection was limited to Mpumalanga Province. Data from Mpumalanga alone may not be a true representation of data from national health

departments in all provinces of South Africa. Additionally, the proposed Cybersecurity Culture Framework only considered a use case demonstrated in hospitals in the one province.

Future work could expand the scope of the research to other provinces and different healthcare categories. It is proposed that future work should include conducting real-time implementation tests to assess the effectiveness of the proposed framework.

Keywords: E-Health, cybersecurity, cybersecurity culture, Cybersecurity Culture Framework.

PUBLICATIONS

Mwim, E., & Mtsweni, J. (2022). Systematic review of factors that influence the cybersecurity culture. In *Proceeding of the International Symposium on Human Aspects of Information Security and Assurance, HAISA 2022*, 147-172. <http://doi.org/10.1007/978-3-031-38530-8>

Mwim, E. N., Mtsweni, J., & Chimbo, B. (2023). Factors Associated with Cybersecurity Culture: A quantitative study of Public E-Health hospitals in South Africa. In *Proceeding of the International Symposium on Human Aspects of Information Security and Assurance, HAISA 2023*, 129-142. Cham: Springer. http://doi.org/10.1007/978-3-031-38530-8_11

Mwim, E. N., Mtsweni, J., & Chimbo, B. (2023). Conceptual mapping of the cybersecurity culture to human factor domain framework. In *Proceeding of Advances in Information and Communication Conference (FICC)*, 729-742. Cham: Springer.

https://doi.org/10.1007/978-3-031-28073-3_49

Mwim, E., N., Mtsweni, J., & Chimbo, B. (2026). An Empirical Evaluation of the Main Factors of a cybersecurity culture in South African E-Health Institutions Using Multiple Linear Regression. *Journal of Cybersecurity and Information Management*, (17)2, 178-199. DOI: <https://doi.org/10.54216/JCIM.170213>

TABLE OF CONTENTS

DECLARATION	ii
ACKNOWLEDGEMENT	iii
DEDICATION	iv
ABSTRACT	v
PUBLICATIONS	vii
TABLE OF CONTENTS	viii
LIST OF FIGURES	xviii
LIST OF TABLES	xxi
LIST OF ABBREVIATIONS	xxiv
CHAPTER 1: BACKGROUND AND OVERVIEW OF THE STUDY	1
1.1 INTRODUCTION	2
1.2 BACKGROUND TO THE RESEARCH PROBLEM	4
1.3 PROBLEM STATEMENT	8
1.4 RESEARCH QUESTIONS AND OBJECTIVES	9
1.5 RESEARCH METHODOLOGY	12
1.6 RESEARCH MOTIVATION	14
1.7 RESEARCH LIMITATIONS	14
1.8 LAYOUT OF THE THESIS	15
1.9 CONCLUSION	16
CHAPTER 2: E-HEALTH STATE OF THE ART	18
2.1 INTRODUCTION	19
2.2 FRAMEWORK OF THE LITERATURE REVIEW	19
2.3 BACKGROUND FOR E-HEALTH	21
2.4 ELEMENTS OF AN E-HEALTH ECOSYSTEM	26
2.5 E-HEALTH STAKEHOLDERS	27
2.6 E-HEALTH SYSTEMS	29
2.6.1 ELECTRONIC MEDICAL RECORD SYSTEMS (EMRs)	30
2.6.2 TELEMEDICINE	31
2.6.3 CLINICAL DECISION SUPPORT SYSTEMS (CDSSs)	32
2.6.4 PHARMACY INFORMATION SYSTEMS (PISs)	33
2.6.5 PATIENT-CENTRED HEALTH INFORMATION SYSTEMS	33

2.6.6	HOSPITAL INFORMATION SYSTEMS (HISs).....	34
2.6.7	CYBER-PHYSICAL SYSTEMS (CPSs).....	35
2.6.8	LABORATORY SYSTEMS	35
2.6.9	OTHER E-HEALTH SYSTEMS	36
2.7	PUBLIC VERSUS PRIVATE HEALTH SECTORS.....	38
2.8	BENEFITS OF E-HEALTH	40
2.9	CHALLENGES TO E-HEALTH.....	41
2.9.1	INCREASED TIME	41
2.9.2	E-HEALTH TECHNOLOGY ICT INFRASTRUCTURE AND OTHER RESOURCES	41
2.9.3	TECHNICAL SUPPORT	42
2.9.4	INCREASED INEQUALITY.....	42
2.9.5	COST	43
2.9.6	FUNDING.....	43
2.9.7	SYSTEM ISSUES	43
2.9.8	LEGISLATION, POLICY AND STANDARDS	44
2.9.9	BUREAUCRACY	45
2.9.10	HETEROGENEITY	45
2.9.11	HUMAN FACTORS	46
2.9.12	SECURITY CHALLENGES.....	48
2.10	CONCEPTUAL MAPPING TO RESEARCH GAP	49
2.11	FOCUS ON SECURITY AS A CHALLENGE IN E-HEALTH.....	49
2.12	IMPORTANCE OF E-HEALTH DATA AND INFORMATION	51
2.13	CONCLUSION.....	52
CHAPTER 3: CYBERSECURITY CHALLENGES IN E-HEALTH.....		54
3.1	INTRODUCTION.....	55
3.2	CYBERSECURITY AND INFORMATION SECURITY DEFINITIONS.....	55
3.2.1	INFORMATION SECURITY	56
3.2.2	CYBERSECURITY.....	58
3.2.3	COMPUTER SECURITY	61
3.2.4	RELATIONSHIP AND DIFFERENCES BETWEEN INFORMATION SECURITY AND CYBERSECURITY	61
3.3	CYBERSECURITY IN E-HEALTH.....	66

3.4	WHY ARE E-HEALTH ORGANISATIONS TARGETS FOR CYBER THREATS?	67
3.4.1	DEPENDANCE ON ICT SYSTEMS AND INFRASTRUCTURE.....	68
3.4.2	LACK OF RESOURCES	69
3.4.3	DATA AS A VALUABLE SOURCE FOR FINANCIAL GAIN.....	70
3.4.4	LACK OF TRAINING AND AWARENESS OF SECURITY ISSUES	70
3.4.5	SECURITY ‘HOLES’	71
3.4.6	RAPID INCREASE OF AND CHANGING CYBER-ATTACK METHODS.	71
3.4.7	FRAGMENTED GOVERNANCE.....	72
3.4.8	CULTURAL BEHAVIOUR.....	73
3.4.9	OTHER FACTORS	73
3.5	E-HEALTH ORGANISATIONS’ CYBERSECURITY CHALLENGES	74
3.5.1	COMPLEXITIES OF HEALTHCARE ORGANISATIONS	74
3.5.2	TECHNOLOGICAL ADVANCEMENT	75
3.5.3	OUTDATED TECHNOLOGY	76
3.5.4	CHANGING GOVERNMENT POLICY	77
3.5.5	EMERGING THREATS	77
3.5.6	LACK OF PREPAREDNESS BY HEALTHCARE ORGANISATIONS.....	78
3.5.7	LACK OF RESOURCES	79
3.5.8	LACK OF AWARENESS, EDUCATION AND TRAINING.....	80
3.5.9	ERRORS RELATED TO HUMAN FACTORS	81
3.5.10	ACCOUNTABILITY	82
3.5.11	MISSING CYBER INCIDENT RECORDS	82
3.5.12	LACK OF UNDERSTANDING AND ECONOMIC ASSESSMENT.....	83
3.5.13	SECURITY CULTURE.....	83
3.5.14	OTHER CYBERSECURITY CHALLENGES	84
3.6	ADDRESSING CYBER THREATS AT E-HEALTH ORGANISATIONS.....	87
3.6.1	DATA BREACHES.....	88
3.6.2	MALWARE.....	96
3.6.3	RANSOMWARE.....	96
3.6.4	MEDJACK (MEDICAL DEVICE HIJACK).....	101
3.6.5	SPEAR PHISHING	102
3.6.6	DENIAL OF SERVICE (DOS) ATTACKS.....	102
3.6.7	INSIDER THREATS.....	102

3.6.8	OTHER CYBER THREATS.....	103
3.7	CONSEQUENCES OF CYBER-ATTACKS ON E-HEALTH.....	104
3.7.1	COST IMPLICATIONS	104
3.7.2	OTHER CONSEQUENCES OF CYBER-ATTACKS ON E-HEALTH.....	106
3.8	APPROACHES TO CYBERSECURITY CHALLENGES	107
3.8.1	LEGISLATIVE APPROACH	108
3.8.2	NON-LEGISLATIVE APPROACH	108
3.9	CONCLUSION	110
CHAPTER 4: CYBERSECURITY CULTURE AND THEORETICAL FRAMEWORK...		111
4.1	INTRODUCTION.....	112
4.2	REVIEW OF CHAPTERS LEADING TO CYBERSECURITY CULTURE (CSC)	113
4.3	CULTURE	115
4.4	ORGANISATIONAL CULTURE.....	116
4.5	SECURITY CULTURE.....	118
4.6	INFORMATION SECURITY CULTURE.....	119
4.7	ORDER OF CONCEPTS LEADING TO CYBERSECURITY CULTURE	119
4.8	BACKGROUND OF CYBERSECURITY CULTURE	120
4.8.1	CYBERSECURITY CULTURE	122
4.8.2	IMPORTANCE OF CYBERSECURITY CULTURE	123
4.9	CYBERSECURITY CULTURE LEVELS AND ECOSYSTEM	126
4.10	STEP 1 OF THE CONCEPTUAL PROCESS.....	128
4.11	THE PROTOCOL FOR THE SYSTEMATIC REVIEW.....	129
4.11.1	SEARCH STRATEGY	129
4.11.2	DATA EXTRACTION.....	132
4.11.3	REPORTING THE FINDINGS OF THE REVIEW	133
4.12	DEFINITIONS OF CYBERSECURITY CULTURE	134
4.12.1	HUMAN CHARACTERISTICS.....	136
4.12.2	CONTEXT OR ENVIRONMENT	137
4.12.3	SETA (SECURITY EDUCATION, TRAINING AND AWARENESS).....	138
4.12.4	TECHNOLOGY	138
4.12.5	MANAGEMENT.....	138
4.13	CYBERSECURITY CULTURE FACTORS.....	139
4.13.1	DEFINITIONS OF CYBERSECURITY CULTURE FACTORS	142

4.13.2	CATEGORIES OF CSC FACTORS	144
4.14	THEORETICAL FRAMEWORK AND RESEARCH MODEL.....	147
4.14.1	CYBER-SECURITY CULTURE THEORETICAL FRAMEWORK (FAOR) 148	
4.14.2	SECURITY CULTURE MODEL (SCM)	149
4.14.3	OCYBERSECURITY CULTURE FRAMEWORK	151
4.14.4	THE HUMAN FACTOR DIAMOND (HFD) FRAMEWORK.....	153
4.14.5	THE TECHNOLOGY, ORGANISATION, PEOPLE AND ENVIRONMENT THEORETICAL FRAMEWORK (STOPE).....	155
4.15	COMPARISON OF THEORETICAL FRAMEWORKS.....	157
4.16	CONCEPTUALISATION OF E-HEALTH CSC COMPONENTS.....	158
4.16.1	PREPAREDNESS (P) AND RESPONSIBILITY (R) (ORGANISATIONAL CULTURE).....	159
4.16.2	EXTERNAL ENVIRONMENT AND NON-ORGANISATIONAL MANAGEMENT (EENOM).....	160
4.16.3	INTERNAL ORGANISATIONAL MANAGEMENT (IOM).....	160
4.16.4	TECHNOLOGY (TECH)	161
4.16.5	CYBERSECURITY CULTURE	161
4.16.6	SUMMARY OF THE CYBERSECURITY CULTURE CONSTRUCTS.....	162
4.16.7	CSC FACTORS MAPPED TO THE CONSTRUCTS.....	163
4.17	CONCLUSION	164
CHAPTER 5: RESEARCH METHODOLOGY		166
5.1	INTRODUCTION.....	167
5.2	RESEARCH DESIGN	167
5.3	RESEARCH PHILOSOPHY	169
5.4	RESEARCH APPROACH.....	172
5.4.1	DEDUCTIVE RESEARCH APPROACH	172
5.4.2	INDUCTIVE RESEARCH APPROACH.....	172
5.4.3	APPLYING DEDUCTIVE AND INDUCTIVE APPROACHES	173
5.5	RESEARCH STRATEGY	174
5.5.1	CASE STUDY	176
5.5.2	SYSTEMATIC LITERATURE REVIEW	180
5.5.3	CONCEPTUAL FRAMEWORK ANALYSIS	195
5.6	RESEARCH CHOICE	200

5.6.1	QUALITATIVE AND QUANTITATIVE RESEARCH METHODS	200
5.6.2	MIXED METHOD RESEARCH (MMR)	201
5.6.3	CONVERGENT PARALLEL MIXED METHOD	202
5.7	TECHNIQUES AND PROCEDURES	203
5.7.1	DATA COLLECTION PROCESS	204
5.7.2	DATA COLLECTION INSTRUMENTS	206
5.7.3	RESEARCH QUESTIONS AND DATA COLLECTION INSTRUMENTS	210
5.7.4	DATA ANALYSIS	211
5.8	POPULATION	220
5.9	SAMPLING METHOD	221
5.9.1	CONVENIENCE SAMPLING	224
5.9.2	PURPOSIVE SAMPLING	226
5.9.3	SNOWBALL SAMPLING	227
5.9.4	SAMPLING STRATEGIES VERSUS DATA COLLECTION METHODS	228
5.9.5	SAMPLING SIZE	228
5.10	ETHICAL CONSIDERATIONS	229
5.11	CONCLUSION	231
CHAPTER 6: QUANTITATIVE DATA COLLECTION AND ANALYSIS		232
6.1	INTRODUCTION	233
6.2	QUANTITATIVE DATA ANALYSIS: STEP 1 OF THE CONCEPTUAL PROCESS	233
6.3	RELIABILITY-VALIDITY SUMMARY	234
6.4	QUANTITATIVE DATA COLLECTION	235
6.5	DATA ANALYSIS STEPS	237
6.5.1	DATA CLEANING	237
6.5.2	DEMOGRAPHIC ANALYSIS OF THE PARTICIPANTS	238
6.5.3	RESEARCH CONSTRUCTS	242
6.5.4	ASSESSMENT OF THE CONSTRUCTS' RELIABILITY AND INSTRUMENT RELIABILITY	243
6.5.5	ASSESSMENT OF THE INSTRUMENT'S VALIDITY USING EXPLORATORY FACTOR ANALYSIS (EFA)	245
6.5.6	DESCRIPTIVE ANALYSIS	254
6.5.7	PEARSON CORRELATION COEFFICIENT ANALYSIS	261
6.6	CONCLUSION OF THE QUANTITATIVE ANALYSIS	267

CHAPTER 7: QUALITATIVE DATA COLLECTION AND ANALYSIS.....	269
7.1 INTRODUCTION.....	270
7.2 QUALITATIVE DATA ANALYSIS: STEP 1 OF CONCEPTUAL PROCESS...	270
7.3 QUALITATIVE DATA INCLUDING DEMOGRAPHIC INFORMATION	271
7.3.1 PARTICIPANT SELECTION.....	272
7.3.2 INTERVIEW PROCESS.....	273
7.3.3 DATA CLEANING	274
7.3.4 DEMOGRAPHIC INFORMATION	275
7.4 THEMATIC DATA ANALYSIS PROCESS	276
7.4.1 STAGE 1: FAMILIARISATION WITH THE DATA.....	277
7.4.2 STAGE 2: GENERATION OF INITIAL CODES.....	278
7.4.3 STAGE 3: CATEGORISATION OF CODES AND THEME CREATION...	279
7.4.4 STAGE 4: NAMING AND DEFINING THEMES.....	280
7.5 IDENTIFIED CYBERSECURITY CULTURE THEMES	302
7.6 TRIANGULATION OF FINDINGS	304
7.6.1 QUALITATIVE AND QUANTITATIVE COMPARISONS OF MODELS	304
7.6.2 TRIANGULATION OF FACTORS.....	309
7.6.3 COMPARING THE TRIANGULATION RESULT WITH THE SYSTEMATIC LITERATURE REVIEW DATA	311
7.7 CONCLUSION OF THE QUALITATIVE ANALYSIS CHAPTER	314
CHAPTER 8: DESIGN AND DEVELOPMENT OF THE CONTEXTUAL CYBERSECURITY CULTURE FRAMEWORK (CCSCF).....	316
8.1 INTRODUCTION.....	317
8.2 CONTEXTUAL FRAMEWORK FORMULATION STEPS	317
8.3 THE CONTEXTUAL FRAMEWORK OF THE STUDY	319
8.3.1 THE CCSCF OVERVIEW DIAGRAM.....	320
8.3.2 THE SIX SEGMENTS OF THE CCSCF	321
8.4 THE FRAMEWORK OBJECTIVE AND PRINCIPLES.....	322
8.4.1 THE FRAMEWORK OBJECTIVES	322
8.4.2 THE FRAMEWORK PRINCIPLES	323
8.5 HIGH-LEVEL FRAMEWORK STRUCTURE.....	325
8.6 ELEMENTS OF THE FRAMEWORK	328
8.6.1 CYBERSECURITY CULTURE (CSC).....	329
8.6.2 INTERNAL ORGANISATIONAL MANAGEMENT (IOM) ELEMENTS..	329

8.6.3	HUMAN PREPAREDNESS (P) AND RESPONSIBILITY (R)	334
8.6.4	TECHNOLOGY (TECH) ELEMENTS	337
8.6.5	EXTERNAL ENVIRONMENTAL AND NON-ORGANISATIONAL MANAGEMENT (EENOM) ELEMENTS.....	339
8.7	FRAMEWORK ACTIVITIES AND OUTCOMES	342
8.7.1	IOM ACTIVITIES.....	343
8.7.2	P AND R ACTIVITIES	345
8.7.3	TECH ACTIVITIES	346
8.7.4	EENOM ACTIVITIES	347
8.8	THE FRAMEWORK IMPLEMENTATION TIERS	348
8.8.1	IMPLEMENTATION TIERS: CAPABILITY MATURITY LEVELS.....	352
8.8.2	ACTIVITIES-BASED IMPLEMENTATION TIER MATURITY LEVEL...	354
8.9	CONCLUSION OF THE CHAPTER.....	361
CHAPTER 9: USE CASE IMPLEMENTATION AND FRAMEWORK EVALUATION.		362
9.1	INTRODUCTION.....	363
9.2	FRAMEWORK ASSESSMENT: PHASE 7 OF THE FRAMEWORK PROCESS 363	
9.3	THE FRAMEWORK USE CASE IMPLEMENTATION PROFILE	365
9.3.1	E-HEALTH CYBERSECURITY CULTURE CAPABILITY MATURITY PROFILE	367
9.3.2	USE CASE IMPLEMENTATION	376
9.4	COMPARATIVE ANALYSIS	387
9.4.1	COMPARISON MEASURES	388
9.4.2	COMPARATIVE ANALYSIS AGAINST EXISTING FRAMEWORKS.....	389
9.4.3	SUMMARY OF THE FRAMEWORK COMPARISON.....	394
9.5	EXPERT REVIEWS.....	396
9.5.1	EXPERT REVIEWS INSTRUMENT	397
9.5.2	SELECTION OF EXPERTS	398
9.5.3	INTERVIEW PROCESS	400
9.5.4	ANALYSIS OF EXPERT REVIEWS.....	401
9.5.5	QUANTIFYING EXPERT CONSENSUS.....	413
9.5.6	IMPROVING THE FRAMEWORK AS RECOMMENDED.....	414
9.6	CONCLUSION OF THE CHAPTER	425
CHAPTER 10: CONCLUSION		426

10.1	INTRODUCTION.....	427
10.2	OVERVIEW OF THE STUDY	427
10.3	CONTRIBUTIONS OF THE STUDY	433
10.3.1	THEORETICAL CONTRIBUTION	433
10.3.2	METHODOLOGICAL CONTRIBUTION	435
10.3.3	PRACTICAL CONTRIBUTION	436
10.4	LIMITATIONS OF THE STUDY	437
10.5	FUTURE WORK	438
10.6	CONCLUSION	440
	REFERENCES	442
	APPENDICES	508
	APPENDIX_1: CHAPTER 4.....	508
	APPENDIX_1A: Definitions of the identified CSC factors	508
	APPENDIX_2: CHAPTER 5.....	508
	APPENDIX_2A: Ethical clearance.....	508
	APPENDIX_2B: Hospital permission	509
	APPENDIX_2C: Mpumalanga Provincial Department of Health permission	510
	APPENDIX_3: CHAPTER 6.....	511
	APPENDIX_3A: The questionnaire	511
	APPENDIX_3B - Other parts of demographic information	520
	APPENDIX_3C - Cronbach's Alpha reliability of the construct items.....	522
	APPENDIX_3D: Communalities.....	524
	APPENDIX_3E - Total variance explained.....	527
	APPENDIX_3F - Descriptive statistics	530
	APPENDIX_4: CHAPTER 7.....	533
	APPENDIX_4A: Interview questions.....	533
	APPENDIX_4B: Open code	538
	APPENDIX_4C: Initial 24 themes with their original codes	538
	APPENDIX_5: CHAPTER 8.....	541
	APPENDIX_5A: IOM elements and related activities	541
	APPENDIX_5B: Preparedness and responsibility elements and related activities	543
	APPENDIX_5C: Technology elements and related activities	545
	APPENDIX_5D: EENOM elements and related activities.....	546

APPENDIX_6: OF CHAPTER 9.....	549
APPENDIX_6A: Capability profile template for the activities of preparedness (P) and responsibility (R).....	549
APPENDIX_6B: Capability profile template for the activities of technology (TECH) elements.....	550
APPENDIX_6C: : Capability profile template for the activities of EENOM elements	551
APPENDIX_6D: Expert review questions	552

LIST OF FIGURES

Figure 1.1: Linking Research Questions and Research Objectives (Own source)	12
Figure 1.2: Thesis Layout (Own source)	15
Figure 2.1: Framework of Literature Review (Own source)	21
Figure 2.2: E-Health Ecosystem (Own source)	26
Figure 2.3: E-Health Stakeholders (Fottler et al., 1989).....	29
Figure 2.4: Human Factors Related to E-Health Implementation (Own source)	46
Figure 3.1: Security Goals of E-Health Data and Information	66
Figure 3.2: Reasons Healthcare Organisations are Targeted by Cyber-Criminals (Own source)	68
Figure 3.3: Causes of Data Breaches (IBM Security, 2019).....	81
Figure 3.4: Extraction of Cybersecurity Challenges (own source).....	86
Figure 3.5: E-Health Cybersecurity Threats (own source)	88
Figure 3.6: 2017 and 2018 Data Breaches by Industry (ITRC, 2019).....	89
Figure 3.7: 2019 Data Breach Report by Industry (ITRC, 2020)	90
Figure 3.8: 2023 Data Breach Report (ITRC, 2024)	90
Figure 3.9: Sample of Thedarkoverlord Data Breached Database Up For Sale (Cox, 2016; Storm, 2016)	92
Figure 3.10: Average Data Breach Cost per Record by Industry Sector (IBM Security, 2019)	105
Figure 3.11: Average Cost of Data Breaches by Industry (IBM Security, 2019).....	106
Figure 4.1: Issues Leading to the Introduction and Discussion of Cybersecurity Culture in Chapter 4 (own source).....	113
Figure 4.2: Logical Order Leading to the Domain of Cybersecurity Culture (Own source).120	
Figure 4.3: Cybersecurity Culture Levels (Da Veiga, 2016)	127
Figure 4.4: Cybersecurity Culture Ecosystem (Adapted from Alvarez-Dionisi & Urrego- Baquero, 2019).....	128
Figure 4.5: Step 1 and Phases 1-3 of the Adapted Conceptual Framework Technique (Adapted from Jabareen, 2009)	129
Figure 4.6: Search Database for the First Phase (own source)	130
Figure 4.7: PRISMA Method for the Inclusion and Exclusion of the First Phase (Moher et al., 2009)	132
Figure 4.8: Factors of Cybersecurity Culture (own source generated from ATLAS.ti)	140

Figure 4.9: Categories of Cybersecurity Culture (own source)	146
Figure 4.10: Cybersecurity Culture Theoretical Framework (Georgiadou et al., 2020b).....	148
Figure 4.11: Security Culture Model Theoretical Framework (Da Veiga, 2019).....	150
Figure 4.12: Conceptual Framework of OCybersecurity Culture (Huang & Pearlson, 2019)	151
Figure 4.13: The Human Factor Diamond (HFD) Framework (Alhogail, et al., 2015)	154
Figure 4.14: STOPE Theoretical Framework (Bakry, 2003; Bakry & Bakry, 2005).....	156
Figure 5.1: Research Process Onion (Adapted from Saunders et al., 2016).....	168
Figure 5.2: Research Process Model (Adapted from Saunders et al., 2016)	169
Figure 5.3: Carolina Hospital (Internet).....	179
Figure 5.4: Witbank Hospital (Internet).....	180
Figure 5.5: Systematic Literature Review Process (Xiao & Watson, 2019)	183
Figure 5.6: Synthesis Conceptualisation (Snilstveit et al., 2012; Thomas et al., 2012)	192
Figure 5.7: PRISMA Method for the Inclusion and Exclusion of the First Phase (Revisited) (Adapted from Moher et al., 2009)	194
Figure 5.8: Conceptual Framework Analysis Phases (Adapted from Jabareen, 2009)	197
Figure 5.9: Convergent Parallel Mixed Method (Adapted from Creswell & Creswell, 2023)	203
Figure 5.10: Model of the Data Collection Process (own source).....	205
Figure 5.11: Data Collection Method (own source)	210
Figure 5.12: Stages of Qualitative Analysis (Adapted from Braun & Clarke, 2006).....	215
Figure 5.13: Provinces in South Africa (places.co.za).....	225
Figure 6.1: Step 1 of the Conceptual Framework Analysis (Adapted from Jabareen, 2009)	234
Figure 6.2: Quantitative Data Analysis Process (own source)	237
Figure 6.3: Scree Plot (own source generated from SPSS)	254
Figure 6.4: Quantitative Analysis Model (own source).....	267
Figure 7.1: Phases 1-5 of the Conceptual Framework Analysis Process (Adapted from Jabareen, 2009)	271
Figure 7.2: Qualitative Analysis Process (own source)	272
Figure 7.3: Stages of Qualitative Analysis (Adapted from Braun & Clarke, 2006).....	277
Figure 7.4: Summary of Preparedness Meta-theme (own source generated from ATLAS.ti)	281
Figure 7.5: Summary of Responsibility Theme (own source generated from ATLAS.ti)	285
Figure 7.6: Summary of Management Theme (own source generated from ATLAS.ti).....	290

Figure 7.7: Summary of Environment Theme (own source generated from ATLAS.ti).....	299
Figure 7.8: Summary of Technology Codes (own source generated from ATLAS.ti).....	301
Figure 7.9: Cybersecurity Culture Themes of Public E-Health Institutions (own source)....	304
Figure 7.10: Model of the Final Thematic Diagram (own source generated from ATLAS.ti)	305
Figure 7.11: Revisited Quantitative Analysis Model (own source).....	305
Figure 8.1: Phases of the Conceptual Framework Analysis (Adapted from Jabareen, 2009)	318
Figure 8.2: The CCSCF Overview Diagram (own source).....	320
Figure 8.3: The CCSCF Themes (own source).....	326
Figure 8.4: IOM Theme Elements (own source)	330
Figure 8.5: Human Preparedness (P) and Responsibility (R) Themes Elements (own source)	334
Figure 8.6: Technology (TECH) Theme Elements (own source).....	338
Figure 8.7: EENOM Theme Elements (own source).....	340
Figure 8.8: CCSCF Implementation Tiers (Adapted from Casey et al., 2015; National Institute of Standards and Technology, 2018)	350
Figure 9.1: Step 3 (Phases 7 and 8) of the Adapted Framework Technique (Adapted from Jabareen, 2009)	364
Figure 9.2: Evaluation Methods for CCSCF (own source).....	365
Figure 9.3: Mapping Framework Use Case Profile (own source)	366
Figure 9.4: Overview of CCSCF Elements for Comparison (own source)	388
Figure 9.5: Initial high-level framework structure DIAGRAM A (own source)	419
Figure 9.6: Improved high-level framework structure DIAGRAM B (own source)	419
Figure 9.7: The CCSCF Overview Diagram (Revisited).....	420
Figure 9.8: Step-by-step Guide to Using CCSCF (own source).....	421
Figure 9.9: The Implementation Tier Diagram Reflecting Progression	424

LIST OF TABLES

Table 1.1: Summary of Research Questions, Methodology and Planned Output	13
Table 2.1: Summary of the Health Information Systems Identified.....	36
Table 3.1: Information Security Definitions	57
Table 3.2: Cybersecurity Definitions.....	59
Table 3.3: Computer Security Definitions	61
Table 3.4: Relationship and Differences Between Information Security and Cybersecurity ..	62
Table 3.5: Reasons Why Healthcare Institutions are Targeted.....	74
Table 3.6: Cybersecurity Challenges	85
Table 3.7: 2022 - 2023 Data Breach Report (ITRC, 2024)	91
Table 3.8: Incidents of Data Breach in Healthcare	95
Table 3.9: Successful Ransomware Attack Incidents on Healthcare Institutions.....	99
Table 4.1: Cybersecurity Culture Definitions	135
Table 4.2: Cybersecurity Culture Factors and Their Occurrence in Literature	141
Table 4.3: Cybersecurity Culture According to Category	147
Table 4.4: Theoretical Framework Comparison	157
Table 4.5: The Research Constructs	159
Table 4.6: Contributions of Literature on the Cybersecurity Culture Constructs.....	162
Table 4.7: Mapping Cybersecurity Culture Factors to Identified Constructs	163
Table 5.1: Summary of Research Strategies and Their Applicability in this Research.....	175
Table 5.2: Eight Step Process for Systematic Literature Review	182
Table 5.3: List of Databases Searched for the Literature Review	186
Table 5.4: Data Extraction Form	190
Table 5.5: Summary of the Types of Mixed Method Research (MMR)	202
Table 5.6: Summary of the Questionnaire Sections.....	207
Table 5.7: Research Sub-Questions Addressed by the Data Collection Instrument.....	210
Table 5.8: Summary of Research Questions and Associated Data Collection	211
Table 5.9: Non-probability Sampling Methods (Fink, 2003; Henry, 1990)	223
Table 5.10: Sampling Frame and Responses	229
Table 6.1: Compact Reliability and Reliability	234
Table 6.2: Age of the Participants.....	239
Table 6.3: Gender of the Participants	239

Table 6.4: Education Level of Participants.....	240
Table 6.5: Other Demographics of the Participants.....	241
Table 6.6: Cronbach’s Alpha Reliability of the Construct Items.....	244
Table 6.7: KMO and Bartlett’s Test	246
Table 6.8: Summarised Extraction of the Instrument Communalities.....	247
Table 6.9: Factor Loading and TVE of Preparedness Construct	249
Table 6.10: Factor Loading and TVE of Responsibility Construct	250
Table 6. 11: Factor Loading and TVE of Management Construct	251
Table 6.12: Factor Loading and TVE of Technology and External Environment Constructs	252
Table 6.13: Summarised Descriptive Statistics	255
Table 6.14: Likert Scale Mean Interpretation (Adapted from Pimental, 2010; 2019).....	255
Table 6.15: Descriptive Statistics for Preparedness Construct	256
Table 6.16: Descriptive Statistics for Responsibility Construct	257
Table 6.17: Descriptive Statistics for Management Construct	258
Table 6.18: Descriptive Statistics for Environment Construct	260
Table 6.19: Descriptive Statistics for Technology Construct	260
Table 6.20: Descriptive Statistics for Cybersecurity Culture Construct.....	261
Table 6.21: Pearson Correlation Analysis	262
Table 6.22: Constructs Correlation Decisions	266
Table 7.1: Interview Participant’s Details	273
Table 7.2: Demographic Information	275
Table 7.3: The 22 Themes Identified from Stage 3	280
Table 7.4: Preparedness (P) Theme Category.....	282
Table 7.5: Responsibility (R) Theme Category	285
Table 7.6: Management Theme Category.....	291
Table 7.7: Environment Theme Category.....	299
Table 7.8: Technology Codes	302
Table 7.9: Triangulation of Quantitative and Qualitative Findings	309
Table 7.10: Final Categorised and Integrated List of Cybersecurity Culture Factors	312
Table 8.1: Internal Organisation Management (IOM) Elements and Related Activities	343
Table 8.2: IOM Relation Example of Activity Ref No Column and Activities	344
Table 8.3: Human Preparedness (P) and Responsibility (R) Elements and Related Activities	345

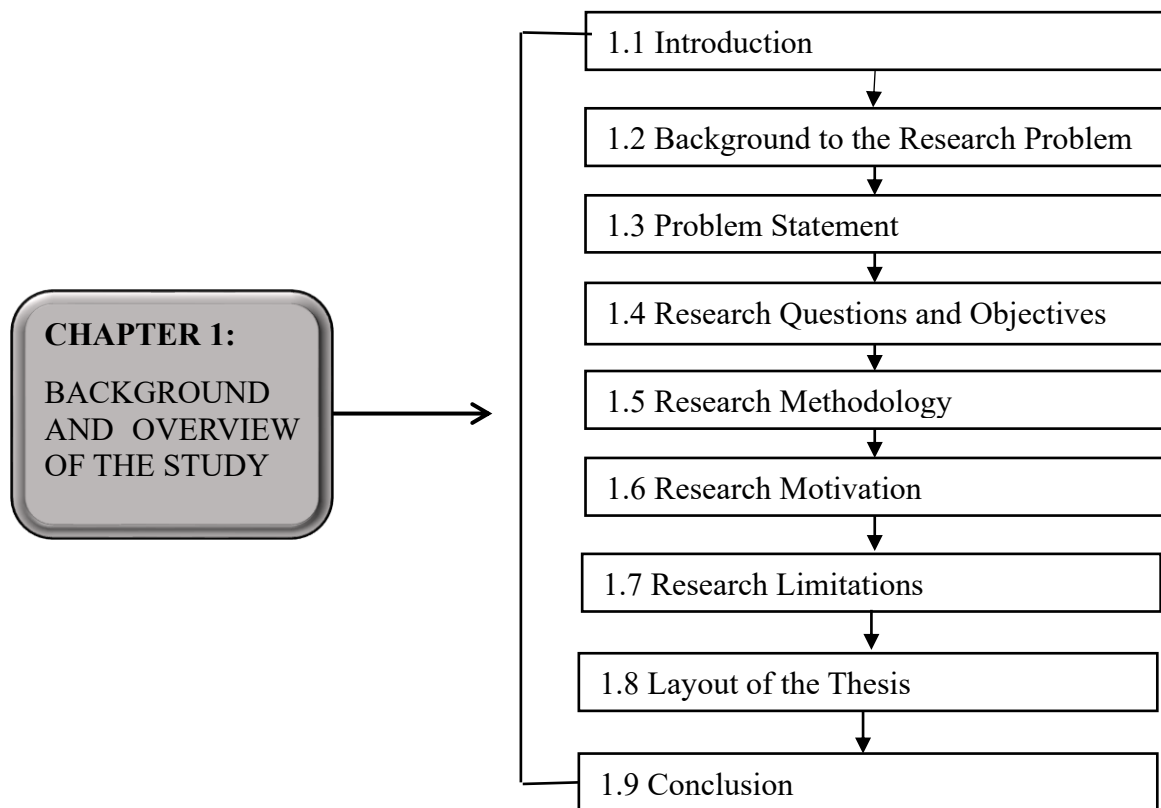
Table 8.4: P & R Relation Example of Activity Ref No Column and Activities	346
Table 8.5: Technology (TECH) Elements and Related Activities.....	346
Table 8.6: TECH Relation Example of Activity Ref No Column and Activities.....	347
Table 8.7: EENOM Elements and Related Activities.....	347
Table 8.8: EENOM Relation Example of Activity Ref No Column and Activities	348
Table 8.9: Implementation Tiers Capability Maturity Level	353
Table 8.10: IOM Activities Implementation Tiers Capability Maturity Level.....	355
Table 8.11: Human Preparedness and Responsibility Activities Implementation Tiers Capability Maturity Level.....	357
Table 8.12: Technology Activities Implementation Tiers Capability Maturity Level	359
Table 8.13: EENOM Activities Implementation Tiers Capability Maturity Level	360
Table 9. 1: Capability profile template for the activities of IOM elements	369
Table 9.2: Intended Capability Percentage Range	373
Table 9.3: Weight Percentage Range	376
Table 9.4: MP Department of Health Capability Profile for the Activities of IOM Elements	379
Table 9.5: MP Department of Health Capability Profile for the Activities of Human Preparedness (P) and Responsibility (R) Elements	382
Table 9.6: MP Department of Health Capability Profile for the Activities of Technology (TECH) Elements.....	385
Table 9.7: MP Department of Health Capability Profile for the Activities of EENOM Elements	386
Table 9.8: IOM Comparative Factor Analysis for the Proposed Framework.....	390
Table 9.9: Human Preparedness and Responsibility Factor Comparative Analysis.....	392
Table 9.10: Human Preparedness and Responsibility Factor Comparative Analysis.....	393
Table 9.11: Expert Review Participants.....	399
Table 9.12: Participants' Sector, Job and Area Frequency	402
Table 9.13: Number of Participants per Organisation Type	403
Table 9.14: Reviewers' Qualifications and Years of Experience.....	404
Table 9.15: Expert Consensus.....	413
Table 9.16: Reviewers' Recommendations and Improvements	414
Table 10.1: Final List of Cybersecurity Culture Factors Used for the Proposed Framework	430
Table 10.2: Objectives, Finding, and Framework Component Mapping	439

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
BHIS	Basic Hospital Information System
CDSS	Clinical Decision Support System
CIA	Confidentiality, Integrity and Availability
CIS	Clinical Information System
CS	Cybersecurity
CSC	Cybersecurity Culture
CPS	Cyber-Physical System
EHIS	Electronic Health Information System
EHIT	Electronic Health Information Technology
EHCR	Electronic Health Care Record
EHR	Electronic Health Record
EMR	Electronic Medical Record
EHS	Electronic Health Service
EPR	Electronic Patient Record
G	Groundedness
HDO	Healthcare Delivery Organisation
HISs	Health Information System
HIS	Hospital Information System

HIT	Health Information Technology
ICT	Information and Communication Technology
IS	Information Systems
IoMT	Internet of Medical Things
IOT	Internet of Things
ISO	International Organisation for Standardization
NCIS	Nonclinical Information System
NHI	National Health Insurance
NHS	National Health Service
MDMs	Medical Device Manufacturer
OECD	Organisation for Economic Co-operation and Development
PHMSs	Personal Health Management System
PII	Personal Identifiable Information
PIS	Pharmacy Information System (PIS)
POPIA	Protection of Personal Information Act
REID	Radio Frequency Identification
THIS	Total Hospital Information System
WHO	World Health Organization

CHAPTER 1: BACKGROUND AND OVERVIEW OF THE STUDY



1.1 INTRODUCTION

Information and Communication Technology (ICT), particularly the Internet, plays a prominent role in transforming human lives worldwide. ICT has had a major impact on many activities in the world in which we live, including those studied by researchers who focus on the social, medical, educational and economic aspects (Baker et al., 2003; Chavula, 2013; De Lange & Von Solms, 2012; Graham & Dutton, 2019; Ragnedda & Muschert, 2013). As a source of information, the Internet has become evermore popular as increasing numbers of individuals have online access. Undoubtedly, the Internet has created an abundance of new possibilities in terms of communication and wide access to, sharing and exchange of information (Chavula, 2013).

Although it is impossible to accurately predict the Internet's future evolution, developments indicate that it has already had a profound impact on the operation of healthcare institutions, their treatment of patients, and the management of healthcare data (Chavula, 2013; De Castro, 2015; Harries & Yellowless, 2013). Hence, Internet technology has been prioritised in providing healthcare services both in developed countries and increasingly in developing countries (Osunyomi & Grobbelaar, 2015).

The use of ICT in the healthcare sector has enabled the implementation of electronic health (commonly called E-Health) services. This has presented opportunities that assist countries, governments and healthcare institutions to achieve their objectives more effectively and efficiently. Research shows that the use of electronic information systems and E-Health information technology has become important in improving numerous aspects of healthcare. These include supporting personal care workers, decreasing the frequency of medical errors, reducing medical costs, facilitating patient identification, encouraging active aging and managing resource allocation (Appari & Johnson, 2010; Krüger et al., 2011; Massoudi et al., 2019; Perez et al., 2022; Popescu et al., 2022; Robbins et al., 2018; Salge et al., 2015). Additionally, development in artificial intelligence (AI) technologies has contributed to and enabled considerably more efficient use of medical resources (Chang, et al., 2023).

In recent years, the use of Electronic Health Information Systems (EHIS) by a variety of stakeholders has intensified globally (in this study, EHIS stakeholders include patients, E-Health providers, healthcare professionals, policymakers and medical insurance companies). EHIS are used to replace existing healthcare paper records, resulting in easier and faster access

to and sharing of healthcare information than ever before (Dahlstrom, 2002; Khubone et al., 2020). Adoption of EHIS is expected to continue to increase, with developing countries following in the footsteps of developed countries who have invested significantly in E-Health systems (Davis et al., 2016; Stroetmann et al., 2011; Yüksel et al., 2017).

While the use of the Internet in the health sector continues to grow, it offers many opportunities and advantages to stakeholders in cyberspace. However, the risks to healthcare data and systems security, privacy, availability and integrity have also increased (Alzubi et al., 2021; Appari & Johnson, 2010; Hassan et al., 2017; Krishnamoorthy et al., 2023; Yüksel et al., 2017). For example, patients' medical records can be made public or be compromised in various other ways that result in them not being available at the required time. In addition, health ICT systems can be manipulated, causing them to malfunction. These cyber risks present serious challenges that ultimately can be seen as human rights violations and can be considered to be not only the result of targeted cybercrime by attackers but also due to ignorance on the part of users or organisations (Da Veiga, 2016). The issue of the responsibilities of users highlights the importance of human factors in addressing cyber risks.

Von Solms and van Niekerk (2013) argue that people in their personal capacity and society are harmed directly by cybersecurity attacks. In the case of E-Health, patients, concerns about associated privacy risks could impact their willingness to divulge health information, and this can in turn result in life-threatening consequences or even loss of life among others (Aldosari, 2025; Alzubi et al., 2021; Yüksel et al., 2017).

It is claimed that healthcare organisations have not managed to keep up with cybersecurity threats, making them particularly vulnerable to evolving cyber threats like ransomware (Aldosari, 2025; Kruse et al., 2017). Ransomware attacks pose serious challenges to E-Health institutions and the health and privacy of patients. To deal with cyber threats and risks in any institution, a coordinated and unified cybersecurity capability has to be employed (Aldosari, 2025; Gcaza, 2017; Gcaza et al., 2015)

It should be noted that in this study, cybersecurity and information security are not viewed as interchangeable; nor is cybersecurity considered to be a subset of information security. Instead, the terms may be viewed as two distinct subsets of security (Whitman & Mattord, 2012) or with cybersecurity being seen as a superset of practices in information security (Rout, 2015). The study views cybersecurity as the practice that protects information resources in addition to the practices that protect other assets, such as individuals who are active online and the

cyberspace environment itself (Rout, 2015; Reid & van Niekerk, 2014a; von Solms & van Niekerk, 2013).

Based on this, cybersecurity is defined in this research is as follows:

Cybersecurity holds a broad view of security practices as it includes the protection of information, individuals active in cyberspace, the cyberspace environment, and assets that extend beyond the borders of an organisational context since cyberspace allows access to information from outside the borders of the organisation.

This research supports the view that information security and cybersecurity are similar but not identical, and this shaped the approach that was adopted in this research.

Therefore, work on cybersecurity culture in E-Health institutions was not treated as information security culture in that environment. This influenced the focus of the literature reviewed in this study.

The remainder of this chapter presents the research outline. **Section 1.2** provides the background of the research problem. This is followed by the problem statement in **Section 1.3**. Research questions and objectives are articulated in **Section 1.4**. Introduction to the research methodology follows in **Section 1.5**. Research motivation and research limitations are presented in **Sections 1.6 to 1.7**. The layout of the thesis is provided in **Section 1.8** and finally, the conclusion is given in **Section 1.9**.

1.2 BACKGROUND TO THE RESEARCH PROBLEM

Cyber-criminals increasingly target healthcare institutions as the industry embraces evolving technologies and increasingly relies on EHIS (Ghafur et al., 2019; Luna et al., 2016; Sendelj & Ognianovic, 2022). It is clear from security incident and data breach reports that the health sector is more seriously affected by this criminal onslaught than other sectors (Mc Loughlin, 2024; Sendelj & Ognianovic, 2022; Symantec, 2015, 2017; Verizon, 2018).

Based on data collected in 2015 worldwide, healthcare security incidents represented 37% of the reported security breaches (Symantec, 2015). In 2017 the health sector was shown to be one of the three most affected services and the sector with most data breach incidents (Symantec, 2017). In the 2018 Verizon report, healthcare institutions were among the top three victims of data breaches (Verizon, 2018). More recent reports give similar statistics, depicting healthcare as one of the top industries affected by data breaches (IBM Security, 2023; Mc Loughlin 2024; Verizon, 2022, 2024).

According to global overview data breaches and incidents reports compiled from the developing and developed world, the health sector is one of the main targets of security breaches (Mc Loughlin, 2024), and human error is considered to be a leading cause of security incidents (Ponemon Institute, 2018; Verizon, 2018, 2022, 2024).

The findings from the literature review on cybersecurity in healthcare organisations confirmed the report statistics given in the preceding paragraphs indicating that healthcare institutions were prime targets of information theft and remain vulnerable to evolving security threats (Kruse et al., 2017; Sendelj & Ognianovic, 2022).

Research indicates that cyber threats manifest in the form of data security incidents which include cases where data is stolen, breached, deleted or corrupted, service denial and hacking of online healthcare devices (Ghafur et al., 2019; Luna et al., 2016; Wang et al., 2013). These threats cause direct harm to patients as an unauthorised change to a patient's healthcare record could result in wrong decisions by healthcare professionals (Ghafur et al., 2019).

The case of the Life Healthcare Group data breach incident that occurred in South Africa in June 2020 (Mungadze, 2020) is evidence that this country is not an exception regarding healthcare cyber threats. Incidents of cyber-attacks on healthcare institutions in other countries include the Ryuk attack on the Druid City Hospital (DCH) regional medical centre in October 2019, the computer disruption at Campbell Country Health (CCH) in September 2019, and the WannaCry attack on the UK National Health Service (NHS) in 2017 (Alder, 2019a; Beahm, 2019; Ghafur et al., 2019; Ghosh & Ashok, 2017; Taylor, 2019).

Healthcare information security is costly (Luna et al., 2016), but healthcare data breaches also carry a significant cost (Ghafur et al., 2019). Reports show that the cost of data breaches in healthcare is almost twice as high as in other sectors (IBM Security, 2019; Ponemon Institute, 2018). More recent reports indicate that the cost of healthcare data breaches continues to increase; for example, a 2023 report shows that data breach costs had increased by 53.3% since 2020 (IBM Security, 2023). The report noted that for thirteen consecutive years, the healthcare industry showed the highest costs in relation to data breaches (IBM Security, 2023). The 2024 global overview also showed a cost increase from 2023 (IBM Security, 2024). This highlights that coordinated cybersecurity efforts need to be immediate and significant. In South Africa, the cost of data breaches has also shown an increase in recent years. For example, 2017 and 2018 saw an increase of over 12% (Moyo, 2018).

Security is viewed globally as being the responsibility of the country's government (International Telecommunication Union (ITU), 2008a, 2021; Wamala, 2011). In addition, cybersecurity is considered to be essential for maintaining national security (Gcaza, 2017; Gcaza & von Solms, 2017a; Jansen Van Vuuren, 2016; State Security Agency, 2015). Several nations have published their national cybersecurity strategies (NCSS), which outline their stance on cybercrime and cybersecurity issues (Klimburg, 2012; Luijff et al., 2013). South Africa has followed suit by developing and approving the National Cybersecurity Policy Framework (NCPF) (State Security Agency, 2015). The country also signed the cybercrime bill (South Africa, 2017) into law (South Africa, 2020) to legislate the objectives of its cybersecurity strategy at the national level.

However, it has been argued that the existence of a cybersecurity strategy and legislation is merely one, albeit a crucial component of the solution to dealing with cyber threats and crime (Da Veiga, 2016). In the past, cybersecurity efforts have focused almost exclusively on using technical means, like anti-virus software and firewalls, to diminish cyber risks and threats (Holdsworth & Apeh, 2017; Pfleeger & Caputo, 2012; Van 't Wout, 2019). However, it may be argued that since there have been numerous unsuccessful technological efforts, technology alone is not sufficient to counter the cyber risks and crimes, and the reason for this is that these often occur due to factors related to human problems (Cavelty, 2007; Forte & Power, 2007; Gcaza, 2017; Gcaza et al., 2017).

Human factors, both with malicious and non-malicious origins, affect the security chain, and if not addressed, will continue to impact negatively on the security process (Appari & Johnson, 2010; Hassan et al., 2017; Kadena & Gupi, 2021; Oladipo et al, 2024; Pollini et al., 2022; Thomson et al., 2006). Consequently, cybersecurity processes should also be investigated from the human perspective instead of focusing primarily on technological controls (Da Veiga, 2016; Gcaza et al., 2015; Gcaza,et al, 2017; Leenen et al., 2018; Leenen & Van Vuuren, 2019; Pfleeger & Caputo, 2012; Wiley et al., 2020).

A lack of a culture of safeguarding security constitutes a security weakness, as having a security culture significantly influences stakeholder compliance with security controls and policies (Bulgurcu et al., 2010). Hence, the Organisation for Economic Cooperation and Development (OECD) security risk management council recommends the promotion of cybersecurity culture as a way of securing information systems and organisational networks (Organisation for Economic Co-operation and Development (OECD), 2005). The International

Telecommunication Union (ITU) also notes the contribution of cybersecurity culture to cybersecurity (International Telecommunication Union (ITU), 2008b). A large number of researchers support the sentiment expressed by the ITU and OECD (Corradini, 2020; Da Veiga, 2016; Da Veiga et al., 2020; Gcaza, 2017; International Telecommunication Union (ITU), 2008a; Holdsworth & Apeh, 2017; Leenen & Van Vuuren, 2019; Saigushev et al., 2020; State Security Agency, 2015; Wiley et al., 2020).

The South African government agrees that cybersecurity culture is fundamental to achieving national security. In their approved NCPF, the government highlighted the promotion of cybersecurity culture as one of its key objectives (State Security Agency, 2015). Additionally, a national strategy for promoting cybersecurity culture at the national level in South Africa was proposed by South African academics (Gcaza, 2017; Gcaza & von Solms, 2017a). Furthermore, Gcaza (2017) developed a national strategy for cultivating cybersecurity culture. Other governments have promoted the development of cybersecurity culture. For example, the 18 OECD member countries foster a security culture (Organisation for Economic Co-operation and Development (OECD), 2005).

While cybersecurity culture is crucial for achieving a secure cyberspace, the culture must be cultivated, and what constitutes the culture must be understood. Research argues that promoting cybersecurity culture at any level must first be understood and measured to guide change (Da Veiga, 2016). Hence, there have been several attempts to define cybersecurity culture (Da Veiga, 2016; ENISA, 2017; Gcaza et al., 2017; Gcaza et al., 2015; Reid & van Niekerk, 2014a). Similarly, researchers have tried to establish what constitutes cybersecurity culture (Corradini, 2020; Reid & van Niekerk, 2014a), while others have set out to develop a methodology for measuring cybersecurity culture at different levels (Da Veiga, 2016). Notwithstanding these efforts, cybersecurity culture is still in its infancy (Da Veiga, 2016; Gcaza & von Solms, 2017b), and research focusing on the area of cybersecurity culture is still considered to need extension (Gcaza, 2017; Gcaza et al., 2017; Gcaza & von Solms, 2017b).

There is a need for cybersecurity culture constructs to be contextualised, taking into account the intended audience, regulatory environment and industry where the cybersecurity culture is to be nurtured (Da Veiga, 2016). Many different sectors and environments exist where cybersecurity is essential and where establishing a cybersecurity culture would help reduce cyber risks and crime. The study looked at cybersecurity culture from the perspective of E-Health institutions, and the South African context was used as a specific case.

1.3 PROBLEM STATEMENT

Despite all the acknowledged problems, costs, incidents and successful cyber-attacks against various sectors of the economy, the cybersecurity efforts initiated by healthcare institutions seem to lag in adopting cybersecurity and cybersecurity culture practices (Kruse et al., 2017; Sendelj & Ognianovic, 2022). While interest is growing in cybersecurity culture, there is still limited work related to the human aspects of cybersecurity (Corradini, 2020; Da Veiga, 2016; Gcaza, 2017; Gcaza et al., 2015; Gcaza & von Solms, 2017b; Leenen & Van Vuuren, 2019). Most of the cybersecurity culture research and development has also been at international and national levels. In contrast, there is limited investigation into cybersecurity culture from the perspectives of institutions and individuals, particularly in a data-sensitive environment like E-Health.

No widely accepted key concepts are evident in the discussions of cybersecurity culture, and this has led to the existence of a weak cybersecurity culture being viewed as an ill-defined problem area (Gcaza, 2017; Gcaza & von Solms, 2017b). Furthermore, there is no comprehensive and articulated list of factors developed solely from the perspective of cybersecurity culture (Mwim & Mtsweni, 2022). Systematic literature reviews to provide the definition, factors and frameworks of cybersecurity culture were found to be inadequate from the standpoint of this research, as the authors viewed information security and cybersecurity as the same (Uchendu et al., 2021).

No framework exists for establishing a cybersecurity culture in public E-Health institutions in South Africa. Corradini (2020) and Da Veiga (2016) argue that available cybersecurity culture frameworks were found to be inflexible and hence could generally not be adopted by other sectors as they could not be easily adapted to fit different contexts or circumstances (Corradini, 2020; Da Veiga, 2016). In addition, no theoretical frameworks have considered frameworks, such as Human Factor Diamond (HFD) and Strategy, Technology, Organization, People and Environment (STOPE), in the development of cybersecurity culture. Furthermore, existing cybersecurity culture frameworks omit factors related to technology as a component or dimension of the framework (Da Veiga, 2019; Georgiadou et al., 2020b; Georgiadou et al., 2021a; Gioulekas et al., 2022; Huang & Pearlson, 2019; Leenen & Van Vuuren, 2019; Mitrovic et al., 2023).

The lack of a well-established cybersecurity culture negatively affects the promotion of a positive cybersecurity posture and the reduction of cyber threats and risks in the E-Health

sector. In addition, this negatively affects national security, because the healthcare sector cannot achieve the NCPF objective of promoting cybersecurity culture.

Having explained the research problem, the problem statement is summarised as follows:

The healthcare sector is increasingly exposed to cyber threats that compromise data confidentiality, integrity, and availability. Incidents such as data theft, corruption, unauthorised access, denial of service attacks, and the hacking of connected medical devices pose direct risks to patient safety, as altered or inaccessible records can lead to incorrect clinical decisions. Evidence from international cases, including attacks on the NHS in the United Kingdom and hospitals in the United States, demonstrates the global scale of the problem. South Africa is not exempt, as was highlighted by the 2020 Life Healthcare Group data breach. The financial implications of such incidents are severe, with healthcare consistently experiencing the highest data breach costs across industries, a trend that continues to rise annually. While cybersecurity strategies and legislation are necessary, technical controls alone have proven insufficient. Research suggests that many cybersecurity failures stem from human-related factors, indicating the need for a greater focus on behavioural and cultural dimensions of security. However, the cybersecurity culture within healthcare in Africa remains underdeveloped, with limited empirical research guiding its implementation. Therefore, there is a critical need to explore and strengthen cybersecurity culture in healthcare institutions to effectively mitigate cyber risks and protect patient well-being.

Subsequent sections outline the research questions, objectives and methodology related to this research problem.

1.4 RESEARCH QUESTIONS AND OBJECTIVES

This research sought to develop a contextual framework for establishing a strong cybersecurity culture in the public E-Health sector to assist with the problems identified. Context is important as it influences the factors and components in a framework that can contribute to the development of a workable cybersecurity culture in an institution. The importance of context is highlighted as a critical point that emerged from the definitions of cybersecurity culture (see **Section 4.12.2**). Based on this, the *Contextual Cybersecurity Culture Framework (CCSCF)* is viewed as a structured way of analysing cybersecurity culture in the given organisational context, and to understand pertinent factors associated with the creation of cybersecurity culture and its management. The E-Health contextual framework proposed in this study aims

to portray and interpret how internal and external interconnected cybersecurity culture factors or components interact to achieve a culture of cybersecurity in an E-Health setting.

This section highlights the research questions derived to solve the main research problem and the associated research objectives they seek to achieve.

This research seeks to answer the following main research question:

How can a contextual framework for establishing cybersecurity culture in the public E-Health institution in South Africa be developed and evaluated?

The objective of the main research question is:

To show and explain the processes followed in the research to develop a contextual framework for establishing a cybersecurity culture in public E-Health institutions.

• **RESEARCH SUB-QUESTIONS AND OBJECTIVES**

The main research question and objective can be better understood by breaking them down into sub-questions with corresponding objectives.

- **Research Sub-Question 1 (RSQ 1):** What cybersecurity threats and challenges confront E-Health institutions?
- **Research Sub-Objective 1(RSO 1):** To determine the cybersecurity threats and challenges that E-Health institutions face.
- **Research Sub-Question 2 (RSQ 2):** What essential factors associated with cybersecurity culture are identified in existing literature that should be considered in developing a Cybersecurity Culture Framework for public E-Health institutions?
- **Research Sub-Objective 2 (RSO 2):** To consult existing literature to identify essential factors associated with cybersecurity culture that need to be considered in developing the Cybersecurity Culture Framework for public E-Health institutions.
- **Research Sub-Question 3 (RSQ 3):** What factors are associated with cybersecurity culture in public E-Health institutions?
- **Research Sub-Objective 3 (RSO 3):** To identify relevant factors associated with cybersecurity culture in public E-Health institutions that need to be considered in developing a suitable Cybersecurity Culture Framework.

- **Research Sub-Question 4 (RSQ 4):** What constructs from existing cybersecurity culture frameworks and other relevant frameworks can inform the design of a contextual Cybersecurity Culture Framework for public E-Health institutions?
- **Research Sub-Objective 4 (RSO 4):** To identify constructs from existing cybersecurity culture frameworks and other relevant frameworks that can support the cultivation of cybersecurity culture in public E-Health institutions.
- **Research Sub-Question 5 (RSQ 5):** How can the factors identified through this research be applied to design and develop a contextual framework for establishing cybersecurity culture in public E-Health institutions?
- **Research Sub-Objective 5 (RSO 5):** To determine how the factors identified in this research can be utilised to develop a contextual framework for establishing cybersecurity culture in public E-Health institutions.
- **Research Sub-Question 6 (RSQ 6):** How can the contextual Cybersecurity Culture Framework be evaluated for relevance, uniqueness and appropriateness?
- **Research Sub-Objective 6 (RSO 6):** To explore how the Cybersecurity Culture Framework that is developed can be evaluated for relevance, uniqueness and appropriateness.

Figure 1.1 depicts how the research questions were mapped to the research objectives. The logic that informed this mapping is to show the interconnectedness between the research questions and objectives. Addressing each research-sub question leads to achieving the corresponding research-sub objective associated with it.

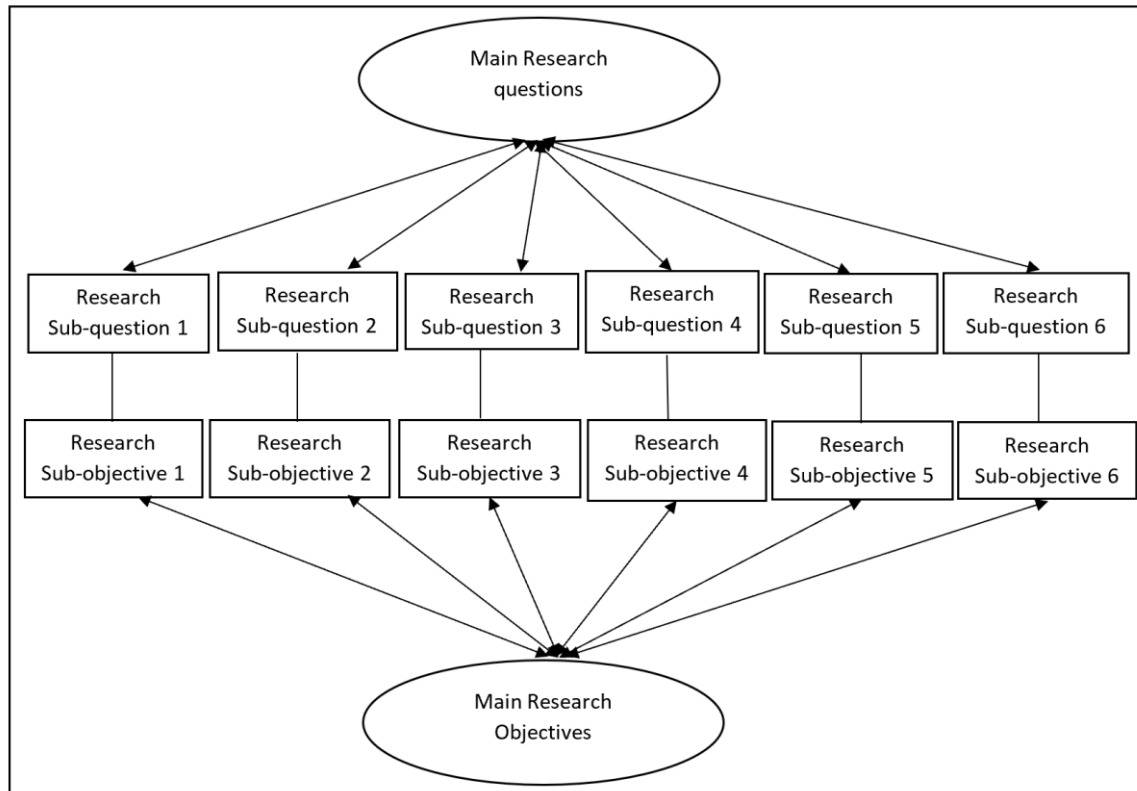


Figure 1.1: Linking Research Questions and Research Objectives (Own source)

The method and design that the researcher followed to answer the research questions and achieve its objectives are unpacked in **Section 1.5**.

1.5 RESEARCH METHODOLOGY

This study aimed to develop a contextual framework to assist with the establishment of cybersecurity culture in public E-Health institutions. To achieve the research purpose, the study was grounded in a pragmatic worldview. The pragmatic philosophy emphasises the practical consequences of the solution proposed to address the research problem (Rylander, 2012) and focuses on answering the research questions (Saunders et al., 2016).

Ontologically, pragmatism can follow a research approach that is subjective or objective or a combination of both, hence it has the advantage of flexibility. Pragmatism is not based on a particular philosophical doctrine. Hence, it can allow the research to make use of various methods, techniques and procedures that allow the research questions to be answered (Creswell & Creswell, 2018; Morgan, 2007).

The research reported on in this thesis followed both deductive and inductive research approaches. Public E-Health institutions in Mpumalanga province, South Africa, were used as

case studies for conducting the research. Mixed Method Research (MMR) strategies were used to collect data using multiple methods and procedures.

The quantitative data was analysed using frequency tables, Cronbach's alpha, Exploratory Factor Analysis (EFA), descriptive statistics and Pearson Correlation, while the qualitative data and document analysis (systematic review) were analysed using themes. The study adopted the research process of Saunders et al. (2016), which is discussed in detail in Chapter 5, to explain various elements of the research methodology.

The design and development of the proposed framework were achieved by adapting the conceptual framework analysis phases (Jabareen, 2009).

Table 1.1 summarises the methods followed and the outcomes achieved for the different research sub-questions and their corresponding sub-objectives. Table 1.1 was also used to depict how the sub-questions and sub-objectives informed the development of the CCSCF in this study.

Table 1.1: Summary of Research Questions, Methodology and Planned Output

RQ and Objective	Methodology	Outcome	Link to framework
RSQ1 & RSO1	A literature review was conducted.	The cybersecurity threats and challenges that confront E-Health institutions were identified.	-
RSQ2 & RSO2	A systematic literature review was conducted.	The factors associated with cybersecurity culture in the literature were identified.	The identified cybersecurity culture factors formed part of the proposed framework elements.
RSQ3 & RSO3	Two research methods, namely a survey and interviews, were used for data collection.	The study identified the factors associated with cybersecurity culture in public E-Health institutions.	The identified cybersecurity culture factors formed part of the proposed framework elements.
RSQ4 & RSO4	A systematic literature review was conducted.	Cybersecurity culture frameworks were identified and discussed. From there, cybersecurity culture constructs were identified.	The identified cybersecurity culture constructs formed the core themes to inform the proposed framework of the study

RQ and Objective	Methodology	Outcome	Link to framework
RSQ5 & RSO5	The conceptual framework analysis phases were applied.	The design and development of a contextual Cybersecurity Culture Framework for E-Health institutions was completed.	The overall design and development of the Cybersecurity Culture Framework was achieved by following the phases of the conceptual framework analysis.
RSQ6 & RSO6	Expert reviews were conducted.	An expert evaluation report for the contextual Cybersecurity Culture Framework was compiled.	Expert reviews were used to evaluate the framework, and the report obtained together with the recommendations made were subsequently used to improve the framework.

1.6 RESEARCH MOTIVATION

E-Health institutions are a favourite target for cybercrime. An important contributing factor is human-related error. Cybersecurity culture is a research area related to cybersecurity and includes human factors, but limited research focuses on the topic. There is little empirical research investigating cybersecurity culture in Africa, and no cybersecurity culture research has been done in the context of South African E-Health institutions. Therefore, there is a need to initiate a study located in South Africa to devise a solution including human-related aspects for addressing cyber threats and cybersecurity culture challenges.

This research was motivated to assist E-Health institutions, predominantly public E-Health institutions in South Africa, with a contextualised framework that would provide structural guidelines for establishing a cybersecurity culture. District and tertiary hospitals located in the rural and urban areas made up the two categories of hospitals used for the study. However, the framework may also be applied in other contexts with similar concerns.

Institutions adopting the developed framework may help to manage the growing number of cyber threats and cybersecurity challenges, and this could significantly reduce the impact of cyber incidents and data breaches, thereby improving cybersecurity within institutions.

1.7 RESEARCH LIMITATIONS

Limitations are delineated below, but others are also explained in detail in Chapter 10.

- The development and evaluation of the proposed framework were limited to the context of one province, namely Mpumalanga, where the research was conducted.

- The investigation was limited to the use case sample from public healthcare institutions.
- The method used to select quantitative, qualitative and expert reviews from participant samples was purposive.

1.8 LAYOUT OF THE THESIS

The layout of the thesis is presented in **Figure 1.2**.

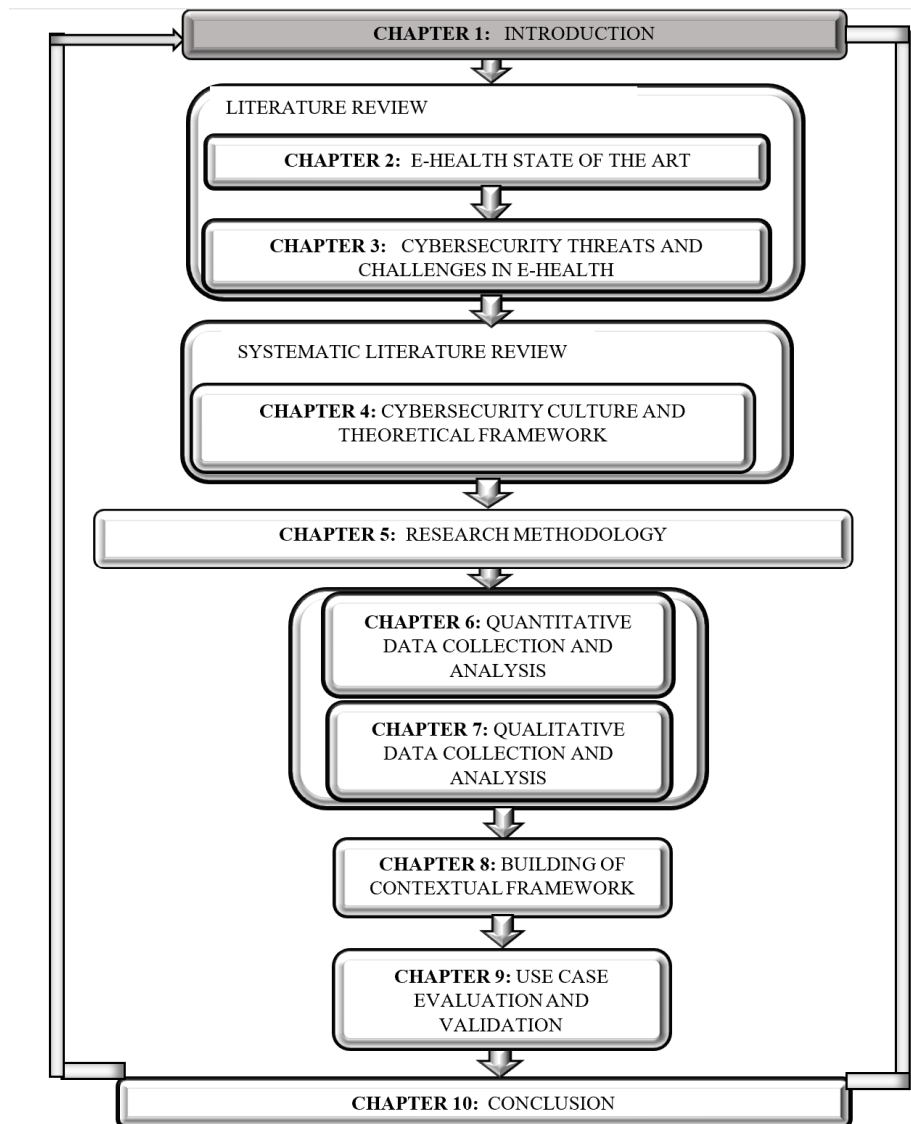


Figure 1.2: Thesis Layout (Own source)

Chapter 1 introduced the research study. The chapter presented the background to the research problem, research questions and objectives, and an introduction to the research methodology. The chapter also highlighted the motivation and limitations of the thesis.

Chapter 2 provides background to the E-Health sector. It defines E-Health and the E-Health ecosystem and provides information on E-Health systems, E-Health stakeholders and how they connect. The chapter also discusses the challenges faced by E-Health institutions.

Chapter 3 presents a review of cybersecurity in general. It discusses cybersecurity challenges in E-Health institutions, provides background for cybersecurity and information security, and describes cybersecurity threats that confront healthcare institutions.

Chapter 4 presents the systematic literature review that was conducted to identify the factors associated with the cybersecurity culture. The chapter also reviews the cybersecurity culture frameworks and describes the research constructs.

Chapter 5 explains the research design and methodology that were introduced in Chapter 1. The philosophical assumptions underpinning the research project, as well as how and where the researcher collected and analysed data to answer the research questions, are also provided.

Chapter 6 presents the quantitative data collection and analysis performed and explains their use in identifying factors associated with cybersecurity culture from the system users' perspectives.

Chapter 7 describes the processes of qualitative data collection and analysis used to identify factors associated with cybersecurity culture from the perspectives of ICT staff, including the ICT manager.

Chapter 8 deconstructs and integrates the cybersecurity culture factors derived from the systematic literature review, quantitative and qualitative data collection, and the analysis performed to develop a contextual framework for establishing cybersecurity culture in E-Health institutions.

Chapter 9 presents the framework evaluation process using case implementation, comparative analysis and expert reviews.

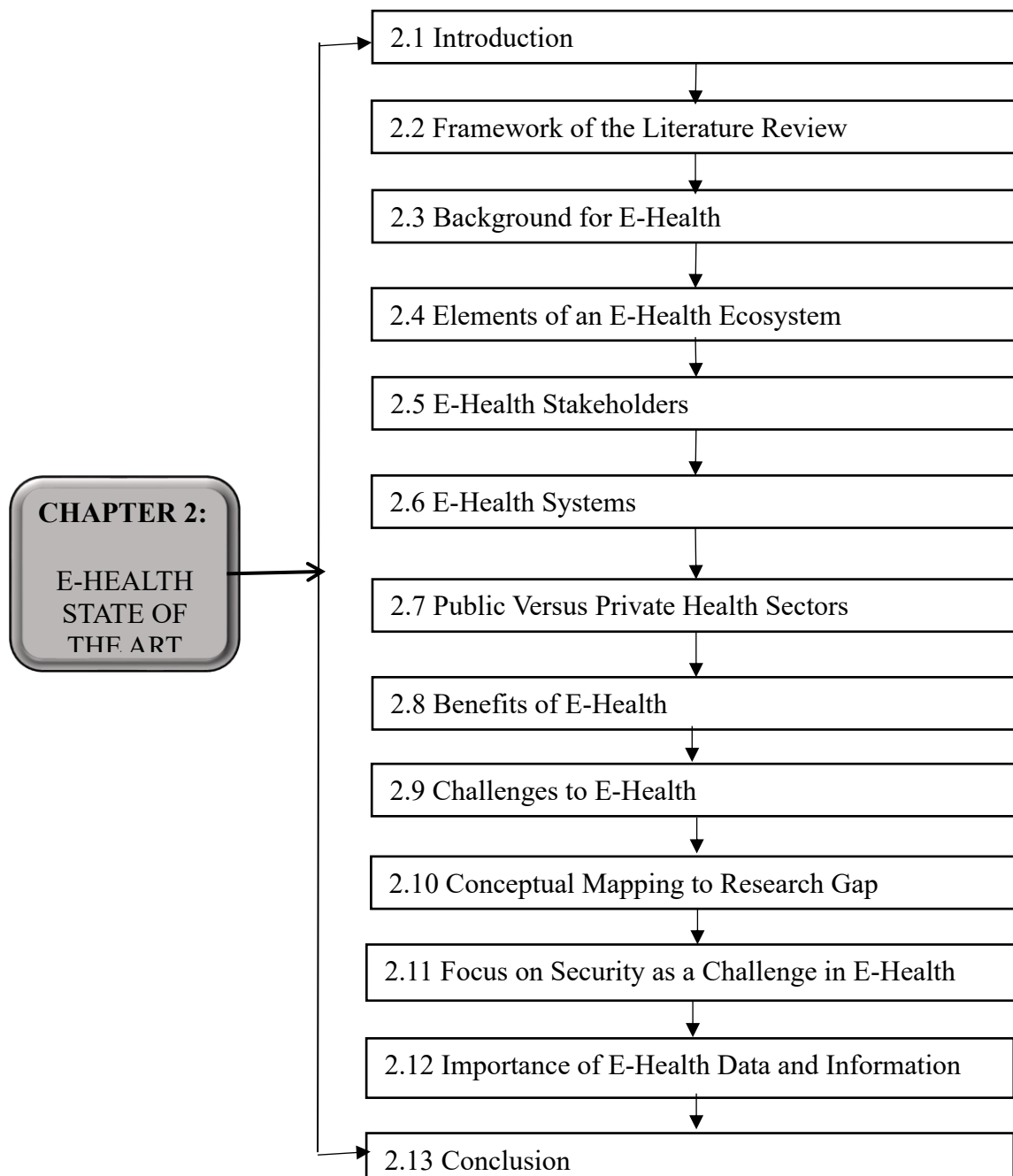
Chapter 10: Concludes the thesis with a summary, limitations, research contributions and future research recommendations.

1.9 CONCLUSION

The main objective of this research was to develop a contextual framework for establishing a cybersecurity culture in E-Health institutions. Chapter 1 was used to provide an overview of the study. The chapter covered the research background, problem statement, research questions

and objectives, overview of the research methodology and the layout of the thesis. The next chapter provides background to the E-Health sector.

CHAPTER 2: E-HEALTH STATE OF THE ART



2.1 INTRODUCTION

Technological innovations are rapidly evolving and affect operations in several sectors, including healthcare. The introduction of these new technologies into healthcare services is essential as they have the potential to improve the quality of healthcare by increasing efficiency, participatory consultation, patient accessibility, empowerment and improving medical diagnoses (Horner et al., 2013; Krüger et al., 2011; Mandava et al., 2016; Pagliari et al., 2005).

Chapter 1 provided an overview of the research study. This chapter provides an overview of E-Health by addressing the “What”, “Who” and “Where” of E-Health. (1) It identifies security concerns, particularly security issues resulting from the interconnected nature of Internet-based health ICT devices. (2) It lays a foundation by describing E-Health's current state as the domain of focus for establishing cybersecurity culture in this study. This is because cybersecurity is a broad research area that applies to a variety of domains.

The next **Section 2.2** provides a framework for the literature review. A background to the concept of E-Health follows in **Section 2.3**. The chapter discusses E-Health elements in **Section 2.4**. A discussion on the categorisation of E-Health stakeholders is given in **Section 2.5** and different E-Health systems are highlighted in **Section 2.6**. A distinction is made between public and private healthcare institutions (see **Section 2.7**) to determine how these affect E-Health. **Sections 2.8** and **2.9** discuss the benefits and challenges of E-Health adoption. In **Section 2.10**, a discussion is provided on the conceptual mapping of the research gap. This is followed by a deliberation on security as the E-Health challenge focus of this study (see **Section 2.11**). The importance of E-Health data and information is stressed in **Section 2.12**. **Section 2.13** is the conclusion to the chapter.

2.2 FRAMEWORK OF THE LITERATURE REVIEW

As stated in Chapter 1, this research aimed to develop a contextual framework for establishing cybersecurity culture in E-Health. To achieve this, the literature review was structured to cover three chapters (Chapters 2, 3 and 4) as the topic deals with a variety of concepts relating to E-Health, cybersecurity and cybersecurity culture.

Since the final focus of this study was on cybersecurity culture, the literature review sections given in Chapters 2 and 3 provided background on the concepts of E-Health and cybersecurity.

As such, the reviews in Chapters 2 and 3 were not considered to be part of any of the phases of the conceptual framework analysis followed in the development of the research framework.

Chapter 2 provides an overview of E-Health, its opportunities, challenges and the significance of E-Health data and information. Chapter 3 investigates the literature on cybersecurity to understand core issues with the topic as it relates to E-Health; it examines reasons why E-Health organisations are highly targeted by cyber-attacks, cybersecurity challenges for E-Health, various cybersecurity threats affecting the sector, the consequences of cyber-attacks, and measures to address cybersecurity issues.

Chapter 4 presents a systematic literature review of cybersecurity culture as the focus of the study. This review helped the researcher to investigate cybersecurity culture definitions, gaps in existing cybersecurity culture frameworks, and factors associated with cybersecurity culture. This review assisted in the identification of constructs used for the development of the research instruments. Additionally, the information gathered was triangulated subsequently with data collected (see Chapters 6 and 7) for the development of the CCSCF.

Figure 2.1 shows how the literature review was approached in this research.

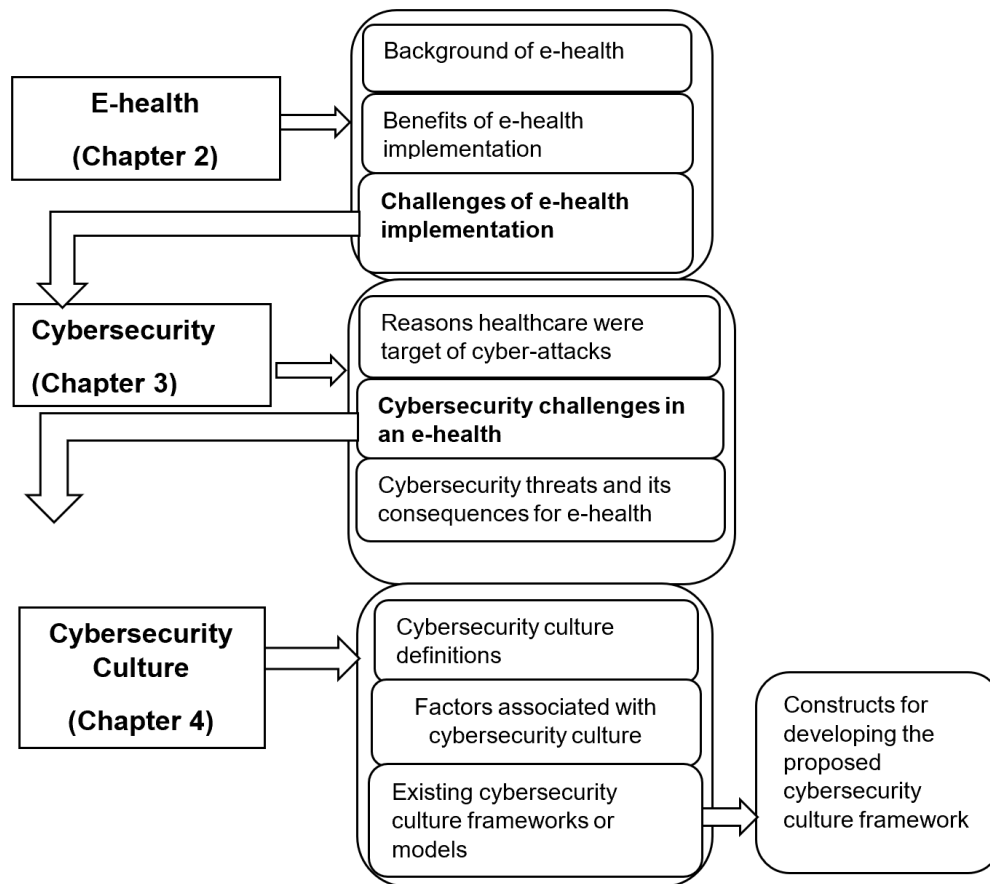


Figure 2.1: Framework of Literature Review (Own source)

2.3 BACKGROUND FOR E-HEALTH

Health covers many areas, from the bureaucratic management of health policies and insurance payments to healthcare service delivery by government, private and non-profit organisations. The involvement of ICT in these activities is called E-Health (Hallberg & Salimi, 2020; Mackenzie, 2010; Zonneveld et al., 2020). The term “E-Health” (occasionally written as “ehealth”) is a broad term that emerged in the late 1990s but is now considered to be a component of digital health (Iyawa et al., 2016). The term was initially created and used by industry and marketing practitioners alongside other “e-words” such as e-commerce, e-government, e-education and e-entertainment for commercial purposes (Bashshur et al., 2011; Eysenbach, 2001; Malakhov, 2023). Hence, the term “E-Health” is generally accepted to reflect the coming together of healthcare and electronic technological advances, often taken to mean “e”; hence “Electronic” and “Health” (E-Health). However, the “e” in E-Health has been suggested to not only refer to “electronic” as it entails other characteristics of what E-Health offers or what E-Health should be. According to Eysenbach (2001), the “e” in E-Health also

reminds the reader of Efficiency, Enhancing quality, Evidence-based, Empowerment, Encouragement, Education, Enabling, Extending, Ethics, and Equity. Moreover, an additional three “e’s” have been highlighted by other authors: Easy-to-use, Entertaining and Exciting. All these elements are now considered to be advantages of E-Health. As a broad term, E-Health can be synonymous with electronic health information technology and electronic health services.

Various formal and informal descriptions and definitions have emerged in the literature. For instance, E-Health was defined as,

“The means to ensure that the right health information is provided to the right person at the right place and time in a secure, electronic form to optimise the quality and efficiency of healthcare delivery, research, education and knowledge” (Deloitte, 2008: 4).

Earlier studies also systematically reviewed the literature on the definitions of E-Health (Oh et al., 2005; Pagliari et al., 2005).

In the field of E-Health, the term has been characterised as,

“not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve healthcare locally, regionally, and worldwide by using information and communication technology (ICT)” (Eysenbach, 2001: 1).

Nevertheless, no agreement has been reached on the precise definition of E-Health, with various definitions, including disparate concepts (Bashshur et al., 2011; Juma et al., 2012; Zonneveld et al., 2020).

Some reports say that developing nations do not fully utilise the potential of E-Health technologies due to infrastructural, ICT and network challenges (Horwood et al., 2023; Kiberu et al., 2017; Kovačić et al., 2022). Since this research was conducted in South Africa, it was essential to view how the country defines E-Health. The South African National Department of Health embraced the WHO definition which defines E-Health as follows:

“the use of ICTs for health to track diseases, treat patients, monitor public health care, conduct research and educate people” (Department of Health, 2012a: 7).

The major criticism of this definition is that emphasis was not placed on the secure and integrated use of E-Health systems. As such, a new definition of E-Health is proposed, as presented in the next section.

- **THE RESEARCH DEFINITION OF E-HEALTH**

Based on earlier definitions and the themes that materialised from the numerous definitions of E-Health in literature, the researcher deemed it necessary to redefine the term to incorporate relevant aspects that form part of the driving force of the research reported on in this thesis. The term is, therefore, defined in this research as stated below.

E-Health is the **secure** use of electronic technologies **integrated (interconnected)** through **Internet networks** (that are **interoperable**) by various stakeholders to perform a given healthcare activity in an institution for a commercial purpose (primarily by private institutions) or at no cost by public and non-profit institutions, to achieve a particular favourable outcome (such as patient-provider interaction, fast access to health data, to track diseases and the delivery of healthcare services) at different geographical levels.

It is argued that the essential elements in the definition and diagrammatic illustration of E-Health (see Figure 3.1) are “security”, “integration”, “interoperability” and “Internet”. These characteristics together were found to be lacking in other E-Health definitions but were essential elements in the E-Health definition in this research.

A. Security

Many studies allude to the security of patient data and institutional security as essential factors that affect E-Health implementation (Furusa & Coleman, 2018; Kovačić et al., 2022; Ross et al., 2016). Others note that the significance of the security factor increases as dependency on E-Health systems increases (Black et al., 2011; Gomes & Lapão, 2008). Advancements in the medical adoption of wireless sensor networks and cloud-based computing capabilities have further increased the security concerns regarding patient data. Security is a major concern related to cyber-based healthcare technologies because, from both the legal and ethical perspectives, patient data is confidential (Ahmad et al., 2021; Haque et al., 2014; Yigzaw et al., 2022).

B. Integration and interoperability

E-Health cannot be fully achieved if the systems that underpin it operate in isolation, resulting in an absence of integration and interoperability (Snowdon, 2020; Basahel et al., 2019). Hence, integration and interoperability are fundamental to digital transformation within health systems.

Interoperability is the ability of ICT systems to exchange data and information and share knowledge with other systems and devices linked to the business processes they support (IDABC, 2004). Interoperability refers to the ability of E-Health systems to operate both inside and outside organisational boundaries as a means to enhance effective healthcare delivery for individuals and communities (Fonseca et al., 2009; Walker et al., 2005). Interoperability allows the mobility of health data from its captured stage to where it is needed, and for this to occur in real time (Snowdon, 2020). Organisations cannot create a consumer-enabled healthcare system without features that enable interoperability, as a lack of interoperability is likely to result in a lack of data and transaction coordination in hospitals (Dogac, 2012; Weber & Kuziemy, 2019). Hence, interoperability standards are essential for accurately exchanging data (Department of Health, 2012a).

Integration is closely related to interoperability. Integrated E-Health systems allow connections with other systems, allowing communication between patients and healthcare providers, the export and import of data between systems, and the transformation of clinical information (Detmer et al., 2008). The importance of E-Health systems integration cannot be overemphasised (Desroches et al., 2010; Mandl & Kohane, 2008).

To achieve efficient and successful medical care, E-Health systems must be integrated using Internet technology, and the systems must be interoperable to enable geographical access to real-time health data and information within and across different organisational, geographical and national levels. Existing E-Health systems that are operating in isolation have been argued as one of the problems confronting South Africa's health departments (Masethe et al., 2013).

C. Internet

The Internet is another term highlighted in the definition of E-Health proposed in this research. The emphasis on this term indicates that E-Health incorporates many aspects of ICT, importantly including the Internet. Advancements in cloud computing-based medical systems

allow authorised stakeholders to access medical data from anywhere in the world and have made the term even more prominent and essential in E-Health.

Given the general use of cloud computing, patients and medical practitioners are unable to access medical data without a connection to the Internet (Haque et al., 2014; Hallberg & Salimi, 2020). The increased dependence of healthcare on the Internet is evident in the use of sensors/RFID (radio frequency identification). It also provides opportunities for cyber consultation and treatment, resulting in the emerging terms cyber-medicine and cyber-healthcare. Cyber-medicine is the consultation of doctors or physicians by patients who are located far apart for treatment via the Internet (Mandava et al., 2016).

However, cyber-healthcare implies a broader meaning than cyber-medicine. Cyber-healthcare indicates the digitalisation of all aspects of clinical work, such as imaging, medication, physical therapy, surgery and preventative measures for better healthcare management (Mandava et al., 2016). In the research reported on here, these two terms were not considered differently, and are not equated to E-Health. Instead, they are regarded as areas of E-Health, just like m-health and telemedicine.

Eysenbach (2001) argues that the original idea behind E-Health was to convey the principles and promises of e-commerce into the healthcare arena and to account for new possibilities the Internet offers to healthcare stakeholders.

Figure 2.2 gives a pictorial definition of E-Health and the ecosystem of E-Health in this research.

The E-Health ecosystem shown in **Figure 2.2** illustrates that E-Health stakeholders use integrated and innovative E-Health systems in different healthcare institutions to enhance healthcare delivery to citizens in other geographical areas as set out in the health policy. The arrows in the **Figure 2.2** show the interconnection between the ecosystem's various elements.

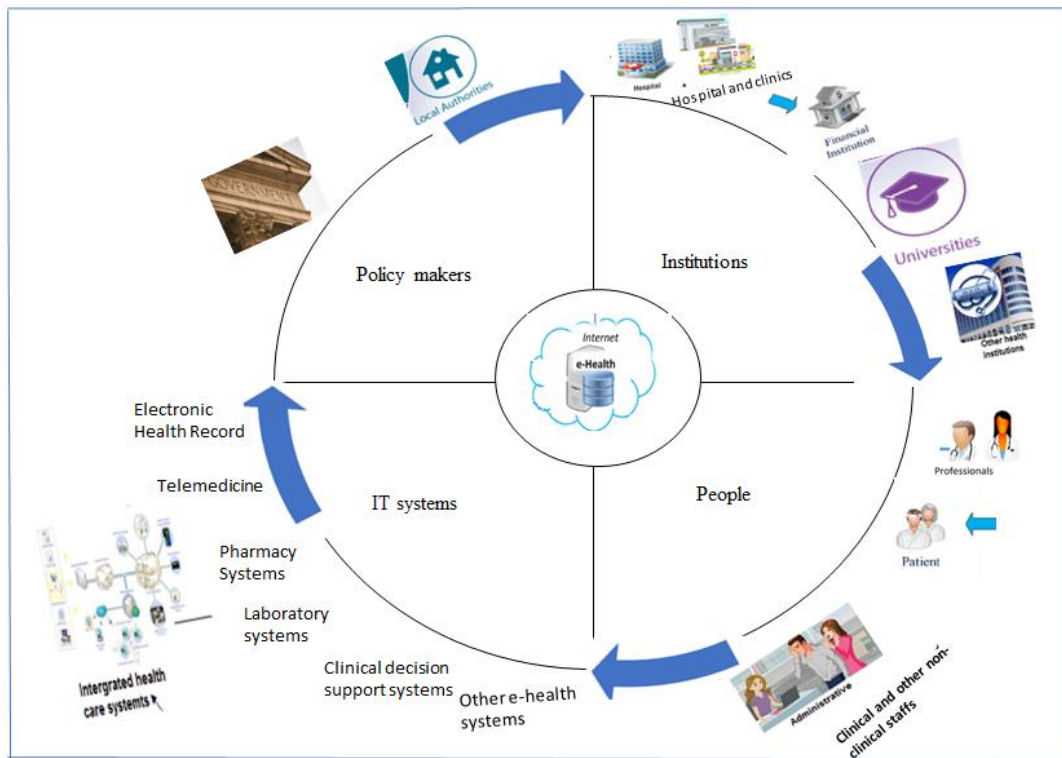


Figure 2.2: E-Health Ecosystem (Own source)

An E-Health ecosystem supports the collaboration between various elements to achieve E-Health. The elements that constitute the E-Health ecosystem are discussed in **Section 2.4**.

2.4 ELEMENTS OF AN E-HEALTH ECOSYSTEM

Figure 2.2 depicts the E-Health ecosystem as defined in this research and has several elements. These include people (the stakeholders), institutions or organisations, systems and technologies, and policymakers.

Stakeholders include patients, citizens, consumers, healthcare professionals (such as doctors and nurses), and non-healthcare personnel (administrative staff, developers, insurance providers, government officials), and any other player contributing to the success or failure of the ecosystem.

Stakeholders make up the primary element that locates, evaluates, uses and communicates healthcare-related information. Collaboration and engagement between stakeholders is essential as they mobilise support, identify opportunities, highlight priorities, and manage and mitigate risk. On the other hand, an absence of stakeholders' engagement contributes to E-Health implementation challenges, including cyber-based security concerns. This stakeholder element of the E-Health ecosystem also involves a bigger group of people who take actions

based on health information and people who use health information to educate themselves and gain knowledge about health issues. E-Health stakeholders are described in detail in **Section 2.5**.

Institutions include medical organisations (such as health centres, clinics, laboratories, pharmacies, and hospitals) and non-clinical institutions (like medical insurance, inventors, universities and research bodies, charitable organisations and associations, and other companies that provide medical services to patients). Hence, institutions include those that use health-related information to conduct research, deliver healthcare, educate, and fund E-Health.

IT systems: The implementation of E-Health depends on a variety of technologies and ICT infrastructure, resulting in one Health Information System (HIS)/IT system or another.

People and healthcare institutions use various ICT systems to enable E-Health in organisations at all levels. ICT Systems are E-Health elements that generate, manipulate, store and disseminate healthcare information electronically using the Internet. The healthcare institutions (including the people, data, and environment) and their ICT systems need to be safeguarded from cyber-based security problems, which can harm the ICT systems and interrupt the successful provision of medical and non-medical services. Various E-Health systems are discussed in **Section 2.6**.

Policymakers are governmental bodies, lawmakers and regulatory authorities who define the strategies and set the rules and regulations governing E-Health and its overall implementation at national, international and organisational levels. This element of the E-Health ecosystem oversees and sets rules on the use of health information. Policymakers are also responsible for setting legislation like the POPIA Act that helps safeguard against cyber-based security problems.

2.5 E-HEALTH STAKEHOLDERS

According to South Africa's eHealth strategy 2012-2017, the successful implementation of E-Health depends on effective collaboration achieved by engaging all stakeholder groups affected by E-Health. This is because E-Health affects various stakeholders and extends across multiple domains such as healthcare provision, personal health, ICT and management.

The concept of hospital stakeholders was discussed in detail in early research (Fottler et al., 1989). The authors viewed hospital stakeholders as people with a vested interest in the hospital. The same sentiment is echoed in the current research on E-Health stakeholders. This is why E-

Health stakeholders are classified using Fottler et al.'s (1989) three types of hospital stakeholders depicted in **Figure 2.3**.

E-Health stakeholders represent various parties (individuals, groups, and organisations) essential in implementing and using E-Health systems. E-Health stakeholders are not necessarily only those from the health sector, but also include those who have an interest in E-Health and are keen to contribute (Talwar et al., 2023; World Health Organization, 2012).

Knowing E-Health key stakeholders helps identify and understand who matters in the E-Health ecosystem and why they matter. Knowledge of E-Health stakeholders is vital, as it helps maintain ongoing engagement and communication, as well as continuous support and guidance for stakeholders. These are essential for successfully implementing the national E-Health vision (Talwar et al., 2023; World Health Organization, 2012).

The E-Health stakeholders are classified into three groups: internal, interface and external. Internal stakeholders operate within the E-Health institutions, including medical and non-medical professionals and management. External stakeholders operate outside E-Health institutions, typically patients, suppliers, competitors, industries, associations, government agencies, third-party players, political groups, professionals' associations and financial communities. The third category interfaces internal and external stakeholder functions to the E-Health institutions, for example, medical professionals and the board of trustees. The key stakeholders include, but are not limited to, patients, citizens, employees (medical and non-medical professionals) and suppliers, but at the centre of all stakeholders are the patients.

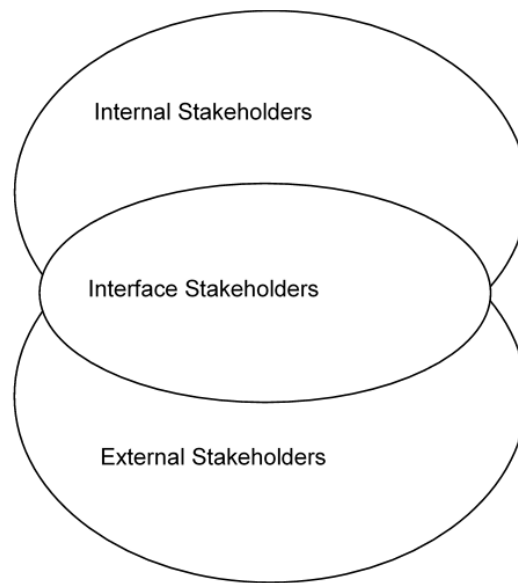


Figure 2.3: E-Health Stakeholders (Fottler et al., 1989)

Stakeholders make use of HISs to support themselves, particularly the patients. Stakeholders collectively evaluate and promote various features of E-Health systems, thereby shaping institutional norms and expectations regarding the use of such systems. The following **Section 2.6** explains different E-Health systems.

2.6 E-HEALTH SYSTEMS

E-Health is applied in different ways suitable for a variety of healthcare requirements. Hence, different systems are used, and these are commonly referred to as Electronic Health Information Systems (EHISs) or Health Information Systems (HISs). Hence, a HIS is a “computer-based information system used in healthcare settings” (Yusof et al., 2008).

According to Ireland’s E-Health strategy,

“E-Health systems are patient-centric and involve the use of modern information systems and technologies to integrate and coordinate the delivery of healthcare to ensure improved patient outcomes, greater efficiencies of delivery, higher levels of transparency and improved ease of access” (An Roinn Slainte Department of Health, 2013:16).

E-Health systems provide various development applications to help patients with medical assistance and diagnosis irrespective of location (Rojas-Mendizabal et al., 2013). However, as indicated in **Section 2.4**, the E-Health systems presented in this section are examples of only

those that need to be safeguarded from cyber threat challenges that would negatively impact the functioning of the integrated E-Health ecosystem.

There are two categories of HIS, Clinical Information Systems (CISs) and Nonclinical Information Systems (NCISs) (Al-Sharhan et al., 2019). CISs include Electronic Medical Records (EMRs), telemedicine, laboratory systems, pharmacy systems, clinical decision support systems, and virtual healthcare. Examples of NCISs are billing systems, inventory control systems, financial accounting systems, and health knowledge management. These systems collect, store, and manage data at various health facilities. Healthcare departments and organisations (such as clinics, medical centres and hospitals) use HISs to aid data processing tasks to improve medical services. Data processed and stored using HISs is also used in research projects and policymaking.

The South African Department of Health views E-Health as encompassing areas, including mHealth and telemedicine, using ICT technologies to strengthen and support healthcare (Department of Health, 2012a). **Sections 2.6.1 to 2.6.9** discuss various HISs in greater detail.

2.6.1 ELECTRONIC MEDICAL RECORD SYSTEMS (EMRs)

EMR is used interchangeably with Electronic Health Records (EHRs) in this research. An EMR allows the creation, acquisition, transmission, use, storage, maintenance and retrieval of patients' (such as lab results, diagnoses, prescriptions and medications) (Evans, 1999; Ross et al., 2015). EMRs allow patients' health record information to be shared and printed as required. The stored historical health data can take various forms (including scanned documents and imaging) (Al-Sharhan et al., 2019). Evans (1999), who created an early EMR, summarised it as an E-Health system that:

- Automates and simplifies existing methods of patients' chart creation, maintenance and retrieval;
- Creates and maintains all patient data electronically, eliminating or supplementing the creation and maintenance of physical data records;
- Provides medical providers with a friendly, easy-to-use, icon-based interface that allows immediate and point of care (source at the point of entry) capturing and analysing patient data quickly and efficiently;
- Manages various formats of patient data, including data from other sources;

- Transforms patient files from static records of clinical interaction into dynamic, comprehensive, real-time records linked to an enterprise-wide clinical database; and
- Makes the patient's EMR instantly available through authorised medical providers across geographical locations.

The characteristics of EMR depicted above are consistent with the International Organisation for Standardization (ISO) definition of EHR (ISO/IEC, 2022).

The purpose of an EHR is to support continuous, efficient and quality healthcare integration (Häyrinen et al., 2008). The following types of HER have been identified: departmental and inter-departmental EMR, electronic patient records (EPRs) (also referred to as computerised patient records (CPRs)), hospital and inter-hospital EMRs, Personal Health Records (PHRs), computerised medical records, digital medical records, clinical data repository, electronic health care records (EHCRs), electronic client records, virtual EHRs and Population Health Records (Häyrinen et al., 2008).

2.6.2 TELEMEDICINE

Advancements in telecommunication technologies have positioned telemedicine as a useful, dependable and feasible E-Health technology (Sood et al., 2007). Telemedicine was initially classified as an ICT health domain (Bashshur et al., 2011). However, this view is not adopted in this research, as more recent literature classifies telemedicine as one of the E-Health systems (Kovačić et al., 2022; Merilampi et al., 2016). When first developed, telemedicine depended entirely on the existing communication technologies (generally, telephone networks using cables) to connect patients with providers. However, with the advancement in ICT, telemedicine now relies on computers and other enabling digital technologies, thereby varying the scope, use and categorisation of telemedicine (Sood et al., 2007; Waller & Stotler, 2018).

Telemedicine is a medical practice that takes place using audio-video communication technologies instead of a traditional co-located doctor-patient consultation (Bird, 1971; Kovačić et al., 2022). The term is now understood as the combined use of telecommunication and computers technologies to provide medical services to persons at a site removed from the provider; the purpose is to improve healthcare access and information in rural areas or areas that are underserved by healthcare specialists (Goldberg, 1996; Grigsby et al., 1995; Perednia & Brown, 1995; Petersen et al., 1996). In the 21st century the term is understood to refer to a

form of telehealth that uses communication infrastructures to deliver services from one geographical location to another (Sood et al., 2007; Tulu et al., 2005).

The differences between recent views and definitions of the term have arisen from the technological and digital innovations that have expanded the genre and scope of telemedicine; telemedicine now plays a larger role than merely connecting patients and providers (Waller & Stotler, 2018). The research interests related to telemedicine may focus on the application or technology (Bashshur et al., 2011). However, what comes out strongly in the definitions is that telemedicine is the delivery of healthcare services to patients who are geographically distant from the physician or provider using a computer, telecommunication and digital technologies that allow communication and exchange of medical information.

Five dimensions of telemedicine have been identified, namely application purpose, application area, environmental, communication infrastructure, and delivery (Tulu et al., 2005). Bashshur et al (2011) classify mobile health (m-health) as a domain of ICT. Other sources define it as a system or aspect of E-Health (Blaya et al., 2010; Department of Health, 2012a). M-health technologies provide additional flexibility as well as other advantages compared to telemedicine. However, the overall purpose is the same: to provide remote medical services and monitoring to patients. M-health is not discussed as a distinct E-Health system in this research, instead, it is considered as a form of telemedicine.

2.6.3 CLINICAL DECISION SUPPORT SYSTEMS (CDSSs)

CDSSs were designed specifically to assist and improve clinical decision-making (Haynes et al., 2010). CDSSs, also referred to as Computerised CDSSs, allow patients' characteristics to be input or retrieved manually. However, software algorithms are used to generate recommendations for each specific patient (Adhikari et al., 2005; Haynes et al., 2010; Randolph et al., 1999).

CDSSs alert, remind, critique, interpret, predict, diagnose, assist and make suggestions to assist the decision maker (Randolph et al., 1999). These recommendations may be delivered to clinicians using EMRs or printouts added to the patient's paper charts to directly help with clinical decision-making regarding individual patients (Randolph et al., 1999).

Examples of CDSS application areas are chest pain diagnosis, infertility treatment, therapeutic drug monitoring and dosing, preventive care, acute care management and timely immunisation administration (Adhikari et al., 2005; Haynes et al., 2010).

2.6.4 PHARMACY INFORMATION SYSTEMS (PISs)

A pharmacy information system is designed to assist pharmacists in ordering, dispensing and tracking medications, with the aim of the safe management and maintenance of the process and information (Alanazi et al., 2018; Blaya et al., 2010). In addition, the systems can help pharmacists manage medication services, improve financial management and increase scientific knowledge about medication management.

Other benefits of PISs include the prevention of medication errors and the minimisation of prescription and dispensing turnaround time (Chapuis et al., 2010). A pharmacy system is a complex system designed for pharmacists and doctors to meet the needs of pharmacy departments (Ismail et al., 2013). Hence, these systems should support the following pharmaceutical activities: inpatient and outpatient order entry, management and dispensing, inventory and purchasing management, reporting, clinical monitoring, manufacturing and compounding, intervention management, medication administration, connectivity to other systems and pricing, charging and billing (Troiano, 1999).

2.6.5 PATIENT-CENTRED HEALTH INFORMATION SYSTEMS

A central E-Health system manages comprehensive patient care information and, in particular, entails a higher level of patient involvement. Such systems assist in the collection of patients' information, integrate it with clinical information, interpret the integrated information, provide clinical recommendations for each individual patient, and facilitate patient action (Krist & Woolf, 2011).

The term 'patient-centred system' is viewed and used synonymously with 'citizen-centred health system' in this research. It entails patients receiving information regarding their health and taking part in making decisions related to their personal health issues as part of disease prevention and follow-up (Gatzoulis & Iakovidis, 2007). Citizen-centred health systems can be supported by Personal Health Management Systems (PHMSs).

PHMSs connect the individual to health information networks (Gatzoulis & Iakovidis, 2007). They can also enable continuous monitoring of different bio-signals, empower the patients by establishing their role in managing health status, optimise communication and create a user-friendly interface between the patient and doctor. PHMSs are available as wearable, portable,

and even implantable devices and in-vitro diagnostic point-of-care devices for usage at home (Gatzoulis & Iakovidis, 2007).

2.6.6 HOSPITAL INFORMATION SYSTEMS (HISs)

Several explanations exist for the purpose of a HIS. It enables the overall management of a hospital's medical and administrative information to assist healthcare workers in performing their duties effectively and efficiently (Winter & Haux, 1995). It is an integrated computer system that records, manipulates, and retrieves both clinical and administrative information related to medical services within the hospital (Suter et al., 2009). Similarly, a HIS is defined as a comprehensive computer system designed to improve the clinical and administrative operations of a hospital (Esfahani et al., 2018; Kim et al., 2002). Hence, a HIS provides opportunities ranging from medical to administrative systems, such as high quality and better patient care, better support for clinical care, patient care planning, cost reduction, and improved decision-making for clinical and administrative staff (Coventry & Branley, 2018; Hsiao & Chen, 2016; Lee et al., 2012a; Seyedin et al., 2024).

Initially (in the 1960s) HISs were designed to support hospital financial services but were later (in the 80s) used to perform clinical activities. HISs are still used to perform both clinical and administrative functions in almost all hospitals. The three categories of HISs are: Total Hospital Information System (THIS), which is typically implemented by big hospitals with more than 400 beds; Intermediate Hospital Information System (IHIS), usually used by hospitals with between 200 and 400 beds; and lastly Basic Hospital Information System (BHIS), mostly implemented by hospitals with fewer than 200 beds (Lee et al., 2012a).

Important HIS functions allow for (Gell & Gitter, 2008; Lee et al., 2012a):

- a) *clinical order entry* - patients can sort out administrative hospital issues before their admission
- b) *scheduling* that allows for the timely sequencing of diagnostic and therapeutic procedures in the necessary order
- c) *creation and maintenance of electronic patient records* - digitally storing all records of patient interaction with the healthcare provider
- d) *structured reporting*, which replaces ordinary paper reporting by allowing presentation of images together with facts and data

- e) *process management* that offers users appropriate overviews and workloads based on their role and activities, as well as clinical pathways that identify activities necessary in all the steps of getting patients the correct treatment.

2.6.7 CYBER-PHYSICAL SYSTEMS (CPSs)

The CPS is a wireless sensor network that combines computation and communication capabilities with physical-world interactions (Haque et al., 2014; Coventry & Branley, 2018; Wang et al., 2011). It is a life-critical, context-aware networked medical system that performs functions such as sensing, processing and networking for both in-hospital and in-home patients (Lee et al., 2012b). It observes patients' conditions remotely and acts regardless of their location. Like many E-Health systems, CPS provides benefits such as facilitating interaction between humans (observing the patients and alerting medical staff) and systems very rapid response, and as a result, better system performance. According to Haque et al. (2014), CPSs in healthcare introduce the “coordinated interoperation of autonomous and adaptive technological devices, and body area networks”.

Architectural flow and operation of CPS include (Haque et al., 2014; Lee et al., 2012b; Wang et al., 2011; Wu et al., 2011):

- a. Collecting patient data using sensors and sending it to cloud storage using a gateway,
- b. Processing data held in the cloud storage and executing queries in real-time,
- c. Processing historical data in response to a query,
- d. Performing calculations and then generating an alarm, and sending these to the observation centre,
- e. Facilitating access by clinicians to patient data stored in the cloud,
- f. Enabling clinicians to consult other healthcare systems,
- g. Receiving responses from other healthcare systems, and
- h. Sending decisions from clinicians and specialists to the actuation component.

2.6.8 LABORATORY SYSTEMS

A computerised laboratory system that performs the functions of data validation, administration, electronic transmission, and storage is classified as a clinical support system (Bemmel et al., 1997). Therefore, laboratory-specific activities, such as reporting lab results to

healthcare workers, are achieved using laboratory systems (Blaya et al., 2010; Coventry & Branley, 2018). Different types of laboratory systems exist and perform specific functions. Those used for medical diagnosis are known as clinical laboratory systems. Other types are industry and environmental laboratory systems. Important benefits of laboratory systems include human error reduction to ensure that test results are reliable, improved productivity and support for important health decision making by patients.

2.6.9 OTHER E-HEALTH SYSTEMS

There are several other HISs, including radiology systems, nursing information systems, picture archiving and communication systems, patient reminder systems, hospital information systems, routine health management systems, antenatal care systems, patient registration systems, and cyber healthcare systems such as triage systems and situation recognition systems.

Table 2.1: Summary of the Health Information Systems Identified

E-Health systems	Description	Authors
EMR/EHR	An E-Health system that allows for the electronic creation, acquisition, transmission, use, storage, maintenance and retrieval of patients' data (such as lab results, diagnoses, prescriptions and medications).	(Evans, 1999; Ross et al., 2015)
Telemedicine	Telehealth systems that use communication infrastructures to deliver synchronous or asynchronous healthcare services in rural and small-town settings to achieve clinical or non-clinical purposes and to address uneven distribution, infrastructural shortage and human resource challenges.	(Sood et al., 2007; Tulu et al., 2005)
Pharmacy information systems	A HIS sub-system designed to help pharmacists oversee the medication process in a safe manner. PIS also assists pharmacists and the hospital in managing medication services, enhancing financial management, and expanding scientific understanding of medication management.	(Alanazi et al., 2018; Chapuis et al., 2010)
Laboratory system	This type of system is used to perform laboratory-specific activities. Its functions and activities include data validation, administration, electronic transmission, storage, and reporting of lab results to healthcare workers.	(Bemmel et al., 1997; Blaya et al., 2010)
Clinical Decisions Support Systems (CDSSs)	Computerised CDSSs are designed specifically to assist with clinical decision-making by matching the characteristics of a specific patient to a computerised knowledge base to generate assessments or recommendations for clinicians.	(Adhikari et al., 2005; Haynes et al., 2010; Randolph et al., 1999)

E-Health systems	Description	Authors
Radiology system	These support radiology services by acquiring and analysing radiology images, storing, manipulating, and retrieving patient information, and carrying out other administrative functions. Examples of radiology systems include Picture Archiving and Communication Systems (PACS).	(Bemmel et al., 1997; Ismail et al., 2013)
Clinical system	Clinical systems are computer-based systems that collect a wide variety of data for patient care, research, management, planning, and maintenance of other systems and data repositories. The system stores, processes, and makes essential clinical information available for the purpose of healthcare delivery. Examples include nursing systems and antenatal care systems.	(Ammenwerth & de Keizer, 2005; Gardner et al., 2014; Ismail et al., 2013)
Patient-centred information system	A system that facilitates patient involvement. The system's functions include collecting patient information, integrating it with clinical information, interpreting clinical information, providing clinical recommendations for each individual patient, and facilitating patient action.	(Cliff, 2012; Gatzoulis & Iakovidis, 2007; Krist & Woolf, 2011)
Patient reminder systems	These systems remind patients to take a particular health action, like attending routine check-ups or taking medication.	(Blaya et al., 2010)
Administrative systems and routine health management systems	These systems document the essential business processes and routine transactions of healthcare organisations. They maintain data related to patients' registrations and schedules, admission, discharge, and transfer. Administrative systems assist healthcare organisations with managing their daily operations. The systems handle billing for medical services and other management processes. Subsystems in the areas of equipment, inventory, finances, and accounting in the clinical environment are commonly included. The overall purpose is to automate the administrative activities of health institutions.	(Glandon & Buck, 1994; Jiang et al., 2000)
Nursing information system	These are clinical systems that manage data from various healthcare environments for the timely and orderly availability of data to help medical workers, particularly nurses, in improving medical services to patients.	(Ismail et al., 2013; Merilampi et al., 2016)
Hospital information system	These computer systems are designed to manage the clinical and administrative functions of a hospital.	(Esfahani et al., 2018; Kim et al., 2002)
Cyber-Physical system (CPS)	This is a wireless sensor network that monitors the physical status of a patient remotely, irrespective of the patient's location.	(Haque et al., 2014)

The overall purpose of E-Health systems is to enhance healthcare (Crock, 2016). The E-Health systems described in Table 2.1 offer many opportunities to different healthcare sectors but have associated challenges. Security issues, particularly cyber-related threats, have been highlighted

as a particularly serious threat that compromises the use of these systems. Before discussing E-Health challenges, categories of the healthcare sector are presented in **Section 2.7**.

2.7 PUBLIC VERSUS PRIVATE HEALTH SECTORS

The purpose of this study was to build a CCSCF for public healthcare institutions using South Africa as a case study. To achieve this, it is essential to understand both the public and private healthcare sectors where E-Health can be implemented and their similarities and differences, particularly in South Africa.

Public and private healthcare sectors are common worldwide, and this is also the case in South Africa (Hassim et al., 2007). This two-tier healthcare system divides South Africa along socioeconomic lines, leading to rich and poor health sectors. To ensure equal access to quality healthcare, the South African government has recently (May 2024) signed the National Health Insurance (NHI) bill into law. The government aimed to use E-Health to ensure equality in healthcare services for all (Department of Health, 2012a, 2017).

The public healthcare system is state-owned. It is funded through state and government funds and used to offer free healthcare services to citizens, especially those without any medical scheme coverage. The major advantages of public healthcare are free access to medical services, including medical visits and medications, and many healthcare facilities. Free healthcare benefits those who otherwise would not be able to afford healthcare. However, public healthcare comes with many shortcomings, such as high patient numbers resulting in rushed appointments and long waiting periods, outdated facilities, poor quality healthcare due to a shortage of key healthcare professionals, and poor disease control and prevention practices (Department of Health, 2017; Young, 2016). Other shortcomings include a delayed response in emergency services, unreliable and error-prone laboratory diagnostics and insufficiently trained staff (Mandava et al., 2016).

On the other hand, the private healthcare sector runs as a business with the purpose of making profits.

“Private sector comprises all private health service providers, professionals healthcare, representative institutions , private health facilities (like hospitals and laboratories), funding mechanisms of private health services and traditional health practitioners.” (Hassim et al., 2007).

In the private healthcare sector, hospitals and healthcare facilities are owned and governed by individuals or groups. As private healthcare sectors are funded by the owners and the overall purpose is to make a profit, citizens pay for healthcare services in this sector. The major disadvantage of a private health system is the high cost of medical care (medical visits and medications) (Hassim et al., 2007; Young, 2016). Hassim et al. (2007) argue that the high cost of private healthcare is a result of collusion among hospital groups, an increase in medical scheme premiums, and the anti-competitive pricing of medicines.

Nevertheless, the private healthcare sector has almost none of the problems that plague the public healthcare sector, which were noted above. It is for this reason that citizens who can afford it purchase private medical insurance to cover the cost of treatment at private facilities (Young, 2016). These citizens are either employed or wealthy, leaving only the poor to use the public healthcare system (Hassim et al., 2007). This deepens the inequalities that currently exist in the country.

In addition to the mismatch in ownership, funding method, economic conditions of citizens, medical costs, and pros and cons between the public and private healthcare sectors, there is also a mismatch between the two healthcare sectors regarding their geographical distribution, and there are also inefficiencies in the use of available human resources (Department of Health, 2017). Private healthcare facilities are mainly located in urban and wealthy areas where most of the available human resources are, while rural hospitals and clinics are faced with serious shortages, including the unavailability of trained staff who choose to work there (Department of Health, 2017; Hassim et al., 2007). The public healthcare sector also lags behind in providing the necessary training and education to health professionals (Department of Health, 2017).

The gaps that exist between the public and private healthcare sectors, such as outdated facilities and a lack of training and education, negatively affect the public E-Health sector in many ways. This is also evident in the ways that cyber-criminals can attack public healthcare systems and how cybersecurity is being approached in the sector.

Irrespective of whether the healthcare sector is public, private, or slowly moving towards NHI, there is a consensus on the important benefits the use of ICT in healthcare brings to the health sector. However, the realisation of these benefits has been slower than anticipated. The next **Sections 2.8 and 2.9** discuss some of the benefits and challenges of E-Health.

2.8 BENEFITS OF E-HEALTH

Over time, as the dependence on and the increasing number of advantages of E-Health have become evident, it has been recognised as an essential component of best practice. According to An Roinn Slainte Department of Health (2013), high-performing E-Health systems support many aspects of patients' diagnosis, treatment and care, and reliably and sustainably deliver efficient, effective, high-quality and safe services to patients. In addition, they are essential to business support and governance at the corporate level and are central to strategic, management and operational development, planning and control. Hence, they act as important and distinguishing enablers of transformation and development at the organisational level but are also critical to population health, well-being and policy formulation at a national level.

The 2012-2020 European Union E-Health action plan indicated that E-Health can benefit all stakeholders, that is, the citizens, patients and healthcare professionals, as well as healthcare organisations and public service authorities (European Commission, 2012). When applied well, E-Health can provide personalised citizen-centric healthcare, improve the effectiveness and efficiency of service, and facilitate both socio-economic inclusion and patient empowerment (European Commission, 2012).

Benefits of E-Health include improved communication between different E-Health stakeholders (Brandeis et al., 2007; Lindner et al., 2007), easy, fast data access and sharing (Ahmad et al., 2021; Rengamani et al., 2010; Yüksel et al., 2017), and decreased healthcare-related costs such as administrative costs (Francis, 2013; Mandava et al., 2016; Wikler et al., 2012; Yüksel et al., 2017). Added benefits are patient prioritisation, patient monitoring, time-saving, system accuracy, more accurate medical diagnosis and the introduction of entirely new health services (participatory consultation) (Ahmad et al., 2021; Mandava et al., 2016).

In addition to these benefits, studies in developing countries show that E-Health is a single solution that solves many disparate problems as it facilitates collaboration between various governmental bodies, gives easy access to healthcare facilities for patients and health workers, and increases the quality of healthcare (Kovačić et al., 2022; Khalifehsoltani & Gerami, 2010; Mostafa et al., 2010).

Despite the number of E-Health opportunities documented, its adoption remains disappointingly low, particularly in developing countries (Juma et al., 2012). This low rate of adoption can be attributed to challenges that hinder its implementations. These challenges are discussed in **Section 2.9**.

2.9 CHALLENGES TO E-HEALTH

E-Health challenges may have internal causes or arise from entities or events that are external to an organisation. They often become evident as cost, human problems, security concerns and time. The underlying challenges are serious, given that E-Health is expanding because of the rapid growth of Internet-based ICT systems. **Subsections 2.9.1 to 2.9.10** outline the E-Health challenges with references to support.

2.9.1 INCREASED TIME

The amount of time that health workers, particularly nurses, spend on documentation has not changed with the implementation of E-Health and this was found to be due to ineffective learning and use of E-Health (Munyisia et al., 2011). However, the time needed to document and retrieve patient data with E-Health systems (for example, HER) was found to increase, resulting in organisational inefficiency (Black et al., 2011). The additional time required to select, implement and learn E-Health systems also slowed physicians' workflow down (Boonstra & Broekhuis, 2010).

Other authors report that the lack of adequate time available for staff members to teach or learn to use the new E-Health systems hinders the adoption of E-Health (Gagnon et al., 2012; Horwood et al., 2023; Police et al., 2011).

2.9.2 E-HEALTH TECHNOLOGY ICT INFRASTRUCTURE AND OTHER RESOURCES

Lack of access to adequate ICT infrastructure and E-Health technologies has been identified as an internal factor that affects E-Health implementation (Furusa & Coleman, 2018). According to these authors, E-Health systems and technologies in some developing countries are limited by inadequate ICT infrastructure and support, and several hospitals lacked suitable technologies for the implementation and use of E-Health.

The most frequent use of ICT tools in the developing world is for procurement and administration functions, highlighting the need to add many other clinical health technologies. The more recent research by Ksibi et al. (2023) affirms earlier research by Catwell and Sheikh (2009) and indicates that hospitals continue to lack adequate technologies and the necessary ICT infrastructure to support E-Health.

Insufficient infrastructure, such as a constant power supply (Oluoch et al., 2012; Saliba et al., 2012), access to suitable mobile phones and computers (Kilsdonk et al., 2011; Oluoch et al., 2012), a reliable Internet connection (Oluoch et al., 2012; Saliba et al., 2012), and enough bandwidth (Saliba et al., 2012) have been described as having a positive impact on the implementation of E-Health.

Lack of other resources, including experts who can implement the systems and train staff to use them (Gagnon et al., 2012; Police et al., 2011), and inadequate medical facilities (Furusa & Coleman, 2018) have also been reported as limitations. The lack of these often makes E-Health projects unsustainable.

2.9.3 TECHNICAL SUPPORT

Technical support by ICT specialists is essential for maintaining and running E-Health systems (Furusa & Coleman, 2018). The authors identified inadequate technical support (due to not having associated ICT departments), a lack of ICT expertise, and unhelpful attitudes and behaviour of ICT staff as challenges that undermine the proper functioning of E-Health systems.

A systematic review by Ross et al. (2016) supports this view and highlights the importance of a strategy that identifies the provision of permanent technical support staff as an essential resource. Lack of technical support staff when needed results in technology downtime and this in turn disrupts workflow and makes it impossible for those in other roles to meet their responsibilities (Ross et al., 2016). Hence, the provision of technical assistance was identified as a complex factor that affects E-Health implementation (Horwood et al., 2023; Moxey et al., 2010).

2.9.4 INCREASED INEQUALITY

The implementation of E-Health systems may intensify existing inequalities in society at the international, national and organisational levels. This inequality is highlighted when referring to users and non-users of E-Health systems.

The characteristics of a country or the size, location and richness of the hospital, influence the type, if any, of E-Health systems that can be implemented. Richer and bigger hospitals, such

as teaching hospitals and hospitals in rich and developed countries and areas, are more likely to implement a variety of E-Health systems (Jha et al., 2009).

2.9.5 COST

Many studies have identified issues related to reduced operating costs as a benefit for implementing E-Health in the introduction, but many others have identified cost (in this case, initial outlay costs) as a challenge for E-Health.

Studies have consistently reported costs associated with acquiring E-Health systems as a major factor that negatively influences E-Health implementation (Benavides-Vaello et al., 2013; Fontaine et al., 2010; Gagnon et al., 2012, 2014). The high cost associated with E-Health implementation was highlighted again more recently as part of the core challenges to E-Health implementation (Al-Sharhan et al., 2019; Ksibi et al., 2023). Cost can be grouped according to the stage of the project: start-up costs include obtaining hardware, professional services and developing infrastructure (Al-Sharhan et al., 2019; Boonstra & Broekhuis, 2010; Police et al., 2011); maintenance costs and operating costs include the cost of updating rapidly changing technology or a need to extend the system to take advantage of additional options (Al-Sharhan et al., 2019; Benavides-Vaello et al., 2013; Police et al., 2011).

2.9.6 FUNDING

Adopting E-Health directly relates to the funding allocated (Mugo & Nzuki, 2014). Increased funding encourages the implementation of E-Health in the developed world, and the same can be expected to apply in the developing world (Zhang et al., 2015). However, developing countries all face national funding problems, which means a limited budget allocated to the health sector. This makes it very difficult to fund high-cost ICT systems, technologies, and services for implementing E-Health.

2.9.7 SYSTEM ISSUES

The following elements are system-related issues highlighted in the literature:

Integration: Poorly integrated healthcare systems have the potential to increase the frequency of medical errors, decrease operational efficiency, and reduce the quality of healthcare services (Basahel et al., 2019; Bygstad et al., 2015; Erku et al., 2023). The significance of integration

has been highlighted as one of the essential characteristics of E-Health (Basahel et al., 2019; Bygstad et al., 2015; Erku et al., 2023).

Interoperability: Lack of interoperable health systems is a major obstacle to E-Health adoption (CSIR & NDOH, 2014; Juma et al., 2012). A study conducted in Uganda confirmed that this is also a challenge to the adoption and implementation of E-Health in Africa (Kiberu et al., 2017). According to the National Health Normative Standards Framework for Interoperability in E-Health, in South Africa, a lack of interoperability between the heterogeneous ICT systems prevents the investments made in E-Health systems from producing the desired network effect (CSIR & NDOH, 2014).

Adaptability: The ability of E-Health systems to adapt to their local context is a factor that has been reported in various E-Health studies. Closely related to adaptability is the interoperability of the E-Health system. The E-Health systems' capability to interface with other systems has been discussed in many E-Health studies that affect its implementation (Archer et al., 2011; Boonstra & Broekhuis, 2010; Gagnon et al., 2012; Goldstein et al., 2014).

Complexity: The complexity of E-Health systems affects their implementation. Complexity factors include, but are not limited to, difficulty in using system hardware and software; real-time inaccessibility; late response time of the systems; unexpected downtime; the unreliability of the system; a lack of user-friendliness of the systems; and lastly, the system's incompatibility with the existing workflow of healthcare organisations (Boonstra & Broekhuis, 2010; Gagnon et al., 2014; McGinn et al., 2011; Police et al., 2011). This factor has been linked to the inability of health professionals to use the implemented system due to their lack of skills and training (Boonstra & Broekhuis, 2010; Goldstein et al., 2014).

2.9.8 LEGISLATION, POLICY AND STANDARDS

Insufficient or the total absence of policies, legislation and liability may impede E-Health implementation at all levels of healthcare (Ksibi et al., 2023; Ross et al., 2016). This was confirmed in the developing country context, as a lack of clearly defined policy was recognised as a factor that obstructs the use of E-Health systems at public medical facilities in a southern African country (Furusa & Coleman, 2018).

More broadly, the need to provide established standards that guide E-Health implementation and use has also been highlighted by many other earlier studies as an external factor that could impact E-Health implementation (Archer et al., 2011; Boonstra & Broekhuis, 2010; Goldstein

et al., 2014; Police et al., 2011; Saliba et al., 2012). The existence of standards may reduce concerns of health professionals over patient data safety and professional liability (Benavides-Vaello et al., 2013; Jennett et al., 2004). The identified absence of suitable laws, governance systems, changing regulations and comprehensive policies in E-Health strategies is considered a problem for E-Health adopters (Al-Sharhan et al., 2019; Khalifehsoltani & Gerami, 2010; Omran et al., 2015). Hence, the call for unified standards indicates a genuine concern regarding the introduction of E-Health systems.

2.9.9 BUREAUCRACY

Health sectors have well-established systems of authority, and generally, they are not flexible. Hence, the Ministry of Health of a country determines the implementation and application of E-Health in hospitals in provinces or regions (Furusa & Coleman, 2018). However, the strict control that exists in the health sector has been identified to have a suppressing effect on the implementation of E-Health systems and technologies by public healthcare facilities (Furusa & Coleman, 2018). Bureaucracy has been recognised as an external element that impairs the adoption of E-Health in hospitals.

2.9.10 HETEROGENEITY

Heterogeneity of the healthcare environment is another key challenge to E-Health implementation (Al-Sharhan et al., 2019). The heterogeneity results from diverse management practices, technologies and resources across healthcare organisations. Heterogeneity is also related to the geographical location of the healthcare institutions; some institutions are located in rural areas while others are in urban areas (Al-Sharhan et al., 2019).

2.9.11 HUMAN FACTORS

Several factors related to people impact the adoption and use of E-Health (see **Figure 2.4**).

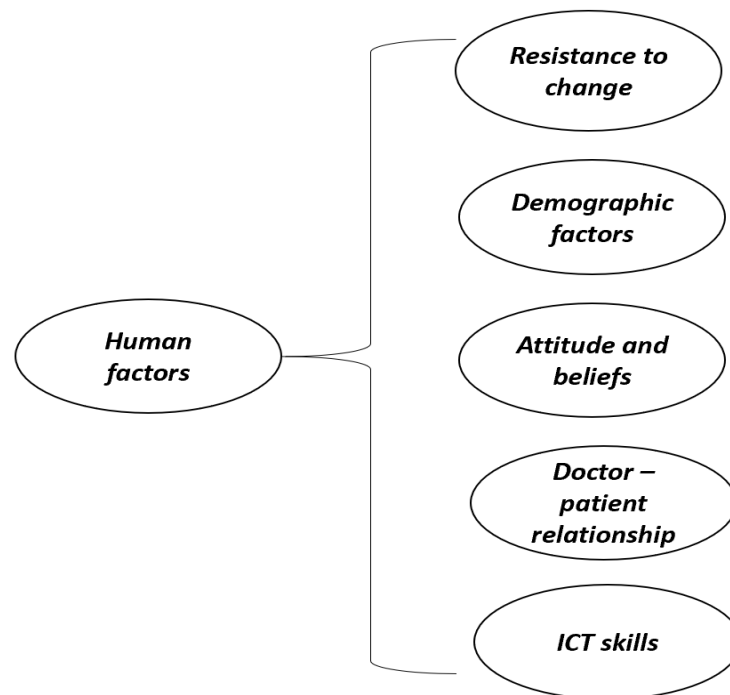


Figure 2.4: Human Factors Related to E-Health Implementation (Own source)

(1) **Resistance to change**: Technology adoption almost always changes the interactions, processes, and procedures in an organisation (Boonstra & Broekhuis, 2010; Furusa & Coleman, 2018). These disruptions can create unhappiness among healthcare professionals, and they will probably oppose the implementation of the systems.

(2) **Demographic factors**: Demographic factors, such as age, have been recognised as being factors influencing the digital divide. The use of ICT has been found to correlate directly with age (Furusa & Coleman, 2018; Ross et al., 2016). Similarly, age has been reported as a factor in the adoption and use of E-Health systems, as younger doctors are more comfortable using ICT than older doctors (Furusa & Coleman, 2018).

(3) **Attitudes and beliefs** have been identified as barriers to the implementation and acceptance of E-Health systems across all health domains (Boonstra & Broekhuis, 2010; Police et al., 2011; Ross et al., 2016). Attitude can affect and be affected by other people's attitudes. For instance, a negative attitude to implementing a new system by one or more members of a group can create resistance by other people as well. However, the attitude and beliefs of health

professionals may also be attributed to demographic factors such as education, age, nationality, sex and medical experiences (Ross et al., 2016);

(4) ***Doctor-patient relationship:*** Health professionals may be concerned that the implementation of E-Health systems could threaten and weaken the doctor-patient relationship (Ariens et al., 2017; Boonstra & Broekhuis, 2010; Furusa & Coleman, 2018; Gagnon et al., 2012; Kart et al., 2007). Some even refuse to approve the introduction of E-Health systems at the organisational level, as they believe these systems have detrimental effects on doctor-patient relationships (Ariens et al., 2017).

Another human factor is identified as minimal engagement, little or no engagement by end-users, leaders and other key stakeholders in the design, development and execution processes leading to the implementation of E-Health systems (Archer et al., 2011; Goldstein et al., 2014; McGinn et al., 2011; Moxey et al., 2010; Police et al., 2011; Saliba et al., 2012). This is often triggered by insufficiently visible management support.

(5) ***ICT skills:*** The human factors element of the ecosystem requires a special set of skills to enable people to search for, identify, understand and evaluate health or medical information from electronic resources and to be able to address health-related issues by applying the information. Healthcare professionals (current or future) and stakeholders who lack this type of skill are said to be E-Health illiterate (Ksibi et al., 2023; Norman & Skinner, 2006). The ICT skills of some nursing students need improvement to allow the successful implementation of E-Health (Tubaishat & Habiballah, 2016). The computer skills of healthcare professionals, their abilities, and experience with the use of ICT-related technologies have been cited in various other studies as factors that influence E-Health implementation (Boonstra & Broekhuis, 2010; Gagnon et al., 2012; Goldstein et al., 2014; Kilsdonk et al., 2011).

Inadequate or non-existent ICT skills, ignorance of E-Health benefits, and insufficient training have also been highlighted as factors that impact E-Health implementation (An Roinn Slainte Department of Health, 2013; Furusa & Coleman, 2018; Lam et al., 2016; Stellefson et al., 2011). Furusa and Coleman (2018) highlight a lack of ICT skills and knowledge of E-Health among medical doctors as factors that make the use of E-Health difficult. Hence, insufficient E-Health skills is a problem that affects both patients and medical professionals including students from different health specialties (Hanik & Stellefson, 2011).

2.9.12 SECURITY CHALLENGES

Ensuring the security and privacy of patient data is covered by essential ethical principles in the medical sector, and security and privacy is possibly the most frequently discussed problem in ICT ethics (Dinev et al., 2016; Ksibi et al., 2023; Triplett, 2024). Security threats have been highlighted as an important issue in E-Health systems, (Alzubi et al., 2021; Krishnamoorthy et al., 2023; Wang et al., 2013). The move towards E-Health has increased the security, privacy, and integrity concerns of E-Health stakeholders (Omran et al., 2015; Yüksel et al., 2017). Since ICT devices and related infrastructure are vulnerable to security breaches, this is a cause of resistance to their adoption in health institutions, as they are seen to weaken the security of patients' data (Omran et al., 2015).

Security challenges involve concern over patients' privacy, and threats made to hospital information records and E-Health systems, such as denial of service, as well as the consequences, such as wrong medical decisions made due to reliance on data that has been tampered with (Furusa & Coleman, 2018; Ksibi et al., 2023; Omran et al., 2015; Robinson, 2008; Triplett, 2024; Wang et al., 2013). Security challenges can relate to the protection of information used entirely within the organisation (information security) as well as the protection of information that is used beyond the confines of the organisation itself (Cybersecurity).

Security related to E-Health data and information remains a concern that affects E-Health implementation and use in public hospitals in developing nations (Al-Sharhan et al., 2019; Furusa & Coleman, 2018; Omran et al., 2015). The factor has the potential to compromise the achievements of E-Health if not adequately resolved (Furusa & Coleman, 2018). This factor is particularly important to healthcare stakeholders, and the successful introduction and continued use of E-Health depends on it.

South Africa is not an exception in this regard. Research has shown that South Africa's public hospitals are experiencing an overwhelming number of cyber threats arising from a combination of factors such as outdated computer systems and power failures (Chuma & Ngoepe, 2022). Other security challenges that South Africa public E-Health facilities face are phishing scams, a variety of other persistent cyber threats and Malware intrusion. The realisation of these has resulted in downtime, slow system performance, operational disruption and failure (Chuma, 2025).

Security and privacy concerns relating to patient data and E-Health systems raise issues of fear and trust in implementing and using E-Health, and this fear will continue to increase with emerging medical devices (Ksibi et al., 2023; Kovačić et al., 2022; Triplett, 2024). Stakeholders must trust that the healthcare data and information being captured, stored, processed, transmitted and used via E-Health systems and technologies are protected. Hence, if not addressed, security and privacy concerns regarding E-Health systems and infrastructure will continue to be a limitation to the implementation and usage of E-Health systems.

The issue of security challenges has allowed the focus area of this study to contribute to finding solutions. By focusing on cybersecurity as part of a broad security strategy, the research proposed the development of a CCSCF as a possible means of addressing security concerns, particularly cybersecurity concerns facing the E-Health implementation in public institutions.

2.10 CONCEPTUAL MAPPING TO RESEARCH GAP

Although **Figure 2.1** was used in Section 2.2 to depict how the literature review was approached, when looked at closely, it can also be seen to be a conceptual map for cybersecurity culture. Based on the challenges to E-Health implementation discussed in this chapter, the research focused attention on the associated security challenges, highlighting the issue of cybersecurity. This was essential given the alarming number of cyber threats targeting E-Health institutions. Based on this, Chapter 3 continues by reviewing literature that discusses cybersecurity in relation to E-Health to understand the underlying issues. From this review, security culture emerges as the central issue, with cybersecurity culture identified as a form of security culture.

Chapter 4 is the last literature review chapter (see **Figure 2.1**). This chapter presents a systematic literature review of cybersecurity culture as the focus of the study, and the constructs and factors used in the development of the proposed research framework are identified.

2.11 FOCUS ON SECURITY AS A CHALLENGE IN E-HEALTH

Based on the E-Health challenges discussed in **Section 2.9**, the urgent challenge that this study focused on was that of security. The significance of ICT-related security and the growing data security threats the E-Health sector faces should not be underestimated.

The importance of securing ICT systems and networks to protect information, people and assets of an organisation has been highlighted (Bakry, 2003). This becomes more urgent as private institutions' dependence on information networks increases, and the undesirable effects of

security challenges on organisations increase in scale and impact (Bakry, 2003; Howard, 1995). Examples of the effects include financial implications, embarrassment, competitive advantage problems and legal issues (Bakry, 2003; Howard, 1995). Reinforcing the security of ICT systems and networks has become essential with the move to electronic (e-based) operations, interactions and transactions across a wide range of sectors, including e-business, e-government, e-learning, E-Health, and e-assessment (Bakry & Bakry, 2005; Bakry, 2003; Bakry & Bakry, 2001).

There are four main dimensions of ICT security, which have been used to motivate the focus on security in this study. The security dimensions assist organisations to identify their main security fears and the measures that need to be applied to protect against them. According to Bakry (2003), these four dimensions are:

- **Object/s that need protection.** These are the institution's assets that need to be guarded. In the context of E-Health in this research, the assets that need protection are ICT systems, patients' data, information, and life, computer records, users, network lines, emails, and servers.
- **The undesired effect of security challenge.** In the E-Health context, the undesired effect would be a) the disclosure and theft of patients' data and information, for example, data breaches, and b) the patient's life, as a disruption of medical care through ransomware attacks can lead to patient death. These two consequences can also result in reputational damage to the E-Health institution.
- **Security challenge intention.** This highlights the purpose of the security incidents. Some of these incidents in E-Health institutions are accidental, due to a lack of information, skills, knowledge, or awareness. Other incidents are malicious acts by employees or outside parties for financial benefit or political gain.
- **Security measures that should be taken.** The Internet and interconnectedness of E-Health elements are discussed in **Section 2.3** call for security measures that allow Internet (cyber-based) attacks to be countered. Cybersecurity, defined in Chapter 1 as security protection in cyberspace, was selected as the security area or measure to be focused on in this study. Additionally, the acknowledgement that human-related challenges exist indicates that the proposed cybersecurity measures should accommodate human behavioural aspects. Hence, cybersecurity culture is the focus of this study.

2.12 IMPORTANCE OF E-HEALTH DATA AND INFORMATION

Data is considered an essential asset of any healthcare organisation as it contains information about E-Health stakeholders, for instance, patients' personal details, medical history, treatment information and health insurance information (Farzandipour et al., 2010; Murphy, 2015). The stakeholders' data is converted into information to assist in the making of informed decisions about patients' health and, hence, forms the basis of every electronic healthcare database system (Murphy, 2015).

Information stored in healthcare systems is considered to be amongst the most confidential of all personal information (Fernández-Alemán et al., 2013; Letsebe, 2017). Therefore, it is not surprising that data security features prominently as an ethical principle espoused by professionals in the sector. Unfortunately, personal medical information has monetary value and is targeted by cyber-criminals (Letsebe, 2017). Due to the sensitive nature of data and information stored in the healthcare system, threats made by cyber-criminals have serious implications for the healthcare organisation and patients (ITRC, 2019). For instance, stolen data can be used to commit several types of identity theft.

Healthcare organisations have become increasingly dependent on advanced Internet-based technologies for their operational activities. The ease and convenience of storing data and information in a digital form, conducting online transactions, claims submission and payment, as well as the easy exchange of patient information between healthcare institutions and patients are all major benefits (Cuenca, 2017; ITRC, 2019; Murphy, 2015; Rengamani et al., 2010). The ever-evolving technological advancements provide flexibility to healthcare organisations and patients, but they also create increasing security concerns as they expose healthcare institutions and stakeholders to new Internet security threats that call for strong cybersecurity (Cuenca, 2017; Farzandipour et al., 2010; Harries & Yellowless, 2013; ITRC, 2019; Koppel et al., 2015).

The healthcare industry has become an attractive target for cyber-criminals because of the sensitive nature of the personal medical information the industry contains (Sendelj & Ognianovic, 2022; Letsebe, 2017). Cyber-criminals with various motives constantly look for ways to breach healthcare security to gain access to valuable resources. Their intentions may be to reveal private medical records publicly, corrupt the data in healthcare critical systems and networks, or disrupt the functioning of those systems and networks, crash the computer systems of hospitals, or to gain financial profit for themselves. Reports of, or experience of, these types

of disruption create a sense of urgency and pressure healthcare institutions to strengthen their security systems, possibly adding to cybersecurity measures.

Threats to healthcare data and information are a significant challenge that affects numerous health sectors (Al-Sharhan et al., 2019; Appari & Johnson, 2010; Yüksel et al., 2017). This is partly because factors that encourage extensive adoption of E-Health can, at the same time, exacerbate security threats in the same environment. For example, the interconnectedness of medical devices and the interoperability of E-Health systems and components offer benefits but also have security weaknesses.

This integration of technologies allows for the fast and effortless sharing of patient health records and knowledge (Coventry & Branley, 2018; CSIR & NDOH, 2014). However, the exchange of patients' data between ICT systems, components, and stakeholders via the Internet exposes them to cyber threats and unauthorised access. Thus, the confidentiality, integrity and availability security goals of such systems can be violated. These potential weaknesses raise the need for cyber-based security in addition to existing security related to paper files and isolated systems. The security, privacy and integrity concerns of E-Health systems and information affect patients' willingness to disclose their health data, which can have life-threatening consequences (Yüksel et al., 2017).

Threats to E-Health information are a serious issue and should be approached seriously, as it could lead to many other problems like reduced data quality, loss of data, erosion of confidence in the healthcare systems, system failure, incorrect healthcare decisions due to erroneous medical data and violation of personal information.

Having discussed E-Health and identified cybersecurity as the focus of this study, Chapter 3 explores cybersecurity in E-Health. This will be followed by a discussion of cybersecurity culture in Chapter 4 to address the cybersecurity challenges in E-Health. The next section concludes the information presented in this chapter.

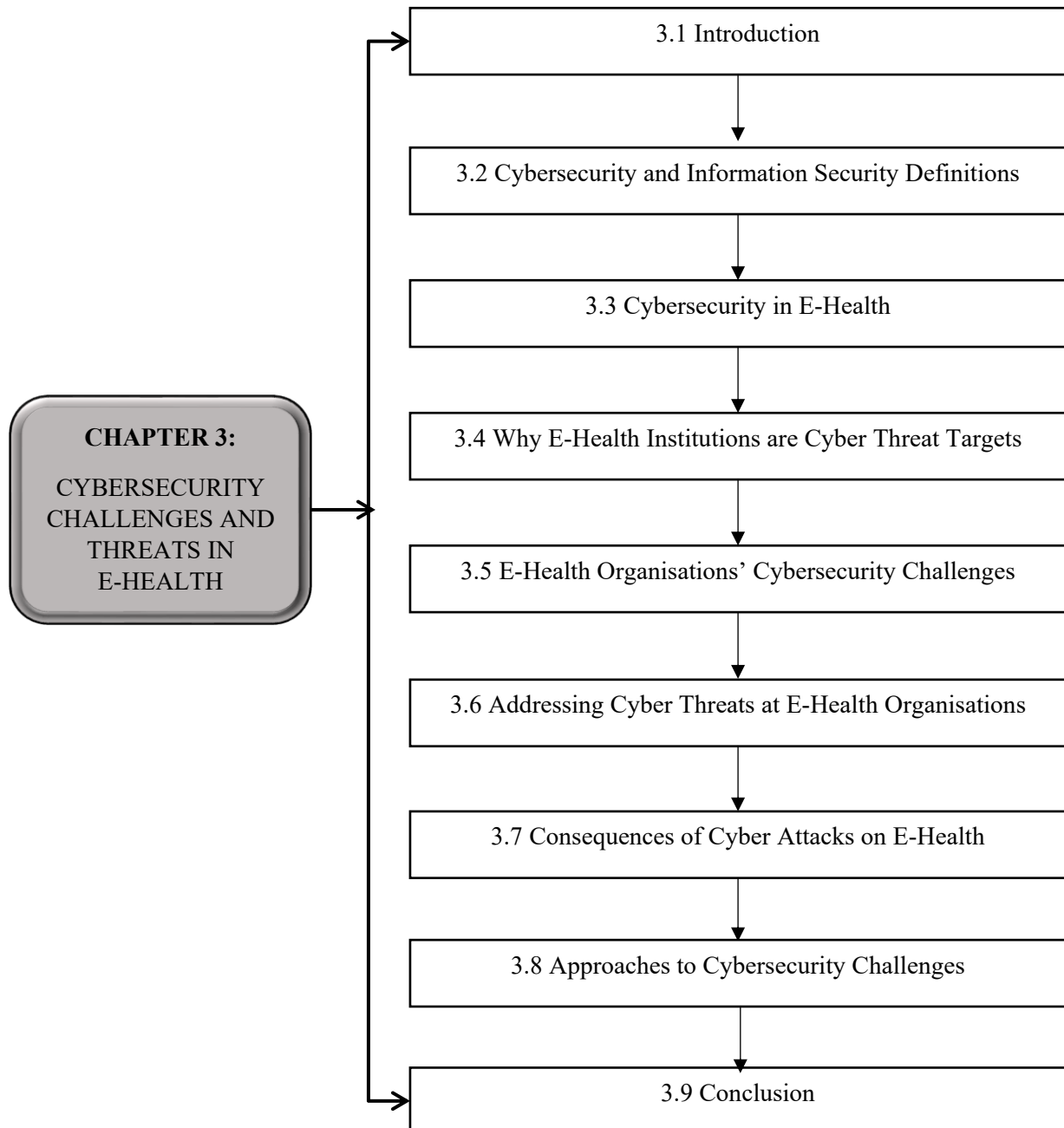
2.13 CONCLUSION

The term E-Health is used widely across the health sector by various stakeholders. Chapter 2 was used to assess the existing knowledge of E-Health. The chapter provided background for the concept of E-Health by looking at various definitions. Based on a critical assessment of these definitions, E-Health was redefined to include important aspects such as security, integration, interoperability and the Internet.

The chapter presented a model of the E-Health ecosystem using four elements, and classified E-Health stakeholders as internal, external and interface groups. Several ICT systems used for different specialised E-Health services were discussed. Differences between the public and private health sectors were presented. Finally, challenges that confront the implementation of E-Health were presented. The two main challenges that stood out were the security and human challenges, primarily because increasing numbers of cyber threat incidents affecting the sector have been reported and because of the role of humans in the security chain.

In the chapters that follow, the focus will shift to security and human challenges of E-Health implementation, particularly cyber-based security challenges commonly referred to as cybersecurity. This is because this research concentrates on building a CCSCF. This allows the researcher the opportunity to explore more cybersecurity threats in E-Health. Considering this, Chapter 3 explores the literature on cybersecurity in E-Health.

CHAPTER 3: CYBERSECURITY CHALLENGES IN E-HEALTH



3.1 INTRODUCTION

In discussing the most recent advances in E-Health, Chapter 2 explored the challenges confronting E-Health systems and the implementation thereof. It was evident from that discussion that the realisation of E-Health potential lies in how, and the degree to which, the challenges confronting E-Health systems are mitigated (Alvarez, 2002). The impact of these challenges can be measured in terms of the time needed to complete work and the extent of the deficit of skills, ICT infrastructure, funding, technical support and security, as well as cost considerations and people-related challenges.

To reduce E-Health implementation challenges, this research focuses on cybersecurity as it relates to E-Health. Chapter 3 defines and differentiates between information security and cybersecurity. Also in Chapter 3, cybersecurity challenges confronting E-Health institutions, the reasons why cyber-criminals target the sector, and the different kinds of cyber threats the industry faces are explored.

Research Sub-Question 1 (RSQ 1) will be answered at the end of Chapter 3.

Research Sub-Question 1 (RSQ 1): What cybersecurity threats and challenges confront E-Health institutions?

Chapter 3 starts by looking at definitions of information security and cybersecurity, their relationships, and differences (see **Section 3.2**). Cybersecurity in E-Health is discussed in **Section 3.3**. **Sections 3.4** and **3.5** explore why healthcare institutions are vulnerable to cyber-attacks and the challenges the institutions encounter in addressing cybersecurity. This provides an answer to **Research Sub-Question 1 (RSQ 1)**. Lastly, cybersecurity threats that confront E-Health institutions, the consequences of the threats, and the approaches to cybersecurity challenges are presented (see **Sections 3.6, 3.7** and **3.8**). The chapter is concluded in **Section 3.9**.

Before exploring other issues, it is essential to understand the concepts of cybersecurity and information security, the relationship between the terms, and how they are used in this study.

3.2 CYBERSECURITY AND INFORMATION SECURITY DEFINITIONS

Information is an essential asset of any organisation and, therefore, information protection has always been a priority in organisations. However, with technological advancements, a greater demand for information security has arisen. This is partly because new and advanced

technologies make generating, storing, and sharing information within and across organisations easier and therefore more organisations store more data.

Various terms such as “network security,” “information security,” “cybersecurity,” and “computer security” have been used to describe the processes and problems related to the protection of information and digital assets (Rout, 2015; Schatz et al., 2017). These terms have been used to describe security measures applied, focusing on different aspects of technology and systems, including the Internet, to protect digital information assets.

Initially, terms used to discuss the security of digital devices and the exchange of information assets were “computer security”, “IT security”, and “information security”. However, more recently, the emphasis has shifted to “ cybersecurity” (Schatz et al., 2017) or “ cybersecurity” and “Information security” (Rout, 2015).

These terminologies, particularly “cybersecurity” and “information security”, were sometimes used interchangeably but at other times were used differently (Astakhova, 2014; Rout, 2015; Gcaza & von Solms, 2017b; Ghernaouti-Hélie, 2009; Republic of Uganda, 2011). The varying use of terms is confusing, as different parties make different assumptions as to what the terms mean (Schatz et al., 2017). Considering this, it is essential to define these two terms clearly and highlight how they are related or are different to set a scene for how “cybersecurity” is viewed in this research.

3.2.1 INFORMATION SECURITY

The origin of information security dates back to computer security (Whitman & Mattord, 2012). The authors argue that computer security was used to secure physical locations, hardware, and software from threats during World War II.

Various authors and standards bodies have defined information security (see Table 3.1).

Table 3.1: Information Security Definitions

Author	Definition
(McConnell, 1994)	Information system security is concerned with the maintenance of three critical characteristics of information, which are Confidentiality, Integrity and Availability (CIA).
(Whitman & Mattord, 2012)	Information security is the protection of information and its essential elements (such as systems and hardware that use, store, and transmit the information) from being accessed, used, modified, disrupted or shared by unauthorised persons. This is done to achieve the three essential characteristics of information (CIA) plus additional characteristics of Accuracy, Authenticity, Utility and Possession.
(ISO/IEC, 2022)	Information security is the preservation of information confidentiality, integrity and availability (CIA). Information security is the protection of information assets from various threats to minimise risks and achieve competitive advantages for business.
(National Institute of Standards and Technology, 2018)	The protection of information and information systems from being accessed, used, disclosed, disrupted or modified to achieve: (a). Integrity, (b). Confidentiality, (c). Availability
(Paulsen & Byers, 2019)	Information security is “The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity and availability.”

According to ISO/IEC standards, information is an essential asset of any organisation. As such, it should be protected like other vital assets, hence the importance of information security, particularly in the current interconnected business environment. The standard indicates that information can take different forms: printed or paper-written, stored electronically, shared via post or electronic medium. Most importantly, information should be continuously and appropriately protected (ISO/IEC, 2022).

The three essential characteristics of information security, commonly known as the CIA triangle model and originating from the computer security industry standard, were expanded by Whitman and Mattord (2012) to include “Accuracy,” “Authenticity,” “Utility,” and “Possession.” The authors argued that characteristics of confidentiality, integrity and availability remain as important in the present age as they were in the time when the focus was on computer security. However, the CIA model has become insufficient in addressing security adequately in the constantly changing technological landscape (Whitman & Mattord, 2012).

The set of information security characteristics covers the whole range of security concerns in an automated environment. They apply to every organisation regardless of its philosophical outlook on information sharing (McConnell, 1994).

Three major points emerge clearly from the definitions. These are, that information is an essential asset of an organisation that needs security, that information security is not a technological product but a process, and that information security definitions focus on the critical aspects of information security (confidentiality, integrity, and availability (CIA) in addition to accuracy, authenticity, utility and possession).

The interconnectedness of infrastructural systems in the last couple of decades has presented new threats, and the widespread use of the term “cyber” in the industry has influenced the shift from the term “information security” to “cybersecurity” with a related broadening regarding matters of concern.

3.2.2 CYBERSECURITY

Attending to cybersecurity is a global concern and has been accepted as a shared responsibility across all levels of society (Hassan et al., 2017; Kortjan & von Solms, 2014). The concept has been wildly defined, with different authors, professions and nations defining it differently (Luijff et al., 2013). However, no harmonised and consistent definitions of cybersecurity exist (Baylon, 2014; Rout, 2015; Fischer, 2016; Luijff et al., 2013).

A review of definitions of cybersecurity was conducted by Luijff et al. (2013). The definition by Godwin III et al. (2014) was one that many countries could use to reach a common understanding of cybersecurity, but it is not widely accepted. The definition views cybersecurity as an aspect of cyberspace capable of resisting, responding to and recovering from intentional and unintentional cyber threats (Godwin III et al., 2014).

The review of the literature on cybersecurity by Luijff et al. (2013) focused on the national definitions. A subsequent review by Schatz et al. (2017) looked at definitions of the term obtained from professional, academic and governmental literature. The later review was conducted to identify definitions of cybersecurity and essential components of the definitions to provide a new and improved definition. The new definition that emerged from the Schatz et al. (2017) review and some selected definitions of cybersecurity are provided in Table 3.2

Table 3.2: Cybersecurity Definitions

Authors	Cybersecurity Definitions
(Schatz et al., 2017)	“The approach and actions associated with security risk management processes followed by organisations and states to protect confidentiality, integrity, and availability of data and assets used in cyberspace. The concept includes guidelines, policies, and collections of safeguards, technologies, tools, and training to provide the best protection for the state of the cyber environment and its users.”
(International Telecommunication Union (ITU), 2008b).	“Collection of tools, policies, security, concepts, safeguards, risks management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, and organisation and user assets. Organisation and user assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties (Availability, integrity, which may include authenticity and non-repudiation, and confidentiality) of the organisation and user's assets against relevant security risks in the cyber environment.”
(State Security Agency, 2015)	In the context of South Africa National Cybersecurity Policy Framework (NCPF), cybersecurity is defined as “A practice of making the networks that constitute cyberspace secure against intrusions, maintaining confidentiality, availability, and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them.”
(von Solms & van Niekerk, 2013)	Cybersecurity is defined as “the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, which are vulnerable to attacks originating in cyberspace.”
(von Solms & von Solms, 2018)	Cybersecurity is “that part of information security which specifically focuses on protecting the confidentiality, integrity, and availability (CIA) of digital information assets against any threats, which may arise from such assets being compromised via (using) the Internet .”
(ISO/IEC, 2012, 2023)	Cybersecurity is the “protection and preservation of confidentiality, integrity, and availability (CIA) of information assist in the cyberspace.”
(ISACA, 2015)	Cybersecurity is “the protection of information assets by addressing threats to information processed, stored, and transported by interconnected information systems.” Any security that intends to protect the organisation and individuals from intentional or unintentional threats and their consequences.

Authors	Cybersecurity Definitions
(Paulsen & Byers, 2019)	Cybersecurity is the “ability to protect or defend the use of cyberspace from cyber-attacks.”
(Rout, 2015; Walls et al., 2013)	"Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack adversaries" “Cybersecurity is a superset of the practices embodied in ICT security, information security, operational technology (OT) security and offensive security”

The cybersecurity definitions in Table 3.2 were selected explicitly for this research as they are comprehensive and inclusive. An essential factor to note is that information resources or assets were not viewed as the only national, organisational, or individual assets that need protection; other assets (ICT technologies, cyberspace itself, cyberspace users, the interest of society at large and the critical national infrastructure) were explicitly included. For example, some authors argued that for assets to be protected, cybersecurity should include anyone and anything reachable through cyberspace (von Solms & van Niekerk, 2013). These definitions accommodate the multiple layers of security needed to protect an organisation’s operation. The layers of security include physical, personal, operational, communications, networks and information security (Whitman & Mattord, 2012).

The conclusion drawn from these definitions was the importance of cybersecurity in securing the assets and operations of E-Health organisations. E-Health should consider cybersecurity vital for protecting all its assets, including medical devices, ICT systems, information, people (patients, doctors and other healthcare workers), and the cyberspace environment itself.

The definitions suggested by researchers and national committees indicate that cybersecurity is essential and that all parties (countries, businesses, and individuals), including the health sectors that notably lag in cybersecurity, should intensify their adherence to cybersecurity measures. Insufficient cybersecurity within the healthcare sector, including strengthening the security of medical devices, is a growing concern, exposing the sector to cyber-attacks. It has resulted in inadequate safeguards for the confidentiality and integrity of healthcare information and data due to security systems' weaknesses (Coronado & Wong, 2014; Coventry & Branley, 2018; Sendelj & Ognianovic, 2022).

3.2.3 COMPUTER SECURITY

Computer security falls outside the scope of this study. However, a limited number of definitions of the concept are highlighted because of the link to information security.

Some researchers consider computer security, also known as ICT security, to be synonymous with information security. For others, computer security is regarded as a broad area of information security covering topics such as network security and data security (Whitman & Mattord, 2012). Table 3.3 provides definitions of computer security.

Table 3.3: Computer Security Definitions

Authors	Computer Definitions
(Rout, 2015)	“Computer security is a discipline applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, in addition to the Internet.” Computer security includes physical protection of computer equipment from theft and information security to preserve the data contained in the computer equipment.
(Kissel, 2011)	Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.

Computer security involves processes and tools to secure digital equipment, information and services from non-malicious or unauthorised access, change or destruction (Rout, 2015). Computer security, like information security and cybersecurity, is a term used to describe the protection of information assets. However, as time changes and technology evolves, the demand for security also advances (ISACA, 2015). As previously stated in **Section 3.2.1**, the confidentiality, integrity, and availability (CIA) goals commonly known as the CIA triangle, adopted in current securities dates back to the industry standard for computer security in place since the development of the mainframe (Whitman & Mattord, 2012).

3.2.4 RELATIONSHIP AND DIFFERENCES BETWEEN INFORMATION SECURITY AND CYBERSECURITY

Information security and cybersecurity are related in various ways, and some authors use the terms interchangeably. Although the terms have many commonalities, significant distinctions exist between them. Table 3.4 is used to summarise these.

Table 3.4: Relationship and Differences Between Information Security and Cybersecurity

Factor	Cybersecurity and Information Security
Relationship	
Layers of security	According to Whitman and Mattord (2012), the security layers needed to protect an organisation's operation include physical, personal, operations, communications, network and information security. Both cybersecurity and information security accommodate these securities.
Process, technology, and people	Also emerged from the definitions was that neither information security nor cybersecurity are technological products, but they are processes through which security is achieved in cyberspace or across the organisation or nation. In both definitions, processes are followed to use technological devices in addition to policies and strategies to protect the organisation, its people, and other assets.
Information assets	Both information security and cybersecurity are critical to securing essential assets. The exploration of various definitions provides evidence that an 'information asset' is not the only significant asset that needs protection by the nation, organisation or individuals during information security or cybersecurity processes; other essential assets also need protection. Information security also protects other essential components of information, such as people and technology. Likewise, cybersecurity also protects other critical digital assets such as the cyber environment (cyberspace), users and organisation assets like ICT technologies and infrastructure (cybersecurity protects everything in cyberspace).
Security concerns or security goals (CIA)	Information security and cybersecurity focus on protecting a range of security goals, which are Confidentiality, Integrity, and Availability (CIA) in an automated environment.
Differences	
Scope or context of security practices provided	The most significant difference that emerged from the definitions of information security and cybersecurity lies in the scope of the security practices provided. Information security deals with the protection of information within the organisational context. Information security focuses on the physical and electronic location of the information. Moreover, information security has narrowly defined security practices, while cybersecurity includes a broad range of practices and tools that are closely related to information and operational technology security. Cybersecurity is a broader security context that provides salutation with greater scope than information security. Cybersecurity protects information generated, stored, used and exchanged in cyberspace. It involves the protection of information beyond the organisational context.

Format/ form of information	Information security protects information regardless of its format. The information can be manual or paper-based documents, digital documents, intellectual documents in people's minds, and verbal or visual communication-based information or documents. However, since cyberspace is a computer-generated universe created by connecting networked systems and associated electronics equipped with computer powers via the Internet, only digital information is protected via cybersecurity, and it is generated, stored, and exchanged electronically via Internet working technologies, information systems and network systems.

It is evident, based on various definitions, that some authors and cybersecurity strategic documents view cybersecurity to mean the same thing as information security, and these sources have used the terms interchangeably (Astakhova, 2014; Ghernaouti-Hélie, 2009; Republic of Uganda, 2011). With this view, cybersecurity is defined directly as information security (ISO/IEC, 2022, 2023).

A somewhat different view is that cybersecurity is related to but is not identical to information security (U.S. Government Publishing Office, 2006).

The view that cybersecurity is a subset or component of information security was also encountered (Barzilay, 2013; ISACA, 2015; Stubley, 2013; von Solms & von Solms, 2018). This is partly based on the view that both securities protect information assets from a whole range of security concerns (CIA) in an automated environment.

However, several researchers defined cybersecurity as an extension of information security; hence, it includes information security, but additional aspects are included (Reid & van Niekerk, 2014a; von Solms & van Niekerk, 2013). Cybersecurity includes ICT security, operational security, nation-state-sponsored attacks and advanced persistent threats (APTs) (ISACA, 2015). Consequently, cybersecurity is seen as a superset of practices that embody other securities like information security, ICT security, operational security, and offensive security (Rout, 2015; Walls et al., 2013).

This view, where cybersecurity is seen as inclusive of information security, is becoming more common in the changing digital landscape with its evolving challenges. An example of a nation taking cybersecurity seriously can be seen in the Uganda National Information Security Strategy (Republic of Uganda, 2011). The early version of the strategy focused on information security and stressed the importance of protecting data and information systems inside organisations (Republic of Uganda, 2011). This early document defined information security as the same thing as cybersecurity. However, the country has shifted priorities by redesigning

the strategy to become a National Cybersecurity Strategy, accommodating the broader concerns of cybersecurity (Republic of Uganda, 2022). In this regard, information security becomes part of broader cybersecurity initiatives which address sophisticated and evolving cyber-related threats.

The synonymous use of the terms cybersecurity and information security brings confusion in research communities and among security practitioners and customers. It obscures critical differences between the two and extends this vagueness to the concepts of cybersecurity culture and information culture (Rout, 2015; Gcaza et al., 2017b; Walls et al., 2013).

Professional associations and researchers indicate that although the terms are often used interchangeably by different groups, profound distinctions do exist between them (Gcaza & von Solms, 2017b; Huang & Pearlson, 2019; ISACA, 2015; von Solms & van Niekerk, 2013). Reid and van Niekerk (2014a) argue that the essential difference is that information security focuses primarily on business continuity, and hence its main aim is to reduce the effects of security breaches and limit damage to organisations' business interests. The primary concern of information security is protecting information within an organisational context.

However, bearing in mind that cyberspace allows information to be shared beyond the organisation's borders, cybersecurity should include security beyond the organisation's borders (Reid & van Niekerk, 2014a). The two concepts also have implications with respect to culture, with the only difference being in the context in which they are applied (Da Veiga, 2019).

Since significant differences exist between information security and cybersecurity, this study assists in preventing academic confusion. The study focuses on cybersecurity, and holds the view that cybersecurity is inclusive of information security but includes aspects beyond those considered by information security. This is a broad view that extends beyond the organisational context. Therefore, cybersecurity is viewed as a superset of information security.

A similar view was applied to information security culture and cybersecurity culture in this research. Cybersecurity culture has been described as an ill-defined concept with components that are not fully defined or demarcated, and knowledge about the domain that is not bounded (Gcaza et al., 2017; Gcaza & von Solms, 2017b; Reid & van Niekerk, 2014b). Therefore, while the study described in this thesis benefited from the work of earlier researchers, it drew from both the thoroughly researched domains of security culture, a subculture of organisational culture, and information security culture.

Since information security is viewed in this research as a subset of cybersecurity, the argument is that the essential purpose of information security is to preserve the three security goals of CIA (ISO/IEC, 2022; McConnell, 1994; Whitman & Mattord, 2012). This also holds for cybersecurity (ISACA, 2015). These goals are the cybersecurity triad (ISACA, 2015).

Cybersecurity deals with protecting the Confidentiality, Integrity, and Availability of information in the cyber environment. Similarly, information security is the protection of confidentiality, integrity and availability of information, but here it is irrespective of its format and location in the organisation. However, the main difference is that cybersecurity protects information generated, stored, exchanged and used in the organisation and its cyberspace (including outside the borders of the organisation). In contrast, information security protects information that is within the organisation.

In addition to protecting information assets, information security protects other essential components of information, like the people who use the information, the technology (hardware, software, network and infrastructures) that stores and transmits the data, and the organisation's processes and procedures. Cybersecurity is extended to also protect everything within cyberspace (ISACA, 2015). This supports the argument that cybersecurity equates to securing cyberspace (Rout, 2015). All these forms of protection aim to achieve the security goals of CIA.

In this research, the notion of cybersecurity is viewed not only as the protection of information in cyberspace, but also the protection of other assets belonging to the organisation and user (individuals in cyberspace, services, operations, and the cyberspace environment itself). It protects everything that has been processed, stored or transmitted via the system, working together with the Internet (ISACA, 2015). Therefore, comprehensive definitions of cybersecurity are adopted in this research. The definition adopted described cybersecurity as a broad security solution with a much greater scope than organisational information security.

Therefore, approaching cybersecurity culture from an E-Health perspective as the focus of this research, the concept has not been restricted or seen as equal to the information security culture, which only focuses on changing behaviour to adhere to an information security policy. Instead, the focus is on policy adherence and personal involvement in organisational cyber safety as recommended by Huang and Pearlson (2019).

Section 3.3 presents cybersecurity objectives in E-Health institutions.

3.3 CYBERSECURITY IN E-HEALTH

It is important to reiterate that, according to the Fundamental Study Guide of the ISACA (2015), the three key concepts that help with a better understanding of cybersecurity and the protection of cyber assets are confidentiality, integrity, and availability (CIA). These are the hallmarks of sound security (Pfleeger et al., 2015). They should be used to build security policies (ISACA, 2015) including those for E-Health.

Cybersecurity, as applied to E-Health, aims to protect the CIA of healthcare data and information. It follows that one of the major threats to healthcare information is anything that compromises the integrity and availability of medical data (Letsebe, 2017). **Figure 3.1** is used to articulate the importance of the cybersecurity goals in safeguarding healthcare data and information.

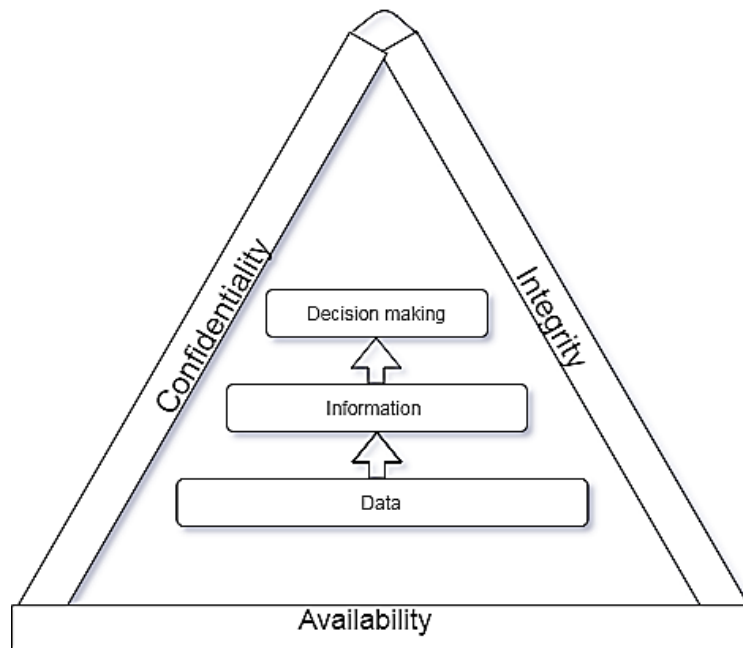


Figure 3.1: Security Goals of E-Health Data and Information

Section 2.12 highlighted the importance of healthcare data and information. Health data is converted into information which is then used by institutions, including healthcare and non-healthcare, such as the government, to make both medical and non-medical, long and short-term decisions (Haas et al., 2011). The data and information are safeguarded by the three fundamental cybersecurity goals of CIA, as they are essential assets for E-Health systems operations (Haas et al., 2011).

Confidentiality is the protection of cyber assets from unauthorised access and disclosure. The level of confidentiality should be guided by the sensitivity of the information (based on the type of information) and the value of the information in a particular time frame (ISACA, 2015). Healthcare systems contain highly sensitive information, such as personal information, medical records and health insurance information, so confidentiality is needed (Haas et al., 2011). Protecting confidentiality ensures that a patient's sensitive information does not end up in the wrong hands (Martin et al., 2017).

Integrity is the protection of cyber assets from unauthorised changes (ISACA, 2015). It is essential to ensure the accuracy and trustworthiness of healthcare data and information (Haas et al., 2011). Integrity is important, as the wrong medical decisions and treatment based on information derived from erroneous medical data might be life-threatening (Martin et al., 2017). Violations of integrity can also lead to successful attacks, making the medical systems unavailable or compromising the confidentiality of healthcare data.

Availability ensures timely and reliable access to information and ICT systems (ISACA, 2015). It ensures consistently reliable access to healthcare data and the critical ICT systems that process and store the data, as well as to medical devices used to monitor or treat patients (Martin et al., 2017). Interruptions in the availability of critical healthcare assets can have serious consequences, including loss of life. The availability of medical information is also essential as it is necessary for making accurate, adequate and timely medical decisions (Haas et al., 2011). Maintaining availability ensures that hackers or malicious insiders cannot delete all copies of healthcare records.

Considering all these, a threat to the security of data and information in E-Health organisations should be taken seriously, because it could have further consequences linked to the security goals. For instance, incorrect healthcare decisions due to erroneous medical data and poor data quality (integrity), loss of data and system failure (availability), and violation of personal information (confidentiality) will lead to loss of confidence in the healthcare systems.

Having discussed the aim of cybersecurity in E-Health, **Section 3.4** presents reasons why healthcare institutions are vulnerable to cybersecurity threats.

3.4 WHY ARE E-HEALTH ORGANISATIONS TARGETS FOR CYBER THREATS?

Healthcare organisations have become a favoured target for cyber-criminals (Jalali & Kaiser, 2018). Information from multiple sources has led to the firm conclusion that cyber-criminals

use threats, including ransomware and data breaches, to take advantage of the vulnerabilities of healthcare medical devices as a way to attack the industry, thus making them highly desirable targets for cyber-attacks (Aldosari, 2025; Kruse et al., 2017; Sendelj & Ognianovic, 2022). E-Health vulnerabilities are weaknesses in the overall operation and implementation of E-Health. To limit security faults and protect healthcare ICT systems from cyber threats that attack data and information, healthcare leaders and security professionals need to understand and effectively manage the aspects of healthcare systems that lead to vulnerabilities. These must be identified and understood (Cuenca, 2017). This is summarised in **Figure 3.2**.

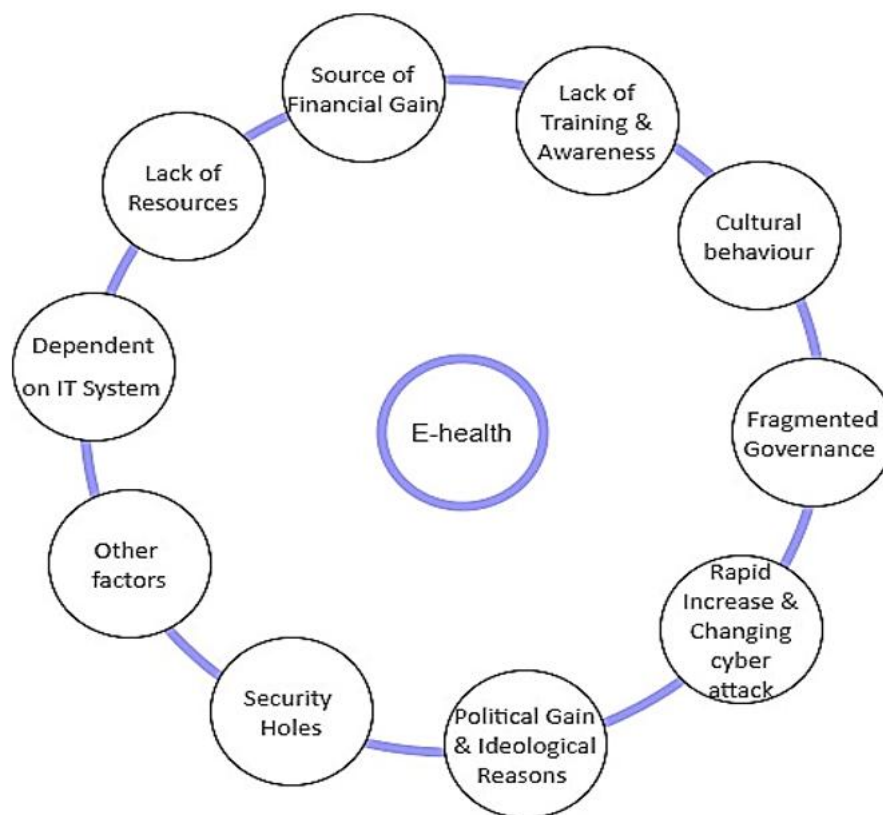


Figure 3.2: Reasons Healthcare Organisations are Targeted by Cyber-Criminals (Own source)

3.4.1 DEPENDANCE ON ICT SYSTEMS AND INFRASTRUCTURE

Healthcare organisations have become increasingly dependent on computer technology to provide up-to-date information for critical patient care. This makes healthcare organisations relatively easy targets for cyber-criminals (Spence et al., 2017). Hospitals are the perfect mark for ransomware attacks, as they depend on updated information stored in ICT systems like EMRs to provide critical care to patients (Zetter, 2016).

E-Health is totally dependent on technological infrastructure; this creates a sense of urgency for healthcare institutions when they are hit by cyber-attacks that make the systems unavailable. As a result, some healthcare institutions are prepared to pay ransom when attacked by ransomware or MEDJACK - the encrypted information or medical devices are critically needed during serious patient care (Zetter, 2016). Dependence on ICT systems and the fact that ICT infrastructure needs to run constantly to support healthcare services means that these institutions are particularly exposed to and harmed by cyber-criminals (Alder, 2016; Koppel et al., 2015).

Disruption of systems or networks when providing patients with medical care is closely related to the healthcare provider's dependence on ICT. Cyber-criminals frequently target healthcare organisations as they know that their core business is to provide critical medical care. Any disruption in the provision of these services due to cyber-attacks, such as denial of medical service to patients and the resulting lack of access to updated medical records for patient treatment, increases many other risks.

The disruption experienced by England's NHS due to the global WannaCry ransomware attack in 2017 and the attacks directed at other medical institutions (see Table 3.9) are evidence of just how dependent healthcare institutions have become on ICT systems. This is a strong justification for the need for continuous security improvement across the healthcare sector (Smart, 2018).

3.4.2 LACK OF RESOURCES

Healthcare organisations do not invest sufficient budget in ICT infrastructures compared with other sectors. Many of these organisations spend less than 2% of their annual budget on ICT compared to organisations in other sectors that spend between 4% and 10% on ICT (Martin et al., 2017). Morgan (2020a) indicates that healthcare organisations spent most of their budgets on research, advanced treatment and patient care.

Inappropriate funding for cybersecurity can lead to data breaches. Less than 47% of healthcare organisations spend 3% of their ICT budget on security (Scott, 2015). Lack of finance can lead to the sector operating with outdated and unsupported legacy systems (Martin et al., 2017).

Furthermore, cybersecurity experts are in short supply, and the limited ICT budget allocation by the sector makes it difficult for healthcare organisations to afford the services of cybersecurity experts (Martin et al., 2017). The limited staff resourcing is not limited to

cybersecurity experts; other ICT staff are also in short supply, contributing to increased cyber-attacks targeting healthcare institutions (Morgan, 2020a).

3.4.3 DATA AS A VALUABLE SOURCE FOR FINANCIAL GAIN

The healthcare sector is attractive to cyber-criminals because it is a rich source of valuable and attractive data for them (Martin et al., 2017). The information is extremely useful to legitimate users as well, but non-functioning systems or inaccessible information affects patients' lives and well-being (e-Estonia, 2018). Hence, medical data is considerably more important than other data, and the financial gain obtained by stealing medical data is the main reason healthcare is targeted by cyber-attacks (Coventry & Branley, 2018). Cyber-criminals can also use personal information, like insurance credentials and social security numbers, to obtain medical services, to use in other organised crime, to dispense medications for sale on the dark web, and even to open a bank account. Even more profitable strategies are because medical practices and hospitals are prepared to pay very high ransoms to regain access to essential medical data and this adds to the reasons for targeting healthcare institutions (Morgan, 2020a).

The multiple potential uses of medical data explain why medical data is regarded as a cyber-criminal's "holy grail" (Wagstaff, 2015). The study by Jalali and Kaiser (2018) identified financial gain, due to the high value associated with medical data, as one of three reasons healthcare is specifically targeted. The fact that healthcare institutions are a source of valuable data that can be stolen for financial gain cannot be emphasised enough.

3.4.4 LACK OF TRAINING AND AWARENESS OF SECURITY ISSUES

Lack of employee training focusing on security awareness, and the lack of attention paid to cybersecurity in general (as is needed to comply with HIPAA federal requirements) are also factors identified as making healthcare providers targets to cyber threats (Zetter, 2016). Awareness of cybercrime has been low, making healthcare providers unnecessarily vulnerable to cyber-attacks (Mello, 2017).

Ahmed et al. (2019) indicate that awareness training is an essential security measure because people can easily be manipulated. Therefore, to improve the security of healthcare data and decrease the vulnerability of the people involved as victims of cyber-criminals, security awareness training must be given attention. Achieving ongoing improvement in security knowledge and the associated skills of employees of healthcare organisations through

organisational training and awareness is one of the best ways of creating a defence against cyber-attacks, and an appropriate investment is essential (Sendelj & Ognianovic, 2022).

3.4.5 SECURITY ‘HOLES’

In addition to technological dependence, Spence et al. (2017) identified security ‘holes’ as being weaknesses in a system resulting from an ICT system design flaw or coding error. This is, therefore, another factor that makes healthcare providers a target of cyber threats. These flaws can also be attributed to a weak security culture that exists in many health institutions. This is often due to the unduly narrow focus of those in the healthcare environment, including healthcare professionals, who seek to provide excellent patient treatment but do not recognise security as also being critical. A weak security culture can result from poor or no security awareness, non-compliance with security practices, and a misperception of security responsibility as being the sole mandate of the ICT department. This attitude compromises security measures like password protection in the institution (Ahmed et al., 2019). However, such a lax security culture arises not only from individual actions but also from inappropriate organisational norms where security is considered not to be at the core of the institutional identity. Historically weak security attitudes or a weak security culture can be taken advantage of by hackers to attack health institutions and cause havoc (Coventry & Branley, 2018; Martin et al., 2017).

Many medical devices were not initially designed with security in mind but are now being connected to the Internet to allow for easy data sharing between medical staff to improve patient care. This creates a new security vulnerability that hackers can exploit to access healthcare institutions’ data (Ahmed et al., 2019). Recent research has highlighted that the vulnerability of medical ICT systems exposes them as targets to cyber-attacks because these devices have been developed to serve a specific healthcare purpose and were not made with cybersecurity concerns in mind (Sendelj & Ognianovic, 2022). Addressing security ‘holes’ in healthcare entails employing the services of security experts, particularly cybersecurity professionals, and ensuring stakeholders' awareness training.

3.4.6 RAPID INCREASE OF AND CHANGING CYBER-ATTACK METHODS

The rapid increase and evolving nature of cyber-attacks present a significant challenge to public E-Health institutions, particularly as healthcare systems become increasingly reliant on

electronic platforms for service delivery. Cyber-attackers continue to shift tactics, adopting more sophisticated and cleverly targeted methods aimed at exploiting vulnerabilities within HISs (Badawi, 2024). The rise of ransomware demands remains one of the most pervasive threats, placing both service continuity and patient safety at risk (Neprash et al., 2022). Furthermore, the integration of emerging technologies, such as Internet of Medical Things (IoMT) devices and cloud-based storage, has expanded the range of healthcare attack possibilities (Ksibi et al., 2023).

These technologies, while improving access to care, often lack robust built-in security controls and are frequently deployed more rapidly than the security frameworks can adapt. The increasingly dynamic nature of cyber threats has also been accelerated by the rise of generative AI-enabled attacks (Tahenni et al., 2025). The rapid evolution of cyber-attacks contributes directly to a heightened cybersecurity risk in the public E-Health environment, demanding improved preparedness, policy reforms and ongoing solutions aligned to international standards. Without continuous adaptation, public E-Health institutions remain highly vulnerable to evolving cyber threats that compromise data security, undermine trust, and threaten patient well-being.

3.4.7 FRAGMENTED GOVERNANCE

Fragmented governance is a contributing factor to cybersecurity attacks on E-Health institutions, particularly where the responsibility for information security, technology management, and clinical service delivery is distributed across multiple departments and administrative levels (Martin et al., 2017). In addition, cybersecurity governance in some health systems lacks clear ownership, resulting in overlaps, gaps and inconsistencies in policy implementation. Policies are often adopted at the national or ministerial level but are not effectively operationalised at facility level. Furthermore, public hospitals commonly rely on decentralised IT structures.

This lack of centralised oversight impedes the enforcement of standardised cybersecurity practices. Fragmented governance can also affect incident response coordination, where delays in decision-making and reporting can worsen the impact of an attack. Furthermore, limited cross-sector collaboration between governmental agencies, private cybersecurity firms, and telecommunications providers reduces access to real-time threat intelligence, leaving institutions slow to detect emerging threats. To implement E-Health successfully, nations need

to act effectively and efficiently and recognise the dynamics of governance structures to attain a proper balance between centralisation and decentralisation.

3.4.8 CULTURAL BEHAVIOUR

Healthcare institutions are known for their primary culture of patient-centeredness (also known as the patient-first culture). This implies that organisational decisions, procedures, and actions are centred around patient treatment, thereby meeting the expectations, experiences, principles, and preferences of their patients. This is considered to be one of the main reasons that healthcare institutions are targeted (Martin et al., 2017). The challenge with this mindset is that healthcare decision makers tend to take a back seat with regards to security, and this can result in serious consequences should a security incident occur. The cultural prioritisation of patient care over cybersecurity practices results in weak security behaviours among the staff as a whole, making healthcare a “soft target” compared to that of other sectors with more mature cybersecurity cultures (Ahmed et al., 2019; Coventry & Branley, 2018; Martin et al., 2017).

Similarly, the healthcare culture of ‘do no harm’ (which may be interpreted as ‘do what we do best, which is save lives’), which is the central tenet of healthcare providers, has also been identified as a reason why healthcare organisations are the key target of cyber-attacks. (CISCO, 2016; Mello, 2017). Hence, the industry lags behind others in cyber resilience, and ICT spending among others (Jalali & Kaiser, 2018). Together, this helps explain the rapid increase in attacks.

3.4.9 OTHER FACTORS

The changing nature of cyber threats has been identified as an additional factor. More recent sources argue that healthcare organisations are vulnerable because they battle to keep up with modern technology (continued use of outdated technology) and the ever-changing cybersecurity threats (Sendelj & Ognianovic, 2022). Linked to this, the healthcare sector has too few and outdated security protocols (Morgan, 2020a).

Another problem is that healthcare organisations are sometimes targeted because of political views and the affirmation that activist attackers might achieve by stealing the medical data; there is even the potential to use medical devices for cyberwarfare (Coventry & Branley, 2018). Examples of medical cyberwarfare include a nation disrupting the healthcare operation of

another country through denial of access to medical systems or databases, or targeting the medical devices of individuals.

Closely related to cyber warfare is the ideological or terrorist motive of targeting healthcare organisations to disrupt the citizens' feelings of safety and induce fear (Jalali & Kaiser, 2018). Despite the ever improving cybersecurity countermeasures, ideological reasons and financial gain remain factors that expose healthcare institutions to cyber-attacks (Jalali & Kaiser, 2018).

The absence of a strong security culture, for example, a lack of cybersecurity awareness and training, is considered a major reason that E-Health sectors are likely to continue to be attacked (Ahmed et al., 2019; Coventry & Branley, 2018; Martin et al., 2017). Table 3.5 summarises other reasons healthcare institutions are vulnerable to cyber threats.

Table 3.5: Reasons Why Healthcare Institutions are Targeted

Paper and/or Authors	Reason
(Coventry & Branley, 2018)	Political gain
(Jalali & Kaiser, 2018)	Ideological reasons, such as cyber warfare and terrorism
(Martin et al., 2017)	Healthcare is a soft target Inability to handle modern technologies and security protocols
(Jalali & Kaiser, 2018)	The industry lags behind other industries.

Given the reasons why healthcare organisations are targeted, **Section 3.5** expands on the cybersecurity challenges faced by healthcare institutions.

3.5 E-HEALTH ORGANISATIONS' CYBERSECURITY CHALLENGES

Cyber threats and attacks affect healthcare organisations despite their different contexts and geographical conditions and descriptions of attack incidents highlight common cybersecurity challenges (Ghafur et al., 2019). This section identifies cybersecurity challenges commonly affecting organisations with electronic (e) based implementations such as E-Health.

3.5.1 COMPLEXITIES OF HEALTHCARE ORGANISATIONS

The healthcare industry lags behind others in securing its essential assets (data and information, people, devices, etc.) and processes. However, the complex nature of healthcare organisations

makes cybersecurity even more challenging. This complexity is a result of the following characteristics of healthcare organisations:

1) Sophisticated technology: The healthcare environment is filled with a great deal of different kinds of technology, making it difficult for them to manage the wide variety of technological systems and services, from maintaining legacy ICT systems to connecting medical devices (Jalali & Kaiser, 2018; Riazul Islam et al., 2015).

2) Internal organisational complexity: In addition to dealing with complex functions related to finance, IT and human resources, they have highly specialised departments like paediatrics, cardiology and radiology with different equipment, workflows, specialised employees with different training and labour force, all of which need support (Jalali & Kaiser, 2018; Smet, 2002).

3) Regulatory pressures: Beyond abiding by the general cybersecurity regulations set by the government, healthcare organisations must adhere to additional specific data protection laws due to the sensitivity of healthcare information (Jalali & Kaiser, 2018; Brookman, 2015).

4) Patient-centred care: While generating profit, at least in the private sector, the first mission of healthcare institutions is to care for their patients (Institute of Medicine, 2001).

These complex characteristics impact the ability of healthcare organisations to maintain robust cybersecurity (Jalali & Kaiser, 2018). This finding aligns with those of the Cybersecurity Fundamentals Study Guide by ISACA (2015), which identified the level of ICT complexity as one of many significant factors that impact cybersecurity in general.

3.5.2 TECHNOLOGICAL ADVANCEMENT

The published literature has identified changing technology as a driver contributing to the healthcare sector's exposure to cyber threats (Kruse et al., 2017; Ahmad et al., 2021). There is a concern that new technologies are emerging fast, and the sector faces pressure to adopt them (Vilakazi & Adebisin, 2023; Petracca et al., 2020). This can undoubtedly create concerns as the technologies are implemented more quickly than new security systems can be created or existing systems can be updated to protect against the new threats.

Rapid technological advancement makes it possible to increase the use of consumer mobile devices for continuous outpatient monitoring (Coventry & Branley, 2018; Kotz et al., 2016; Ksibi et al., 2023). In addition, the introduction and acquisition of newer technologies increases

connectedness (via the Internet or intranet) of medical devices in various ways for effective patient care. This makes accessibility to medical devices from different connection points relatively easy, but it increases the likelihood of cyber-attacks (Coventry & Branley, 2018; Kotz et al., 2016).

Technological advancement increases the vulnerability of the system to cyber-attacks via connected medical devices, hence increasing the chances of attacking medical institutions from various access and connection points. Connected devices can be directly attacked by malicious software, or they can be a channel through which medical systems are attacked, causing massive data breaches (Jump, 2019; Kovačić et al., 2022). The myriad of entry points via personal mobile devices connected to health systems increases the speed with which cyber threat incidents can spread within the medical systems of a country or across several countries (Berr, 2017).

Technological advancement also offers innovative tools for bypassing cybersecurity. According to ISACA (2015), new and emerging security-breaching tools are a major factor that impacts cybersecurity.

Closely related to technological advancement is the fact that many healthcare technologies are Internet of Things (IoT) devices. The 2020-2021 healthcare cybersecurity report highlights the use of IoT devices in healthcare as one of the security challenges that are particular to healthcare (Morgan, 2020b). This challenge is attributed to the fact that a variety of IoT devices run on similar operating systems, making the devices vulnerable to the same cyber threats. The devices' operating systems are small, and their security tends to be bolt-on rather than built-in (Morgan, 2020b).

3.5.3 OUTDATED TECHNOLOGY

Outdated software and hardware contribute to cyber-attacks, as attackers exploit the vulnerabilities of old and obsolete systems (e-Estonia, 2018). These vulnerable devices expose healthcare to cyber-attacks. National healthcare sectors in less economically strong countries may operate on outdated and unsupported legacy systems because they operate on insufficient budget investment in ICT infrastructures (Martin et al., 2017). Outdated technology presents a challenge to implementing cybersecurity, and at the same time, it is a factor that makes healthcare institutions vulnerable to cyber-attacks (Coventry & Branley, 2018). Finally, outdated technology is considered a cyber threat to healthcare organisations (Luna et al., 2016).

The research of Mello (2017) highlights that, in some cases, significant parts of healthcare providers' security systems are outdated and evolving technologies are too expensive and demanding to implement or adapt. Ageing infrastructure was outlined as another reason the healthcare sector is liable to be influenced by cyber-attacks (Ahmed et al., 2019).

3.5.4 CHANGING GOVERNMENT POLICY

Changing government policy in promoting the adoption of healthcare technologies has been identified as a key factor contributing to increased cybersecurity exposure within healthcare organisations. Governments worldwide continue to encourage the digital transformation of health systems to improve service delivery, data accessibility, and patient outcomes. These shifts include the implementation of electronic health records (EHRs), telemedicine platforms, and integrated health information exchanges. However, while such policies aim to enhance efficiency and patient-centred care, they may inadvertently heighten cybersecurity risks if adequate safeguards are not embedded in the implementation processes (Kruse et al., 2017).

The rapid integration of technological tools in healthcare often outpaces the establishment of comprehensive security frameworks. Ahmad et al. (2021) emphasise that E-Health environments handle large volumes of sensitive personal and medical data, making them attractive targets for cyber-attacks. As healthcare organisations transition to interconnected systems, vulnerabilities emerge due to insufficient encryption, weak access controls, or a lack of security awareness among staff. Similarly, Ksibi et al. (2023) highlight that risk management practices in many health institutions remain reactive rather than preventive, with limited resources dedicated to cybersecurity preparedness.

Moreover, policy-driven digitalisation can place smaller or resource-limited healthcare providers at a disadvantage. According to Kovačić et al. (2022), some institutions struggle with access to the necessary technical expertise and funding to implement secure E-Health systems effectively. Consequently, while government policy changes foster technological progress, they must be accompanied by robust cybersecurity guidelines, continuous training and investment in secure infrastructure to mitigate emerging risks.

3.5.5 EMERGING THREATS

New types of threats built to take advantage of emerging healthcare technology have been identified as a trend challenging healthcare security. Despite new regulations trying to protect

medical integrity and patient privacy, new threats target an increasing number of E-Health ICT systems (Kotz et al., 2016). According to Kruse et al. (2017), the inability to keep up with new cyber trends and threats presents healthcare organisations with serious challenges.

Research has indicated that advancement in digital transformation and the adoption of smart ICT, including IoMT in healthcare, brings new risks (Ksibi et al., 2023; Moonsamy & Ahmed, 2023). This is because communication is expected to happen via public infrastructures like the Internet and cloud servers, and some users operate using low-cost devices with limited resources (Ksibi et al., 2023). Examples of emerging risks in the sector include data breaches, ransomware, cyber-attacks, and software malfunctions (Moonsamy & Ahmed, 2023). It is argued that addressing these existing and evolving threats requires the development of strong risk management techniques. Healthcare digital developers must adapt their solutions more rapidly than threats emerge and must constantly devise appropriate new security strategies to secure healthcare data (Djuranovic et al., 2023).

Artificial Intelligence (AI) risks are among the emerging E-Health threats. There is an argument that although the AI predictive algorithm approaches in E-Health have many advantages, they may pose additional concerns regarding the security of healthcare data (Tahenni & Belkhir, 2025). The continuous development of these algorithms increases their ability to extract information from medical records and to draw relevant inferences. Nonetheless, the increase in predictive power also creates and gives rise to security and privacy problems in E-Health systems (Tahenni & Belkhir, 2025).

3.5.6 LACK OF PREPAREDNESS BY HEALTHCARE ORGANISATIONS

The fact that healthcare organisations are not systemically prepared to contain cyber threats can be considered a challenge (Tully et al., 2020). A review by Kruse et al. (2017) found that the healthcare industry lags behind other industries in securing data. This is despite the fact that the sector faces fast technological advancements that expose it to ever-changing cybersecurity trends and threats. Hence, the paper recommended that healthcare organisations constantly adapt to the changing cybersecurity trends and threats like ransomware.

Government incentives to increase the meaningful use of healthcare technologies like EMRs have resulted in substantial increases in ICT utilisation by healthcare providers over a short space of time, and without a well-prepared, adequate network or ICT resources to help fight any attacks (Verizon, 2016). The incentives have encouraged healthcare providers to suddenly

adapt to the use of ICT systems without a proportionate increase in the number and complexity of ICT support staff (Spence et al., 2017).

Lack of security preparedness in the event of a cyber-attack (for example, no clearly described security response procedure) was one of the problems identified with England's NHS after the 2017 global WannaCry attack. Security unpreparedness and unclear allocation of responsibilities made it challenging to assess the institution's cybersecurity resilience and to foresee the economic impacts of the attack on the healthcare or social system (Ghafur et al., 2019).

3.5.7 LACK OF RESOURCES

It is argued that, although the healthcare industry is faced with rapidly changing technology that needs regular updates (to keep up with advancements and cybersecurity holes), the industry is still not spending sufficient time or funding to install technology updates. Instead, significant funding is spent on system integration (U.S. Department of Health and Human Services, 2016). This results in a lack of investment in cybersecurity, including clamp downs on spending by cybersecurity personnel in the sector (Coventry & Branley, 2018).

There is evidence obtained from research that both sufficient time and funding are required to ensure the maintenance and protection of healthcare technology and to achieve security goals related to safeguarding essential information housed in healthcare organisations (Burke et al., 2024; Mbacop et al., 2025). Inadequate resources (that is, insufficient funds and time) can affect a hospital's ability to acquire appropriate numbers of qualified security staff and cybersecurity expertise to set up security barriers (Coventry & Branley, 2018; Verizon, 2016). Jalali and Kaiser (2018) identified such a lack of resources, resulting from declining net revenue and the inability to attract capable ICT experts, as a factor that impacts healthcare institutions' ability to intensify efforts to close the cybersecurity gap.

The absence of resources in terms of technological devices and expertise to properly secure patient data has also been identified as a security challenge that healthcare organisations face (Kotz et al., 2016). England's NHS, a publicly funded and nationalised healthcare system, identified limited budgets and time-consuming approval processes as problems that impact its ability to adapt to ever-changing technological challenges (Ghafur et al., 2019).

A limited budget makes it difficult for healthcare organisations to allocate resources, resulting in a compromised cybersecurity investment (Ghafur et al., 2019). Although all sectors see the

choice of allocating limited resources as a trade-off, given the sensitivity of information in healthcare systems, the potential consequences for patients and the economic impact of security failure can be overwhelming if not addressed (Ghafur et al., 2019).

The resources required to secure healthcare information are costly, making many healthcare organisations reluctant to invest enough to protect sensitive information (Luna et al., 2016). The availability of resources has a direct effect on how healthcare organisations adapt to the ever-changing technological landscape. This hinders progressive investment in ICT, which is considered to be necessary to encourage the establishment of a security culture (Ghafur et al., 2019). Limited funding means limited investment in technological advancement, resulting in healthcare services based on outdated technologies. Low resource availability also impacts technical support for security issues.

ISACA argues that a lack of resources has always been a challenge in all industries (ISACA, 2015). However, the effect of the problem is greater in the health sector partly because only a limited portion of the sector's budget is allocated to ICT. An excessive part of resources is associated with reskilling cybersecurity professionals (Frost & Sullivan et al., 2014). The evolution rate in cybersecurity and the skill sets of cybersecurity professionals are not in alignment. The shortage of suitably skilled cybersecurity professionals has a negative impact on organisations (like the healthcare sector), resulting in increasingly frequent and costly data breaches (Frost & Sullivan et al., 2014).

3.5.8 LACK OF AWARENESS, EDUCATION AND TRAINING

Based on recent literature, the importance of cybersecurity awareness cannot be over-emphasised (Mbacop et al., 2025; Vilakazi & Adebisin, 2023). Healthcare organisations need to be aware of emerging cybersecurity trends and threats to keep up with the protection of healthcare information. Ghafur et al. (2019) highlight a severe lack of awareness of vulnerabilities associated with the software and hardware that were used within the NHS system. According to these authors, vulnerability awareness problems were due to the absence of records of all the software and hardware used within the NHS (Ghafur et al., 2019). As a result, employees lacked awareness of the organisation's ICT technologies and the vulnerabilities associated with the use of the technologies.

Ghafur et al. (2019) also stress the need for a greater emphasis on cybersecurity training for all healthcare employees, given the risks human error poses to data security in the industry. Lack

of ongoing awareness raising, up-to-date training and education on cybersecurity has also been highlighted (Scott, 2015).

3.5.9 ERRORS RELATED TO HUMAN FACTORS

Cyber-criminals or hackers constantly look for careless and gullible users to take advantage of (e-Estonia, 2018). These malicious intruders often gain access to sensitive data without detection because of human error or carelessness (Murphy, 2015).

According to research reports, human error resulting from negligent employees or contractors has consistently been considered one of the three major causes of cyber threats (IBM Security, 2019; Ponemon Institute, 2018). Other causes include malicious or criminal attacks and system glitches as depicted in **Figure 3.3**.

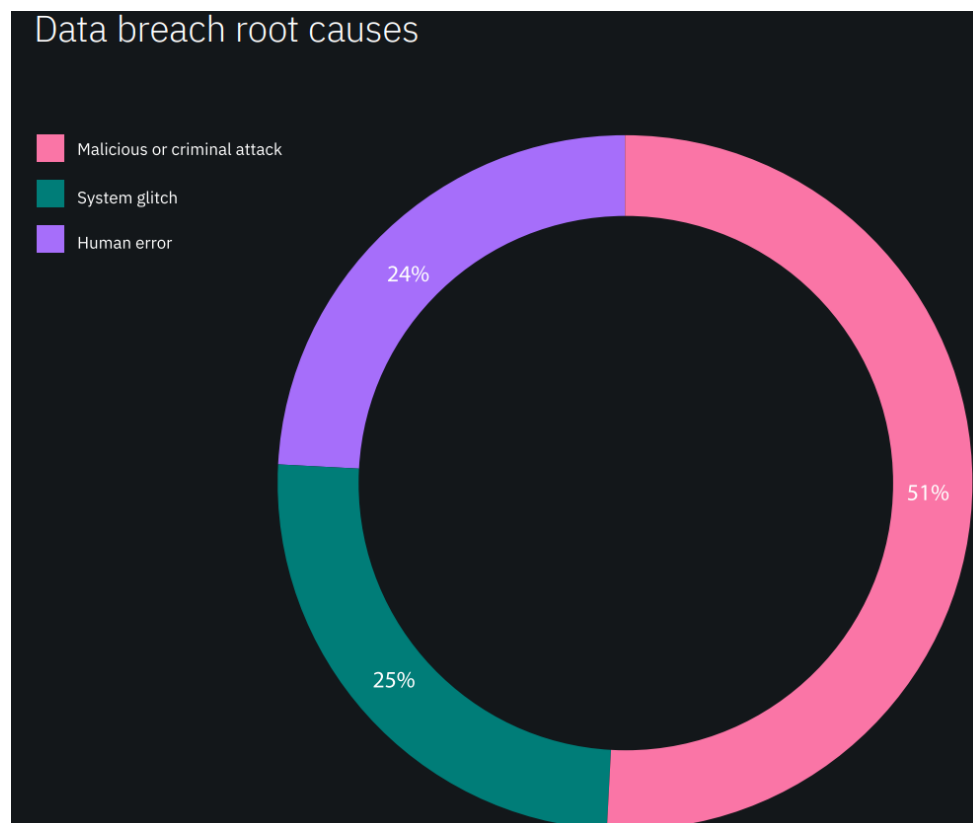


Figure 3.3: Causes of Data Breaches (IBM Security, 2019)

According to the IBM Security Service Cybersecurity Intelligence Index Report, human error was found to contribute to over 95% of security incidents (IBM Security, 2014). The most common error was users clicking attachments that were malicious or unsecured web links (IBM Security, 2014). Employee behaviour, such as employee negligence and clicking on infected

email links, contributed to 46% of data breaches in 2017 (Ghafur et al., 2019). This is unsurprising as employees are often considered the entry point for cyber-attacks like ransomware.

Employees' negligence and their lack of awareness were reported to contribute up to 58% of the company's ransomware attack risk (Ponemon Institute, 2017). Hence, employees are considered the weakest link in the fight against cyber threats (Ponemon Institute, 2017). Errors related to human behaviour is identified by several related research reports as contributing significantly to cybersecurity vulnerability (Glaspie & Karwowski, 2018; Hedström et al., 2013).

Madnick and Mangelsdorf (2017) emphasise the importance of addressing people issues if organisations are to avoid serious cybersecurity problems. These security experts indicated that many of the vulnerabilities in organisations originate from the existing corporate culture and the practices that the organisation has in place; these weaknesses are usually created unintentionally. The research went on to state that if top management were serious about reducing cybersecurity vulnerabilities, they also needed to address managerial and organisational aspects of cybersecurity. If not, the management would miss essential issues when working towards addressing cybersecurity (Madnick & Mangelsdorf, 2017).

3.5.10 ACCOUNTABILITY

Cybersecurity problems identified by NHS England included unclear accountability – “who is responsible for cybersecurity?” (Ghafur et al., 2019). Assigning and enforcing accountability was identified as a significant problem confronting cybersecurity, making it challenging for frontline organisations to seek appropriate resources and help (Ghafur et al., 2019).

3.5.11 MISSING CYBER INCIDENT RECORDS

An inability to keep systematic records of cyber incidents is a cybersecurity challenge and if not addressed can have impact properly documented awareness of cybersecurity incidents affecting organisations. Further, it can affect incident response because keeping incident records helps organisations implement adequate control that mitigate future incidents (Seng, 2023). It is argued that this can lead to organisations missing opportunities because they do not fully understand existing and emerging cyber risks and threats (Ghafur et al., 2019).

Lack of threat information is identified as a difficult challenge for healthcare institutions to overcome. This makes it difficult to answer questions like “Does the threat information apply to my organisation?” or to develop processes to help answer the question (Health Care Industry Cybersecurity Task Force, 2017).

3.5.12 LACK OF UNDERSTANDING AND ECONOMIC ASSESSMENT

Additionally, being unable to measure risks and vulnerabilities at various levels, particularly at the local level of the organisation, makes it challenging to foresee cyber-attacks’ impact on the organisation’s infrastructure, data and patients (Ghafur et al., 2019). There is a need to assess the economic impacts of cyber-attacks to cultivate a security culture and to understand what works (Ghafur et al., 2019). Scott (2015) identifies a lack of management understanding of the importance of patient privacy and security violations, and the organisational consequences associated with losing healthcare information as one of the challenges. The author argued that these challenges are attributed to the insufficient allocation of the ICT budget towards security (Scott, 2015).

3.5.13 SECURITY CULTURE

Research has found that having a security culture in place positively impacts the security perceptions of users related to e-services like e-government, and this affects its implementation positively (Alharbi et al., 2017). The reverse should also be the case, where a lack of security culture will negatively influence the implementation of electronic-based services. Research conducted by Ahmed et al. (2019) supports this finding; a lack of security culture was highlighted as one of the cybersecurity challenges facing the healthcare sector (Ahmed et al., 2019).

Da Veiga, (2019) defines security culture as “the unconscious manner in which things are done in the organisation to secure information”. It refers to employees sharing values, attitudes and knowledge that are then applied to ensure the security of the organisation’s assets. A security culture is considered to be a subculture within the organisational culture (Da Veiga & Martins, 2017; Schlienger & Teufel, 2003). Understanding the influence of security culture requires important connections to the development of an organisational culture, which is rooted in the organisation’s strategy and objectives.

It has been argued that a behavioural control measure that can be used to address human-related issues affecting information protection is the development of a strong security culture (Alhogail, 2015; ENISA, 2017). Only when information is protected throughout its lifecycle, regardless of its usage, can a really robust security culture be established (Da Veiga & Martins, 2015a).

The development of a robust security culture is identified and discussed in this chapter as a cybersecurity challenge in E-Health. In Chapter 4, the term is revisited and described as comprising both an information security culture and a cybersecurity culture. However, this chapter has explained how the concept ‘security culture’ is derived from a broader idea of culture to a more specific concept of cybersecurity culture and is the focus of this research.

3.5.14 OTHER CYBERSECURITY CHALLENGES

In addition to the challenges identified above, the physical location and the size of the medical institution can also affect cybersecurity. Rural hospitals and clinics differ significantly in their priorities compared with teaching hospitals and hospitals in urban areas. Smaller hospitals outsource ICT services more often, and bigger hospitals make more substantive ICT security investments (Menachemi et al., 2005). In addition, there is no consistency across healthcare organisations on the priorities placed on cybersecurity or on steps taken to mitigate against cyber threats and the resulting damages (Jalali & Kaiser, 2018).

The resultant complexity is rich with opportunities for exploitation by cyber-criminals. This complexity is exacerbated by the very limited internal stakeholder alignment, and both affect the effectiveness of cybersecurity and undermine efforts to close cybersecurity gaps (Jalali & Kaiser, 2018). The fact that healthcare vulnerabilities exist countrywide adds to a cybersecurity challenge. Many countries have similar vulnerabilities across healthcare institutions, and this makes it easy for attackers to target healthcare institutions in several countries using identical attack strategies (Park et al., 2010; Zarei & Sadoughi, 2016).

However, Morgan (2020b) highlights insider threats as one of the leading security weaknesses that healthcare institutions like hospitals grapple with. Lack of legal and regulatory compliance by organisations and individual staff members is a reason for healthcare cyber-attacks (Ahmed et al., 2019). Kotz et al. (2016) attribute the cybersecurity challenge to both the change in the movement of seriously ill patients to larger hospitals elsewhere (that is, changes in the “locus of care”) and to the strong economic incentives. This might mean that the healthcare workers

at the new location do not have strong relationships with the patients and might be more careless regarding the protection of the patient data and compliance with existing regulations.

Table 3.6 is used to summarise a variety of challenging factors of cybersecurity development and implementation that were not discussed in **Sections 3.5.1 to 3.5.13**.

Table 3.6: Cybersecurity Challenges

Cybersecurity Challenges	Paper and/or Authors
Location and size of medical institution	(Menachemi et al., 2005)
Increasing endpoint complexity None or low internal stakeholders' alignment Inconsistency on cybersecurity priorities	(Jalali & Kaiser, 2018)
Healthcare vulnerabilities and threats are worldwide	(Park et al., 2010; Zarei & Sadoughi, 2016)
Insider threats	(Morgan, 2020b)
Legal and regulatory issues	(Ahmed et al., 2019)

This chapter investigates the **Research Sub-Question 1 (RSQ 1): “What cybersecurity threats and challenges confront E-Health institutions?”** The researcher achieved this by reviewing the literature firstly on reasons healthcare institutions were targeted by cyber-criminals (see **Section 3.4**) and secondly on the various challenges that hamper the achievement of cybersecurity in healthcare institutions (see **Section 3.5**).

The factors from the two sections were combined to form a database of challenges and reasons depicted in **Figure 3.4**. The database was analysed and evaluated. The challenges were considered non-common since they were not viewed as reasons for targeting healthcare institutions and hence were extracted and kept to the left. The remaining factors proceeded to the predominant cybersecurity challenges holder.

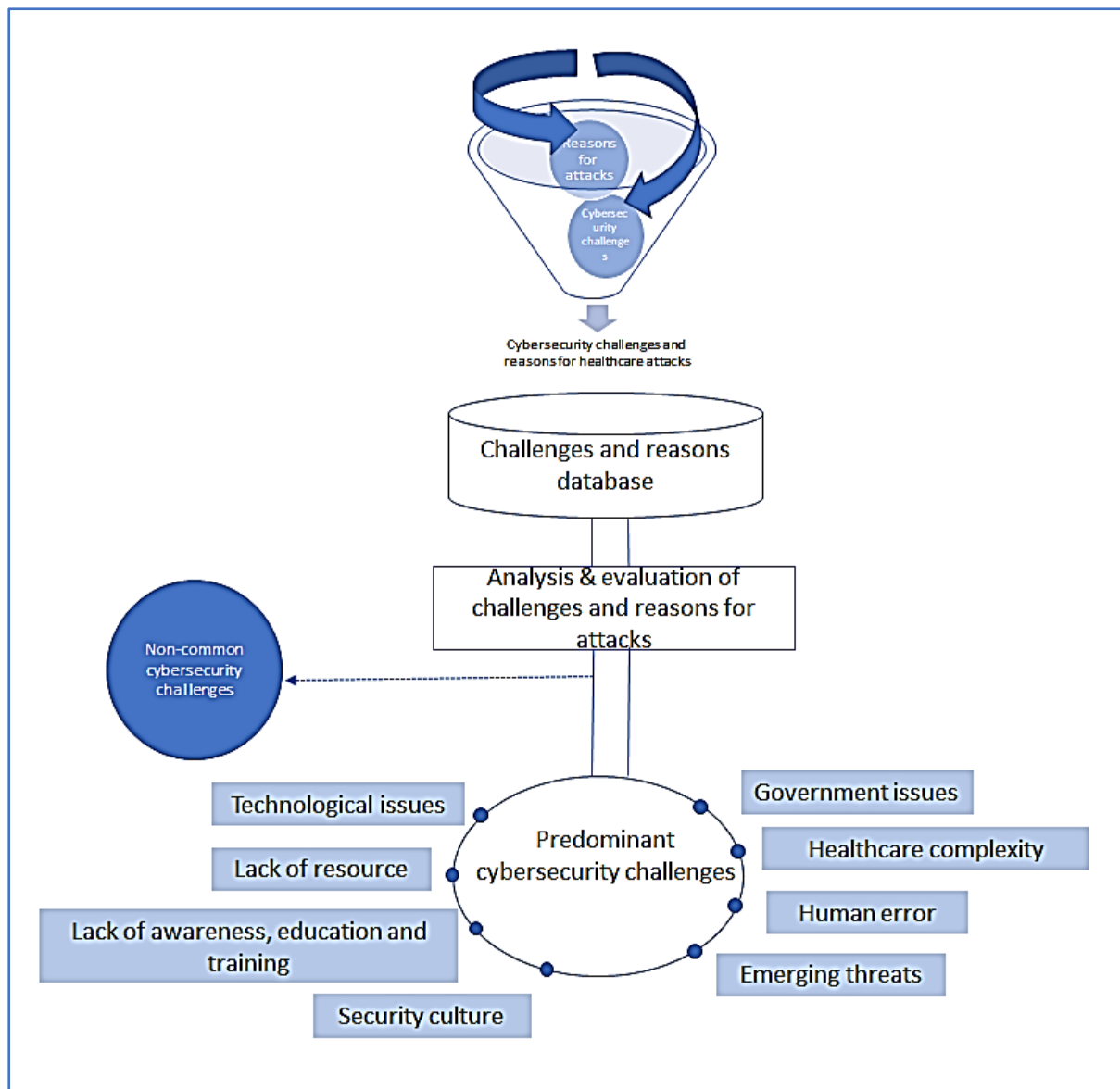


Figure 3.4: Extraction of Cybersecurity Challenges (own source)

Although all the cybersecurity challenges discussed in **Section 3.5** were considered to be important, in this research, only the factors recognised as challenges and reasons for targeting healthcare institutions were considered as predominant cybersecurity challenging factors.

There is a need for a concentrated effort to instil and promote a full understanding of cybersecurity and hence to address the identified cybersecurity challenges. Without this, the health organisations will endanger patients' safety and risk reputational and financial loss (Ghafur et al., 2019).

In the preceding section, the reasons why healthcare institutions are the target of cybersecurity threats and the challenges that confront the institutions were presented. Hence, the research

addressed *Research Sub-Question 1 (RSQ 1)*. Section 3.6 looks at the cybersecurity threats that confront the E-Health sector from a different angle, describing in detail the different types of cyber-attacks and looking for ways to prevent them.

3.6 ADDRESSING CYBER THREATS AT E-HEALTH ORGANISATIONS

The growth in the volume, variation and severity of digital security attacks each year is a reminder that cybersecurity threats are a new reality for many business organisations. The threats culminate in actual malicious cyber-attacks or cybersecurity incidents, which may be either malicious or unintentional. Cyber-attacks are human-driven, are malicious in nature and constantly change. Cybersecurity incidents are generally caused by people, and irrespective of the size or scope of a data breach, it is enabled by an action or failure of someone inside the organisation, even if initiated elsewhere (van Zadelhoff, 2016). However, some cyber threats emerge internally within the organisation while others emerge externally (Luna et al., 2016).

The sheer volume of cybersecurity attacks increases each year, the threat landscape becomes more varied, and attackers worked tirelessly to invent new attack avenues and implement more plans to cover their tracks (Symantec, 2018a).

The cyber threats that confront different organisations vary, but it is widely acknowledged that the healthcare sector has become a primary target for cyber-attacks (Coventry & Branley, 2018; e-Estonia, 2018). For instance, Estonia's healthcare sector experienced 32 cyber-attacks in 2019, and 10 of these cases directly affected hospitals and practitioners' operations (e-Estonia, 2018). Cyber threats to healthcare systems are persistent, ever-growing, evolving, unexpected, and unpredictable, and are concerns for both Healthcare Delivery Organisations (HDOs) and Medical Device Manufacturers (MDMs) (Jump, 2019).

Understanding the threats associated with using automated systems is the starting point for applying control measures (McConnell, 1994). Understanding the cyber threats confronting healthcare institutions is critical to managing their risks (Health Care Industry Cybersecurity Task Force, 2017). As such, this section is dedicated to understanding the cybersecurity threats that often confront healthcare organisations. This will help to align the proposed solution to addressing the effect of the threats in the organisations.

Some types of cyber-attacks that confront healthcare institutions are discussed in the sections that follow and are depicted in **Figure 3.5**.

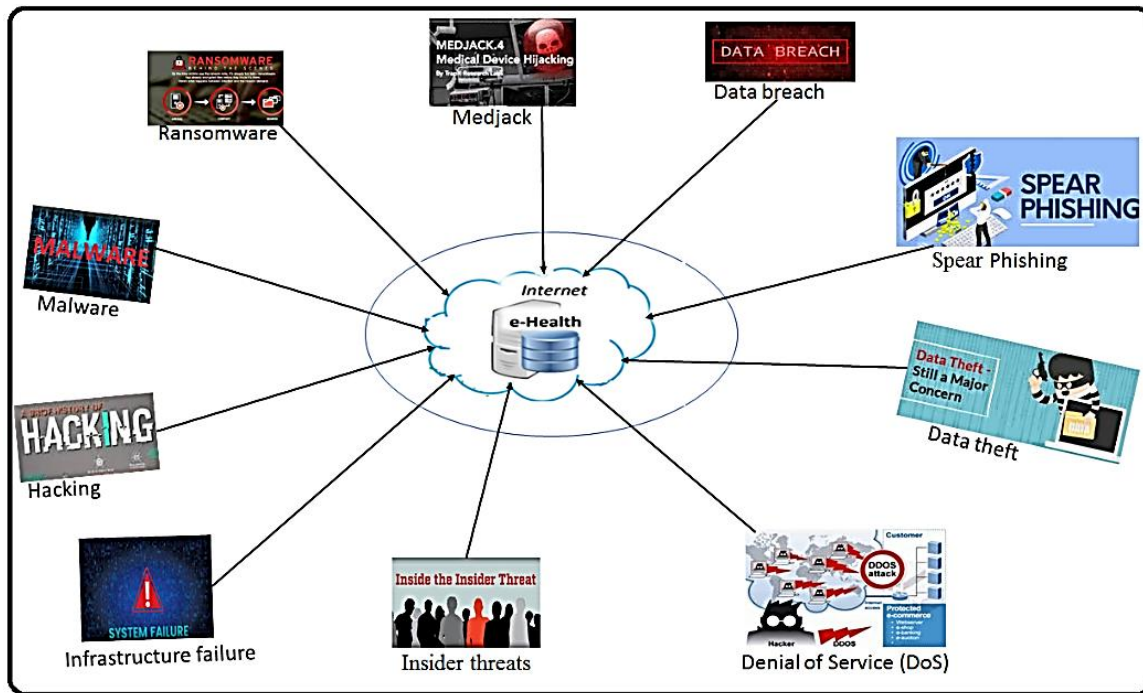


Figure 3.5: E-Health Cybersecurity Threats (own source)

The types of cyber-attack depicted in **Figure 3.5** are elaborated in no specific order in Sections 3.6.1 to 3.6.8.

3.6.1 DATA BREACHES

A data breach is an incident where an individual's personally identifiable information (PII) (name, ID number/social security number, medical records, driver's license details, and financial records) is at risk of being exposed electronically or via a paper form (ITRC, 2019; Ponemon Institute, 2018). As a new reality, data breaches are not a matter of 'if' they will happen, but rather 'when' they will happen (ITRC, 2019).

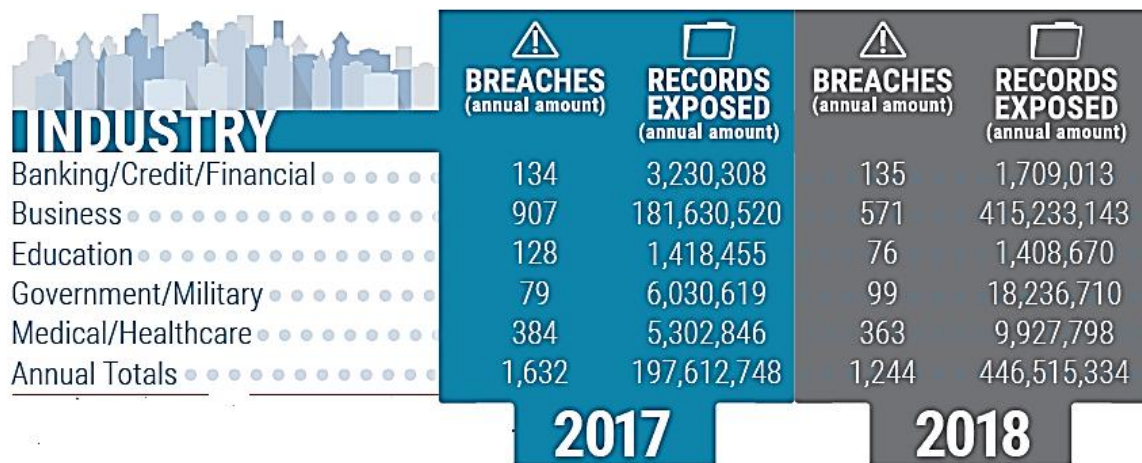
Data breaches present a growing threat in the healthcare industry (Alder, 2024b; Perakslis, 2014). In recent years, the number and size of data breaches have increased significantly (Alder, 2024b; IBM Security, 2023; Ponemon Institute, 2016; U.S. Department of Health and Human Services, 2016; Verizon, 2022, 2024). A high percentage of healthcare organisations have experienced data breaches recently (IBM Security, 2023; Koppel et al., 2015; Symantec, 2018a, 2019; Verizon, 2022, 2024).

3.6.1.1 Healthcare as a Major Data Breach Target

A data breach is among the leading security concerns for many healthcare organisations regardless of the organisation's status (rich or poor) (Alder, 2024b; Cuenca, 2017).

Healthcare is listed in various data breach reports as the first and third industries with the largest data breaches (IBM Security, 2023; ITRC, 2019, 2020; Verizon, 2022). It is the industry with a high number of sensitive PII exposures and with the highest reported data exposure per breach in 2018 (ITRC, 2019).

Figure 3.6 and **Figure 3.7** depict 2017 to 2019 data breach statistics from the ITRC reports. According to the statistics, data breaches saw a general decline in 2017 compared to 2018 (see **Figure 3.6**). However, this decrease is small in the healthcare industry (a decrease of only 21 breaches). However, the 2019 report saw a bounce back with an increased number of breaches, and healthcare showed a significant increase compared to 2018 (see **Figure 3.7**). Healthcare remains the second most frequently breached industry. In 2017 and 2018, data breaches in the healthcare industry contributed the second-highest number of breaches after the business industry (ITRC, 2019).



INDUSTRY	2017		2018	
	BREACHES (annual amount)	RECORDS EXPOSED (annual amount)	BREACHES (annual amount)	RECORDS EXPOSED (annual amount)
Banking/Credit/Financial	134	3,230,308	135	1,709,013
Business	907	181,630,520	571	415,233,143
Education	128	1,418,455	76	1,408,670
Government/Military	79	6,030,619	99	18,236,710
Medical/Healthcare	384	5,302,846	363	9,927,798
Annual Totals	1,632	197,612,748	1,244	446,515,334

Figure 3.6: 2017 and 2018 Data Breaches by Industry (ITRC, 2019)

INDUSTRY	# OF BREACHES	# OF SENSITIVE RECORDS EXPOSED	# OF NON-SENSITIVE RECORDS EXPOSED
Business	644	18,824,975	705,106,352
Medical/Healthcare	525	39,378,157	1,852
Banking/Credit/Financial	108	100,621,770	20,000
Government/Military	83	3,606,114	22,747
Education	113	2,252,439	23,103
2019 TOTALS:	1,473	164,683,455	705,174,054

Figure 3.7: 2019 Data Breach Report by Industry (ITRC, 2020)

The 2022 data breach report (see **Figure 3.7**) shows that healthcare was the most compromised industry (ITRC, 2024). This information is consistent with other data breach reports (Alder, 2024b).

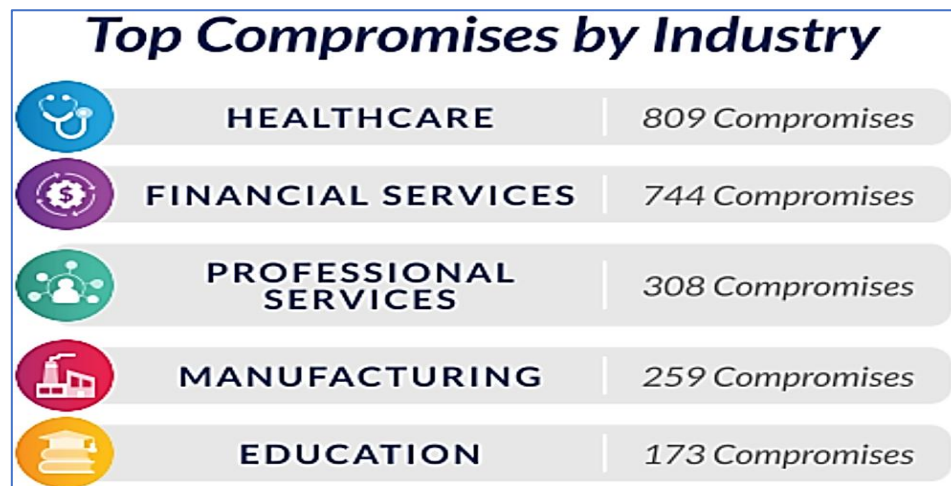


Figure 3.8: 2023 Data Breach Report (ITRC, 2024)

Based on the ITRC's 2024 report, most industries experienced an increase in the number of compromises, while a slight decrease in the number of victims was reported. Three industries, namely healthcare, financial services, and transportation, experienced more than double the number of compromises in 2023 than in 2022 (ITRC, 2024).

Table 3.7 depicts the summary comparison of the 2022 and 2023 data breach statistics.

Table 3.7: 2022 - 2023 Data Breach Report (ITRC, 2024)

Industries	2023		2022	
	Compromises	Victims	Compromises	Victims
Education	173	~4M	99	~2M
Financial Services	744	~61M	269	~27M
Government	100	~15M	74	~2M
Healthcare	809	~56M	343	~28M
Hospitality	45	~6M	34	~70M
HR/Staffing	10	~239K	-	-
Manufacturing	259	~5M	249	~24M
Mining/Construction	71	~222K	-	-
Non-Profit/NGO	105	~10M	72	~1M
Professional Services	308	~30M	223	~6M
Retail	119	~10M	65	~798K
Social Services	15	~193K	-	-
Technology	167	~65M	87	~249M
Transportation	101	~12M	36	~4M
Utilities	44	~73M	-	-
Wholesale Trade	53	~297K	-	-
Other	81	~4M	250	~12M
Unknown	1	0	-	-
Totals	3,205	~353M	1,801	~425M

The data breach statistics by industry from 2022 to 2023, depicted in Table 3.7, show the most compromised industry as healthcare, with 343 compromises in 2022. This significantly jumped up to 809 in 2023 (ITRC, 2024). The HIPAA healthcare data breach statistics report alluded to these statistics, indicating that the healthcare sector performed poorly compared to other industries regarding data breaches (Alder, 2024b).

Hacking is the leading method resulting in healthcare data breaches (Alder, 2024b; Ponemon Institute, 2018; Verizon, 2022). Hacking occurs when computer systems are accessed in an unauthorised way to disrupt operations or obtain information. Hacking into E-Health systems

in particular poses a severe security threat to healthcare organisations (Branch, 2018). The subsequent threats sent to the organisation start with denial of access to health services but can subsequently involve stealing personal and medical information (Branch, 2018).

According to an article on the Computer World website in 2016, a hacker known as “Thedarkoverlord” was reported to be selling 655,000 patient records obtained from three healthcare organisational databases on a dark web marketplace (Storm, 2016). Thedarkoverlord claimed to have gained access to and stolen the databases by exploiting Remote Desktop Protocol (RDP) at three healthcare organisations. The databases contained sensitive data and PII, such as patient’s date of birth, phone numbers, address, full names, gender and race, social security numbers, insurance information, and email addresses. Access to PII enables identity theft and fraud, such as taking out a credit card (Murphy, 2015).

Figure 3.9 shows a screenshot of one of the hacked healthcare organisation databases as proof of the intrusion by Thedarkoverlord; the asking price for this database was \$195,147.

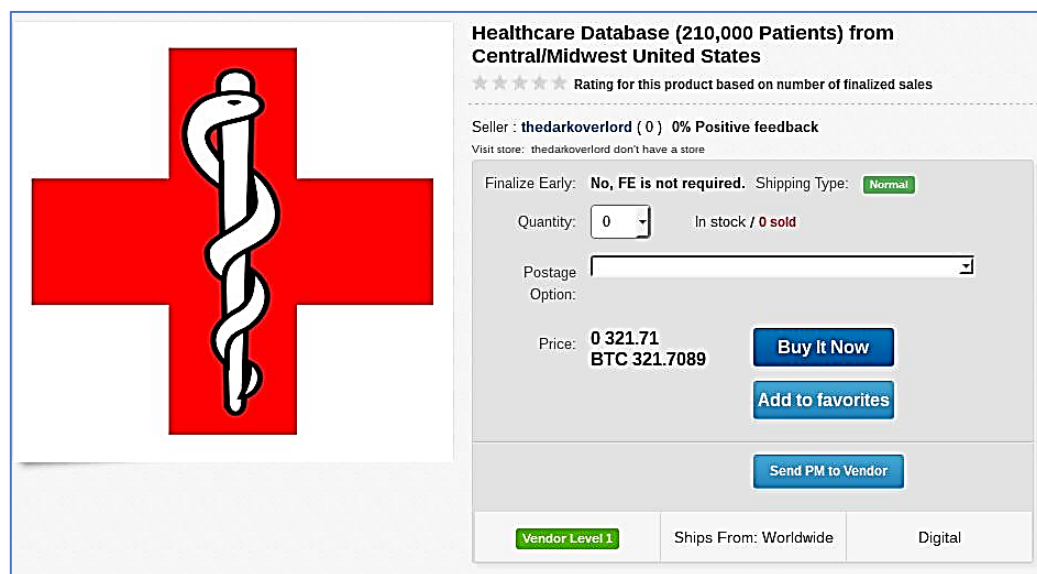


Figure 3.9: Sample of Thedarkoverlord Data Breached Database Up For Sale (Cox, 2016; Storm, 2016)

The other two databases that were up for sale contained 397,000 health records and 48,000 patient records, respectively and were being sold for \$389,390 and \$97,574 on the Internet (dark web). The increase in data breaches targeting healthcare organisations is attributed to the demand for medical data due to the financial gains associated with its sale.

3.6.1.2 Data Breaches Incidents in South Africa

Data breaches in South African organisations have increased in recent years, in healthcare and non-healthcare industries and in public and private sector organisations (Reuters, 2020; Mungadze, 2020). Although South Africa currently has a relatively small average number of data breaches, it emerged as one of the three countries with the highest (43%) probability of having a data breach in future (IBM Security, 2019). South African companies are highly vulnerable to cyber-attacks due to inadequate defences, due to the perceived unaffordability of security measures, and a lack of seriousness regarding cybersecurity (Burger, 2024; Cameron, 2017). However, experts' predictions and warnings are beginning to receive attention as one of the most significant data breach incidents hit the country in August 2020, namely the data breach incident at Experian (Hope, 2020; Mahlaka, 2020). The article in Die Burger (2024) also highlighted the high volume of cybersecurity threats that South African companies faced in 2022.

Experian, one of South Africa's largest credit bureaus and a Data Breach Resolution Company, was hit with one of the country's largest data breaches and self-inflicted injuries known to have occurred up to that time (Hope, 2020; Mahlaka, 2020). The firm, like other credit bureau firms, holds the sensitive data of millions of South African consumers as it obtains clients' personal information from banks, retailers and many other businesses. The massive data breach at Experian left credit information belonging to approximately 24 million South African consumers and nearly 800,000 businesses exposed (Hope, 2020; Mahlaka, 2020).

Experian unintentionally caused the data breach when it handed over the personal information of consumers and businesses to an individual fraudster who contacted the firm pretending to be a legitimate client. Experian revealed that the suspect said they intended to generate marketing leads to offer insurance and credit-related services (Hope, 2020; Mahlaka, 2020). The case of the Experian data breach is a significant example of a cyber threat because of human error or negligence.

The Experian data breach prompted South African banks to warn their customers to change the passwords used for online access to their bank accounts as a precautionary measure. Experian insists that no consumer credit or financial information was stolen by the fraudster, and that the information exposed in the data breach was already publicly available data in the ordinary course of business (Mahlaka, 2020). However, major banks, including Standard Bank, indicated that their clients' demographic information was leaked due to the data breach.

Another example of a data breach affecting a financial company in South Africa is the **Liberty Holdings Ltd incident**. In June 2018, life insurance giant Liberty Life was hacked, and its ICT infrastructure was breached (Chester, 2018). The hackers accessed the company's unstructured email data and compromised attachments (Chester, 2018). The hackers demanded millions of rand in return for not releasing critical information (around 40 TB of data) of Liberty clients (Chester, 2018). Liberty Life clients were worried and afraid that their personal information had been leaked to the dark web.

There was also a data breach affecting a South African private healthcare company, **Life Healthcare Group**. Life Healthcare Group operates private hospitals in South Africa and Botswana. In June 2020, during the COVID-19 pandemic, the Life Healthcare Group reported that its ICT systems suffered a targeted criminal attack that affected its hospital systems, business processing systems and e-mail servers (Reuters, 2020; Mungadze, 2020). The company immediately took its systems offline as a precautionary measure, which forced employees and service providers to switch to backup manual processing systems to ensure continuous operation and provision of patient care (Reuters, 2020; Mungadze, 2020). The company sought the assistance of external cybersecurity experts and a forensic team to assist its internal teams, and the company restored its operations in July 2020.

Data breaches in South Africa are rising alarmingly (Mzekandaba, 2024). According to Kaspersky (2021), 82% of companies in their South Africa case study had experienced cyber incidents, and 11% of them were a result of malicious human behaviours of members of the organisation. Other recent data breaches in South Africa include the TransUnion hack in 2022 (Moyo, 2022). The data breach incident is still considered the biggest hack in South Africa because it involved several million people. Additionally, the attackers demanded R223 million ransom for the compromised data. Other recent breaches were the Department of Justice cyber-attacks in 2021 and May 2024 (Moyo, 2021, 2024) and the national pension data leak (Leyden, 2024).

Experts warn that inadequate security and an increase in connecting devices make African countries, like South Africa, which operate in cyberspace very vulnerable to attacks (Cameron, 2017). The cases of cyber-attacks presented in this subsection are evidence of this.

Table 3.8 highlights a data breach attack incidents on healthcare providers between 2015 and 2024.

Table 3.8: Incidents of Data Breach in Healthcare

Date	Name of the Healthcare	Details of the Attack	Reference
January 2015	Anthem Inc.	In the foreign nation's attack on this database, approximately 80 million items of personal information were compromised.	(Terhune, 2015)
January 2017	Med-Center Health, Kentucky (USA)	A data breach on this hospital system affected approximately 160,000 patients.	(Alder, 2018)
July 2018	SingHealth Hospital in Singapore	This hospital was hit with one of the biggest data breaches of all time. The attack accessed and stole 1.5 million data records, including the prime minister's data.	(Narad, 2024)
June 2019	Laboratory Corporation of America Holdings	LabCorp's third-party billing collection vendor was hacked - the system had 7.7 million customers' personal data stored in it.	(Goldman, 2019)
March 2023	PharMerica Corporation	PharMerica and its parent company, experienced unknown third-party access to their systems and access to the personal medical information of people.	(PharMerica, 2023)
February 2024	Concentra Health Services, Inc.	The protected health information of 4 million patients was breached by their third-party company, Perry Johnson & Associates (PJ&A).	(HIPAA E-Tool, 2024)

Data breaches can be achieved in different ways, including unauthorised access, insider threats (employee error, negligence, improper disposal of forms), responding to phishing emails, erroneous security settings, password misuse, loss of a laptop, and sending unencrypted emails (ITRC, 2019). An emerging form of a data breach, referred to as “unsecured databases,” has affected healthcare-related organisations, for example, the cases of SkyMed Medical Evacuation Membership Service, University of Washington Medical Center and MedicareSupplement.com. According to IBM Security (2019), malicious attacks and system glitches are the most common causes of data breaches. The factors that contributed the most to the cost of a data breach are third-party involvement, compliance failures, extensive cloud migration, system complexity and operational technology (IBM Security, 2019).

3.6.2 MALWARE

Malware is malicious software developed to infiltrate computers and computer networks and can attack healthcare systems and medical devices. According to Verizon (2018), the malware was involved in the second-highest percentage of breaches between 2010 and 2017. Recent research on cybersecurity in the healthcare industry highlights malware as a major cybersecurity threat in healthcare organisations (He et al., 2021; Salama et al., 2024; Sendelj & Ognjanovic, 2022).

Five common types of malware have been identified (Coventry & Branley, 2018; Verizon, 2018).

- a) Adware displays advertisements over the top of other applications.
- b) Chargeware charges users for services without proper notification.
- c) Riskwares have codes and libraries that reduce the overall security of a device.
- d) Spyware or Surveillanceware gathers sensitive information for a third party.
- e) Trojans masquerade as legitimate applications.

Ransomware is a more sophisticated style of malware (Ponemon Institute, 2017; U.S. Department of Health and Human Services, 2016). Although the other types of malware also attack healthcare institutions, ransomware has appeared as the most prevalent malicious code, which mainly targets healthcare institutions (Davis, 2020; Verizon, 2018).

3.6.3 RANSOMWARE

Ransomware, developed by Dr Joseph in 1989, is a wide range of malicious software that restricts access to important individual or company information and demands some form of payment, mostly in digital currency (bitcoin), to lift access (Brewer, 2016). It is enabled by breaching organisations' networks, encrypting their files to restrict access, and requesting a ransom fee for the key to decrypt the file (Bridges, 2008; U.S. Department of Health and Human Services, 2016).

Ransomware is spread through spam emails designed to look legitimate, like invoices or company receipts, to convince recipients to open them. The email contains an infected website link or attachment that contains macros that, when clicked on or opened, download and infect the machine very quickly (Mustaca, 2014; Symantec, 2017). Once installed, ransomware duplicates to network files, internal, external and cloud drives, and encrypts the files.

The process through which ransomware spreads and attacks has five phases: exploitation and information, delivery and execution, back-up spoliation, file encryption, and user notification and clean-up (Brewer, 2016). Since its inception, ransomware has been causing disruptions, but the Colonial order of its attack served as a warning to people about the dangers of this attack (Liska, 2021). Organisations lose revenue both due to system inaccessibility resulting from the encryption and the ransom paid to the attacker to decrypt or release the decryption code.

Ransomware is a sophisticated threat and new variants become increasingly complex (Brewer, 2016; Ponemon Institute, 2017; Symantec, 2017). The second quarter of 2015 saw over four million ransomware variants and 1.2 million newly detected ones, and last quarter of 2017 saw 55% detections by consumers and up to 2% by businesses (Ashford, 2019; Brewer, 2016). There was a 46% increase in the number of ransomware variants in 2017 (Symantec, 2018b).

Over the years, there has been a steady increase in ransomware infections as a result of the profitability associated with this type of attack (Symantec, 2018b). Although in 2017 fewer attacks occurred and ransom demand was lower than in 2016, overall, the threat of ransomware has increased steadily since 2013 (Symantec, 2018b). WannaCry and Petya/NotPetya, were the first ransomware ‘families’ reported with 5.4 billion of WannaCry attacks blocked in 2018. Other families of ransomware include Cerber, Locky, Torrentlocker and Necurs, which were reported as the biggest hitters in cybercrime in 2017 (Symantec, 2018b). Liska (2021) reported the timeline of significant ransomware incidents between 1989 to mid-2021.

In 2017, there was shift in the target audience of ransomware attacks, where attacks towards enterprises increased. This trend accelerated in 2018, with enterprises accounting for 81% of all ransomware attacks (Symantec, 2019). From 2018 to 2019, there was a massive increase in business detections of ransomware, rising 365% percent from the second quarter of 2018 to 2019 (Zamora, 2019). The large increase confirmed the prediction that the number of attacks would continue to increase until a solution was found (Ashford, 2019). This remains the case, as according to the Sophos report, healthcare institutions showed an increase in ransomware attacks in 2024 (Mahendru, 2024).

Section 3.6.3.1 provides details on ransomware cases in healthcare organisations.

3.6.3.1 Ransomware Attacks in Healthcare Organisations

Ransomware attacks, which primarily affect individual consumers, have become one of the most significant threats to businesses. As noted above, incidents of this form of attack have grown significantly in many industries, and this is also the case with healthcare. Healthcare institutions have experienced ransomware attacks since 2012 and hospitals and healthcare facilities have become the key target for these threats (Mansfield-Devine, 2016; Madnick & Mangelsdorf, 2017; Mahendru, 2024; Zetter, 2016). Ransomware is one of the most significant healthcare cybersecurity threats identified (He et al., 2021; Salama et al., 2024; Sendelj & Ognjanovic, 2022).

Details of various ransomware attacks since 2012 follow. In 2012 surgeons at Lake County Hospital's access to the medical records of 7,000 patients was blocked; in 2014, in Clay County Hospital in Illinois, 12,621 patients' medical records were affected (Alder, 2016). In February 2016, a ransomware attack on Hollywood Presbyterian Medical Center in Los Angeles made it impossible for clinicians to access patient medical records, including backed-up files, and access to the medical equipment needed to provide treatment to patients was prohibited for 10 days until the hospital paid a ransom of \$17,000 in Bitcoin (Derse, 2016).

Hospitals throughout the world are affected. In September 2020, at the University Hospital of Düsseldorf (UKD) in Germany, a ransomware attack took advantage of a system vulnerability and caused the hospital's ICT systems to fail (Lakshmann, 2020; AP News, 2020). The failure of the ICT system required the hospital to send patients to other hospitals, and in the process, a patient died (the first recorded casualty). The attack was initially aimed at Heinrich Heine University but was misdirected (Lakshmann, 2020; AP News, 2020).

A recent ransomware attack hit Change Healthcare in February 2024 (Alder, 2024a, 2024b). This attack compromised the secure health information of 1 in 3 Americans, and a ransom of \$22 million was paid to delete the stolen copy of the data (Alder, 2024b). Also in 2024, a ransomware attack against the National Health Laboratory Service (NHLS) of South Africa compromised healthcare services nationwide because NHLS could not process millions of blood tests (Cluley, 2024).

Unfortunately, ransom payment does not guarantee that decryption keys will be made available. Kansas Heart Hospital and Change Healthcare ransomware attacks are examples where the hospitals were attacked and a ransom was paid but instead of the attackers decrypting the data, a second ransom was demanded (Siwicki, 2016). The hospitals did not pay the second

ransom because patients' information and the hospital's routine operations were not affected (Siwicki, 2016).

Table 3.9 summarises the successful ransomware attack incidents on healthcare institutions, listing other ransomware attacks on healthcare providers, showing that ransomware is still an imminent attack that targets healthcare institutions.

Table 3.9: Successful Ransomware Attack Incidents on Healthcare Institutions

Date of attack	Healthcare provider	Details of the attacks	Source
10 Feb 2016	Lukas Hospital in Neuss, Germany	Ransomware attacked the hospital's ICT systems in the form of email attachments. No ransom was paid as the hospital had complete backups. The hospital took all its systems offline until they were thoroughly restored. 20% of their surgeries were rescheduled, and less-severe emergency cases were moved to neighbouring hospitals.	(Schwartz, 2016)
13 May 2016	Ottawa Hospital, Canada	A ransomware attack affected 4 computers in its network. "No patient information was affected. The malware locked down the files, and the hospital responded by wiping the drives."	(Pilieci, 2016)
12 May 2017	United Kingdom (UK) National Health Service (NHS)	This WannaCry ransomware attack affected data and files on 230,000 ICT systems in 150 countries. Although the NHS in England was not the specific target of this attack, it suffered the biggest effect of the attack as it impaired functionality in 80 UK hospitals directly or indirectly. It blocked the critical ICT systems and prevented staff from accessing patients' records and essential services.	(Ghafur et al., 2019; Ghosh & Ashok, 2017)
1 October 2019	DCH Regional Medical Center	Ryuk attacked the DCH health systems and maliciously encrypted targeted files. The attack limited the three hospitals' ability to use the ICT systems and resulted in no access to patient lists. Patients could not be rescheduled for appointments. The operation was shifted to manual mode (paper copies). The hospital paid the attackers for the decryption key to unlock their data.	(Beahm, 2019; Taylor, 2019)

Date of attack	Healthcare provider	Details of the attacks	Source
20 Sept 2019	Campbell County Health (CCH)	A ransomware attack affected 1500 computer systems and prevented them from providing clinical services, particularly to new patients. Many examinations and procedures were cancelled, and some patients were transferred. 17 days later, CCH had not fully resumed all medical service operations due to this attack.	(Alder, 2019a)
28 July 2019	Eye Care Associates in Ohio	This optometry practice could not access its computer system. The attack disrupted the hospital for over two weeks, making it impossible to book new appointments and forcing the hospital to rely on manual records for patient treatment.	(Alder, 2019b)
8 July 2019	Premier Family Medical in Utah	Ransomware locked out specific data within the system. The hospital had to engage a technical consultant to help them regain access to the data.	(Clark, 2019)
15 June 2019	Gray's Harbor Community Hospital (GHCH) and Harbor Medical Group (HMG) in Washington	GHCH and HMG were hit with ransomware attacks, and a \$1 million ransom was demanded. The FBI advised the group not to pay as there was no guarantee that access to the information would be restored after the payment. The group notified their patients but, fortunately, could continue care during the attack and afterward.	(Clark, 2019)
10 June 2019	N.E.O Urology in Ohio	The ICT system was held hostage, causing the healthcare institution to lose between \$30,000 and \$50,000 daily. A ransom of \$75,000 in Bitcoin was paid through a third party to obtain the release of the locked medical files.	(Vallas, 2019)
7 June 2019	Part Duvalle Community Healthcare Centre in Kentucky	A second ransomware attack hit this centre (after the first attack in April, when a backup was used to recover the data and rebuild the computer system). The second attack made approximately 20,000 patient medical records inaccessible, including the appointment scheduling system. The Centre could not use backup and rebuild the system this time and was forced to pay the ransom of \$70,000.	(Alder, 2019c)
March 2019	Brookside ENT and Hearing Centre in Michigan	This Centre was forced to close as all files in the system were erased. The Centre had refused to pay a ransom of \$6,500, fearing more ransom requests, and as there was no guarantee of a successful decryption process.	(Rachel, 2019)

Date of attack	Healthcare provider	Details of the attacks	Source
9 January 2019	Columbia Surgical Specialists in Washington	This ransomware affected about 40,000 patients' data. The hospital paid the attackers a ransom of over \$14,000 to regain access to the data and encrypted files. It was impossible to access patients' information until the ransom was paid.	(Cohen, 2019)
1 February 2024	Lurie Childrens' Hospital	The attackers used Rhysida ransomware to attack the Childrens' Hospital and demanded \$3.6 million for the data stolen.	(Alder, 2024c)

3.6.4 MEDJACK (MEDICAL DEVICE HIJACK)

Medical Device Hijack is a type of malware that targets hospitals' medical devices. MEDJACK attackers infect vulnerable medical devices and use them to steal or corrupt data accessed via the hospital network, and to cause other disruptions (Storm, 2015). The malicious software enables attackers to perform simulated attacks by remotely controlling the affected medical devices, altering operations and transmitting corrupt or false data (TrapX Labs, 2015). Although medical device attacks have mostly been simulated, they can happen in reality (Klonoff, 2015).

Attacks on medical devices have introduced a new and serious threat to healthcare institutions globally; they may be considered the hospital's next security nightmare, with the medical devices being the weakest link in the chain (Newman, 2017; Storm, 2015). MEDJACK has been exploited to compromise medical devices like X-ray equipment, blood gas analysers (BGA), archives of images (x-rays or images derived from sonar, for example) and communication systems (PACS) (Storm, 2015). Other medical devices that present targets for MEDJACK are diagnostic equipment (CT scanners and MRI machines), therapeutic equipment (infusion pumps, medical lasers, and LASIK surgical machines), as well as life support equipment (oxygenation machines, lung and heart machines, ventilator machines, and dialysis machines). Infected medical equipment is identified as an internal threat to healthcare organisations, and it directly affects operations (Luna et al., 2016).

3.6.5 SPEAR PHISHING

Spear phishing is a form of cybersecurity threat spread by employees receiving what appears to be a personal email from high-ranked members of their organisation, requesting them to take specific action or to perform a particular duty that is consistent with their job specifications (Madnick & Mangelsdorf, 2017). The intention is to make the email look legitimate and persuade the recipients to open it. Like all the other forms of cybercrime, spear phishing has been on the increase. Spear phishing has a 70% chance of succeeding compared to untargeted mass phishing email attachments, which have a 1% to 3% open rate (Madnick & Mangelsdorf, 2017). Phishing is also identified as one of the leading cybersecurity threats that healthcare institutions battle with (He et al., 2021; Salama et al., 2024; Sendelj & Ognjanovic, 2022).

3.6.6 DENIAL OF SERVICE (DOS) ATTACKS

Denial of service (DoS) is another form of cyber threat that confronts the healthcare sector. In an attack designed to bring about denial of service, the organisation's network is overloaded with meaningless traffic, this is unnecessary flooding of networks or systems with requests intending to cause disruption (Luna et al., 2016; Martin et al., 2017). Denial of service may be either an internal or an external cyber threat and has direct consequences on the infected healthcare organisation (Luna et al., 2016). Examples of DoS attacks include Ping of Death and Teardrop attacks. DoS and Distributed Denial of Service (DDoS) were identified as the most often reported types of attacks on IoT devices. Hence, a new architecture consisting of detection and mitigation was proposed as a way to address this (Mihoub et al., 2022).

3.6.7 INSIDER THREATS

Among the attacks on the CIA, institutional data has been under threat from within the organisation. This is considered to be a more severe threat than an external attack because insiders are people with authorised access to organisational data (Alsowail et al., 2022). Closely related to the challenge of human error (discussed in **Section 3.5.9**) is the more general insider threat. Threats originating from inside the healthcare institution are both a challenge and a threat to cybersecurity as they present a serious risk of data breaches. Across the globe, healthcare is the only industry where internal sources constitute the biggest threat of data breaches (Verizon, 2018). More than half of fraud incidents in the healthcare sector perpetrated by employees or ex- employees of the organisation include customer data theft (Alder, 2024b;

Vasko & Gardner, 2019). The 2020-2021 healthcare cybersecurity report revealed insider threats as a significant security challenge confronting hospitals (Morgan, 2020b).

Various factors contribute to security threats in an E-Health institution, but these are linked to humans, who are considered the weakest link in the security chain (Al-Shehri, 2012). The usage behaviour of persons in healthcare sectors is one of the ways through which leaks of patients' information are compromised (Rengamani et al., 2010). The increasing evidence of this threat, reflected by increasing numbers of cybersecurity incidents, shows the healthcare sector's inability to understand the security-related behaviour of healthcare staff (Coventry & Branley, 2018). This leaves the industry vulnerable to cyber-attacks (Coventry & Branley, 2018).

Considering their responsibilities as the first line of defence in security, negligent and dishonest employees in healthcare organisations are believed to be threats to themselves, others (patients, co-staff, and organisation) and national security (Dlamini & Modise, 2012).

Human error, in addition to insider threats, is a significant cybersecurity challenge in healthcare institutions. Insider threats were identified as the major threat of data breach in the industry (Alder, 2024b). These security weaknesses are important as they highlight the magnitude of the human (people) problems toward cybersecurity in the healthcare sector. Considering these, tackling human issues to address cybersecurity challenges and threats is considered crucial.

A substantial number of cybersecurity vulnerabilities result from a weak security culture, which is evident in the intentional or unintentional practices of the people in the organisation. Having a strong cybersecurity culture is necessary when tackling this type of human problem. This discussion brings to light the essential aspect of this research: cybersecurity culture. As the focus of this research study, the concept of cybersecurity culture is discussed in detail in Chapter 4.

3.6.8 OTHER CYBER THREATS

In addition to the major cyber threats highlighted above, how the data of an healthcare organisation is falsified, damaged or misused includes intentional data corruption for financial, revenge or political gain (like modifying medical test results or compromising business email by creating fake personal communication); unwitting insiders, usually employees; outdated hardware, software or operating systems; unrealistically low budgets; terrorism; cybersquatting; and critical infrastructure failure. These threats may originate either internally or externally and can directly or indirectly affect the healthcare organisation.

Cybersquatting occurs when a trademark invented by one person is registered as an Internet domain name in another person's name to make a profit.

Cyberterrorism is when an act of terrorism is performed via cyberspace, targeting computers or networks to steal information or instil fear in individuals or groups.

The first global cybersecurity observatory listed the following factors as significant healthcare cybersecurity threats: Limited cybersecurity budgets; sales on the black market of electronic health records; vulnerable IoT and IoMT devices; unsecured mobile devices; cloud security; and under-trained staff (Cybersecurity Observatory, 2020). Some of these factors were discussed in **Sections 3.4** and **3.5** as reasons for targeting healthcare institutions and challenges to cybersecurity in healthcare.

The cyber threats presented in this section were viewed as the most serious threats affecting E-Health organisations and their patients. The magnitude of the threats discussed in this chapter show that healthcare is one of the most challenged industries. The reports and statistics presented are also evidence that cyber threats (like breaches, malware, and hacking) are present in the healthcare industry. People are prepared to pay large sums of money for medical data, and the research shows a high demand for such data.

The consequences of cybersecurity threats to healthcare organisations are highlighted in the **Section 3.7**.

3.7 CONSEQUENCES OF CYBER-ATTACKS ON E-HEALTH

Successful cyber threats can have devastating effects on patients and healthcare organisations. This section discusses some consequences of cyber-attacks on healthcare institutions.

3.7.1 COST IMPLICATIONS

The cost associated with data breaches has increased globally. Healthcare was identified as the top sector in terms of average total cost of data breaches for eleven consecutive years (IBM Security, 2021). The industry experienced a 29.5% increase in a single year (from 2020 to 2021) (IBM Security, 2021).

In South Africa, data breach costs increased by over 12% between 2017 and 2018 (IBM Security, 2019; Ponemon Institute, 2018). The cost is still increasing, with the 2021 cost of

security incidents showing an increase of 15% compared with 2020 (Hand, 2021; IBM Security, 2023).

In the United States, a data breach can cost a single hospital more than \$7 million (Claunch & McMillan, 2013). Heavily regulated industries, which healthcare is, are reported to have the highest industry average total data breach costs (\$6.45 million). This was followed by the financial and energy sectors, \$5.86m and \$5.60m, respectively, as depicted in **Figure 3.10** (IBM Security, 2019). The cost of healthcare data breaches continues to exceed the costs of all other industries. Average costs in 2020 showed an increased from those of 2019 of \$7.13m from \$6.45m (IBM Security, 2021, 2023). In 2023, the sector experienced an increase in average costs from \$10.10m in 2022 to \$10.93m in 2023 (an increase of 8.2%) (IBM Security, 2023). In three years (2021-2023) the average cost of healthcare data breaches rose consistently, showing an increase of over \$3million compared to the \$7.13 million average cost in 2020 (IBM Security, 2023).

The sector was also reported to have the highest per-record data breach cost, amounting to \$429 compared to other industries, indicating an increase from 2018 (IBM Security, 2019; Ponemon Institute, 2018). See **Figure 3.10** and **Figure 3.11** for the statistics of these data breach costs.

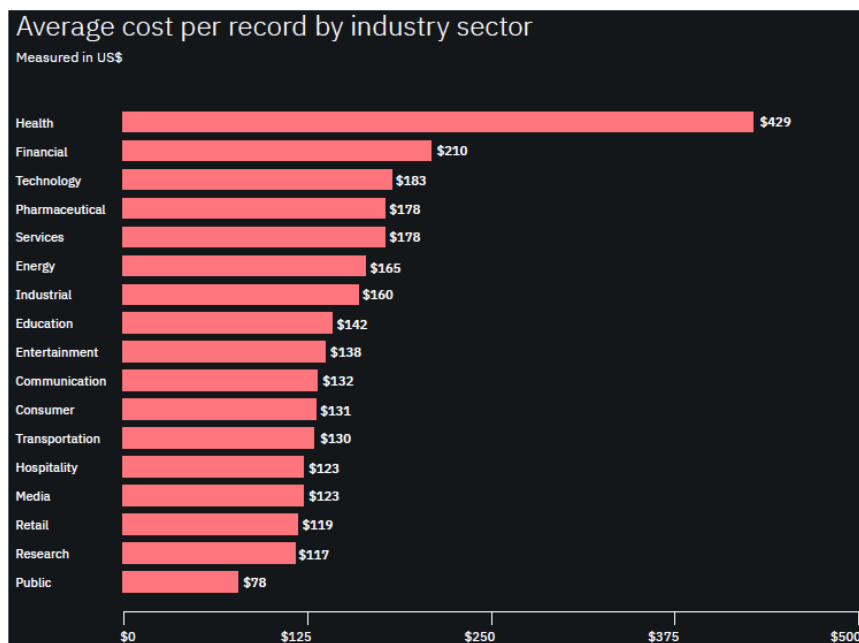


Figure 3.10: Average Data Breach Cost per Record by Industry Sector (IBM Security, 2019)

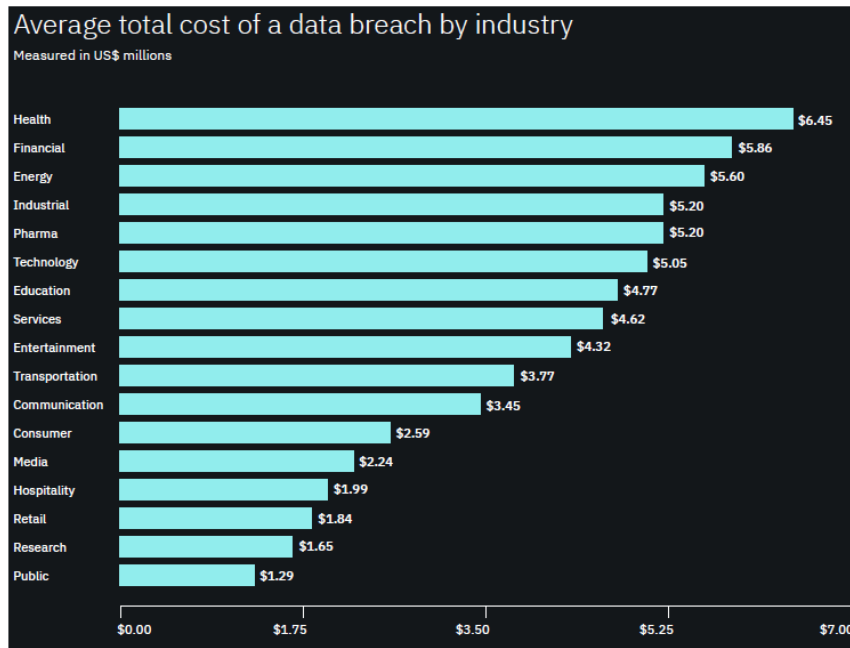


Figure 3.11: Average Cost of Data Breaches by Industry (IBM Security, 2019)

It was predicted that, due to the enormous number and wide range of cyber offences launched in healthcare, that the global healthcare sector would spend more than \$65 billion on cybersecurity products and services between 2017 and 2021 (Mello, 2017). By 2021 and thereafter, overall damages (all industries) due to cybercrime were expected to cost the world at least \$6 trillion annually. It was also predicted that the global healthcare sector industry would spend \$125 billion on cybersecurity from 2021 to 2025 (Morgan, 2020a) and more than \$18 trillion by 2040 (Dieleman et al., 2016).

3.7.2 OTHER CONSEQUENCES OF CYBER-ATTACKS ON E-HEALTH

In addition to costs associated with data breaches, cyber threats have impacts on healthcare institutions that seriously affect their ICT systems operations. Examples of these are litigation, fines and penalties, damage to organisational reputation, compromise of patient safety, financial loss, and financial consequences due to loss of trust by customers (Coventry & Branley, 2018; IBM Security, 2019).

Patients' trust can be compromised, resulting in an unwillingness to share data due to the bad publicity associated with cyber threats; this is particularly evident among patients with stigmatised conditions (Coventry & Branley, 2018; Shenoy & Appel, 2017). The Ponemon Institute and IBM Security Research found that an organisation that lost less than 1% of their

customers due to threats like data breaches had an average total loss of revenue of \$2.8 million. A 4% or more loss of customers resulted in an average of \$6 million.

Other consequences include loss of business resulting from business disruption, system downtime, the cost of new customer acquisition and revenue loss (IBM Security, 2019; Ponemon Institute, 2018). Additional consequences have manifested as data loss, attacks on medical devices and infrastructure and monetary theft (Perakslis, 2014). Murphy's (2015) study revealed that the fear of embarrassment associated with data breaches of personal information is ranked the highest by patients compared to the fear of financial and medical identity theft.

The risk categories associated with ransomware attacks include risk of patient data privacy loss, reputational loss, loss of future business, medical malpractice suits, and risks related to cost and expense. Other risks of malware and ransomware include delays in recovery, or denial of access to healthcare services, impaired functioning of medical devices, stealing of medical records, and deliberate harm to patients (Coventry & Branley, 2018).

Above all, the most devastating consequence of cyber-attacks in the healthcare space is the cost of life. Over the years, cybercrime has damaged the healthcare sector financially; now, it is beginning to claim life. In 2020, the effect of cyber-attacks on hospitals claimed the life of its first victim as a result of a ransomware attack at the University Hospital of Düsseldorf (UKD) in Germany (Lakshmann, 2020; Morgan, 2020a; AP News, 2020).

Although threats have been specifically mentioned, most of the consequences highlighted in this section apply to other cyber threats as well.

The security threats to healthcare sectors are mainly due to its operation's increasing reliance on cyber-based technology; the corresponding consequences call for a focused and coordinated cybersecurity effort from different stakeholders of the healthcare sector. Timely action could ensure that healthcare providers deliver quality care to patients while at the same time protecting their data and information from emerging cybersecurity risks and threats. Hence, this study's move toward a cybersecurity culture as a possible alternative to cybersecurity challenges.

3.8 APPROACHES TO CYBERSECURITY CHALLENGES

Various initiatives and efforts have been made to contribute towards addressing cybersecurity concerns (Harries & Yellowless, 2013; Rengamani et al., 2010). In the health sectors, solutions have largely focused on Legislative and Non-legislative approaches.

3.8.1 LEGISLATIVE APPROACH

A legislative approach to cybersecurity emphasises the use of regulatory controls to protect and prevent threats to the E-Health eco-system to safeguard the three security goals (confidentiality, integrity and availability) (Coventry & Branley, 2018). Setting up a regulation that guarantees healthcare stakeholders' integrity and adhering consistently to cybersecurity regulatory policy have been highlighted as essential to the new data source (Fernández-Alemán et al., 2013; Goozner, 2014). These legislations, regulations, and standards create proactive way of addressing cybersecurity threats and can lead to effective cybersecurity management, which reduces risk to patients' health (U.S. Food and Drug Administration, 2025).

Examples of legislations in response to addressing cybersecurity issues in healthcare sector are: U.S. Health Insurance Portability and Accountability Act (HIPAA) of 1996 [104 - 191] (U.S. Government Publishing Office, 1996); National Institute of Standards and Technology Cybersecurity Framework for improving their critical infrastructure (National Institute of Standards and Technology, 2018); General Data Protection Regulation (GDPR) (European Parliament & Council of the European Union, 2016); Protection of Personal Information (POPI) Act. (South Africa, 2013); and the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC), example ISO 27799:2016 (ISO 27799, 2016).

3.8.2 NON-LEGISLATIVE APPROACH

While regulatory measures are enforced towards securing the cyberspace, there are other non-regulatory measures that complement the achievement of cybersecurity. According to Gcaza, (2017) these measures can be categorised as technological, human, and holistic measures.

- **Technological measure:** Past cybersecurity measures implemented across various sectors have focused on technical solutions (Pfleeger & Caputo, 2012). It has been argued that protecting institution-sensitive data and preventing cyber-attacks requires effective technological measures, including network security, that can be achieved through a strategy of protection, detection, and reaction (Arogundade, 2023). To protect the sensitive healthcare information and systems, cybersecurity approaches have focused on technological tools such as firewalls, anti-virus, and network access control (Kotz et al., 2016). A report by the Ponemon Institute indicated the importance

of technological solutions as a good approach to cybersecurity (Ponemon Institute, 2017).

- **Human measure:** This represents non-technological measures to cybersecurity. It includes solutions such as training, education, and awareness. These measures relate to 'human factors', which show the roles of users in the security process (von Solms & van Niekerk, 2013). The two main dimensions of human measures are knowledge and behaviour (van Niekerk & von Solms, 2006). The two dimensions are interlinked in that desirable behaviour requires accurate knowledge. However, there is a possibility that someone with the right knowledge can display incorrect behaviour. It is imperative that the two dimensions are addressed to properly handle human factors (van Niekerk & von Solms, 2006).
- **Holistic measure:** This is a measure that promotes the use of both technological and human measures in a way that complements and helps to achieve the desired result.

The report by the Ponemon Institute also emphasised the significance of not focusing on technological solutions as an all-in-one solution, but instead as a part of the bigger puzzle of efforts in addressing cybersecurity threats (Ponemon Institute, 2017). Other researchers have also emphasised the importance of not focusing solely on technological solutions, as technical solutions on their own is insufficient to address cyber threats, improve cybersecurity and protect organisational information and systems due to human-related problems (Cavelty, 2007; Forte & Power, 2007; Gcaza, 2017; Gcaza et al., 2017).

Gcaza, (2017) argues that there is a need for a more holistic view to address the challenges of cybersecurity. This is because, according to the author, technological measures without the support of human measures or vice versa will fail. Gcaza's (2017) statement follows an argument that cybersecurity implementation is directly influenced by the direction of the measure applied and the direction is often determined by policymakers.

A holistic view is not static to one measure. Instead, it considers both technological and human measures with the objective of establishing users who maintain controls and honour their role in the security process (Gcaza, 2017). Therefore, the aim of holistic measure is to promote a cybersecurity culture. Research has argued that cultivating a culture of cybersecurity plays an important role in addressing human-related issues (Holdsworth & Apeh, 2017; von Solms & van Niekerk, 2013). As a result, cybersecurity culture is explored in this study as a measure to address the predominant cybersecurity challenges and threats in the healthcare sector.

3.9 CONCLUSION

IT technologies are essential in healthcare operations as they provide critical care to patients. Chapter 3 adopted definitions that describe cybersecurity as the protection of the cyberspace environment, its information, users and other assets. Cybersecurity is regarded as a broad concept as it deals with the protection of information and other assets in general, irrespective of their location.

Chapter 3 helped to answer Research Sub-Question 1 (RSQ 1): *“What cybersecurity threats and challenges confront E-Health institutions?”*

This chapter reviewed the literature to understand why E-Health institutions are vulnerable and highly targeted by cyber threats, the cybersecurity challenges that confront E-Health institutions, and the E-Health cybersecurity threats.

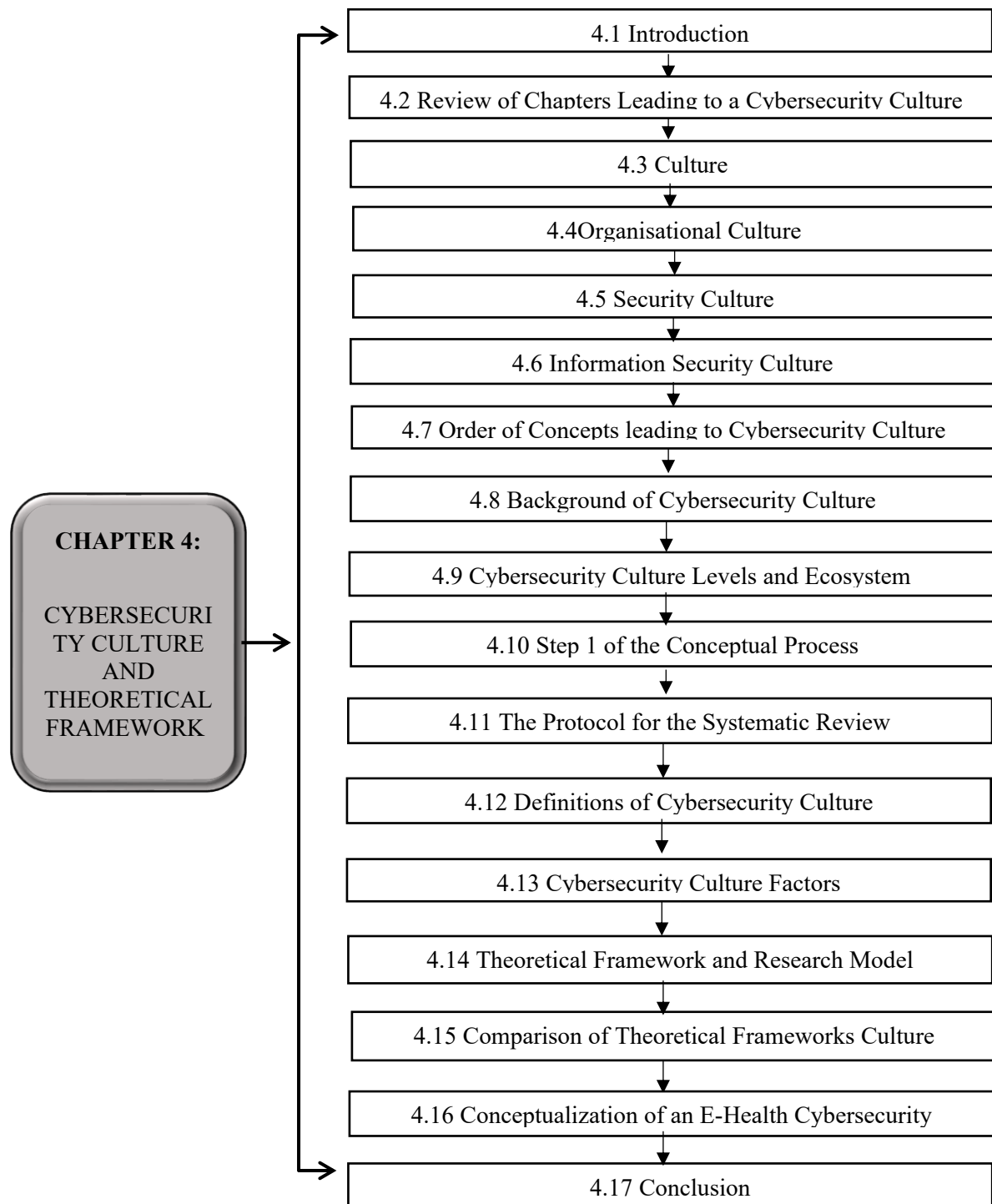
Predominant cybersecurity challenges identified included technological issues, lack of resources, human error, the prevalent security culture and emerging threats. The E-Health cybersecurity threats include data breaches, malware, ransomware, MEDJACK, spear phishing, insider threats, and Denial of Service.

Unauthorised access to critical healthcare data can have devastating consequences for patients and healthcare institutions. Therefore, Chapter 3 identified cyber threats that jeopardised the security of the E-Health institution’s information.

The chapter identified human/people issues and insider threats, which are closely related to each other, as the predominant cybersecurity challenges in the healthcare sector, which are almost always initiated by the actions of people. Insider threats were also identified as a major cause of data breaches in the healthcare sector.

Measures to strengthen cybersecurity show the need for a holistic view of cybersecurity. This view strives towards creating a culture of cybersecurity. Chapter 4 explores the literature on the concept of a cybersecurity culture.

CHAPTER 4: CYBERSECURITY CULTURE AND THEORETICAL FRAMEWORK



4.1 INTRODUCTION

Efforts focusing on cybersecurity from a technological perspective appear not to have been completely successful due to their lack of consideration of the human factor. Therefore, this chapter focuses on cybersecurity culture as part of a proposed measure for addressing cybersecurity challenges.

The chapter gives background information on the topic, security culture, and highlights the importance of cybersecurity culture. Using the systematic literature review protocol, which is described in more detail in the methodology chapter (Chapter 5), this chapter looks at cybersecurity culture definitions, lists of factors associated with cybersecurity culture, and constructs from an existing CCSCF to categorise cybersecurity culture factors. The constructs identified will be used to develop the CCSCF proposed in this study.

This chapter follows the first of the conceptual framework analysis phases followed in this study. The information about factors, concepts, and constructs gathered from the literature in this chapter will be integrated with the triangulation results of Chapters 6 and 7, leading to the development of the framework of cybersecurity culture for E-Health institutions. This chapter aims to address the following research questions:

Research Sub-Question 2 (RSQ 2):

- *What essential factors associated with cybersecurity culture are identified in existing literature that should be considered in developing a Cybersecurity Culture Framework for public E-Health institutions?*

Research Sub-Question 4 (RSQ 4):

- *What constructs from existing cybersecurity culture frameworks and other relevant frameworks can inform the design of a contextual Cybersecurity Culture Framework for public E-Health institutions?*

Section 4.2 presents a summary of the review chapters leading to this core chapter on cybersecurity culture. **Section 4.3** to **Section 4.6** presents the concept of culture, organisational culture, security culture, and information security culture. **Section 4.7** summarised the order of concepts leading to cybersecurity culture. Background of cybersecurity culture, including the cybersecurity culture levels and Ecosystem are discussed in **Sections 4.8** and **4.9**. Step 1 of the conceptual process is presented **Section 4.10** For the review protocol followed in

conducting the systematic review (see **Section 4.11**). The definitions and factors obtained from the cybersecurity culture literature are discussed (see **Sections 4.12 and 4.13**). The theoretical frameworks and research models are explained (see **Section 4.14**) and **Section 4.15** compares the theoretical frameworks. The conceptualisation of the E-Health cybersecurity culture components is discussed in **Section 4.16**, and the chapter is concluded in **Section 4.17**.

4.2 REVIEW OF CHAPTERS LEADING TO CYBERSECURITY CULTURE (CSC)

Figure 4.1 summarises the key factors identified in the initial literature review presented in Chapters 2 and 3. These form the basis for the examination of cybersecurity culture that follows in this chapter. Hence, this section summarises the preceding discussion on (1) the security threats of E-Health, and challenges that hamper cybersecurity in healthcare institutions and (2) prevalent threats and challenges in the institutions that form the basis for the direction of cybersecurity intervention in this research.

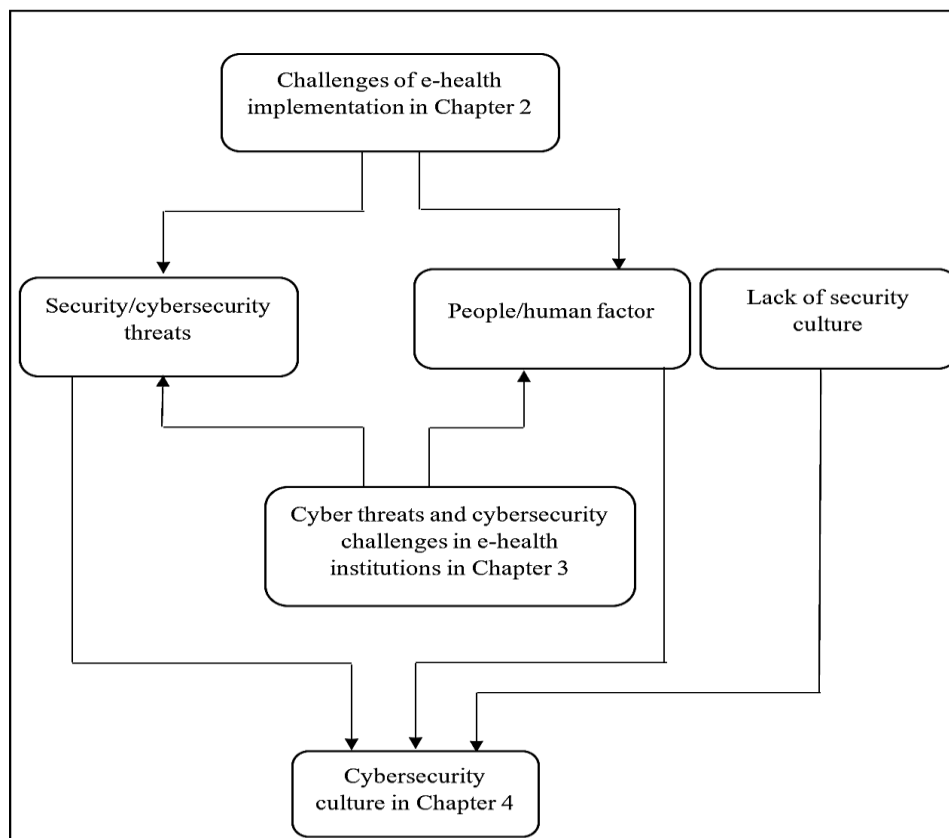


Figure 4.1: Issues Leading to the Introduction and Discussion of Cybersecurity Culture in Chapter 4 (own source)

Among the challenges confronting E-Health organisations (see Chapter 2), challenges related to the security of patient data (medical and non-medical) and human factor issues were

emphasised. These two main challenges formed the focus of this research, firstly because of the significance of patient data in this electronic age and the negative implications that compromising such data will have on the patient and organisation, and secondly, the importance of the relationship between security and humans.

Cybersecurity threats and challenges to healthcare institutions are expected to increase as more healthcare institutions, including hospitals, adopt and use a variety of healthcare technologies that are connected via the Internet or cyberspace to create an integrated E-Health system.

The significance of the term ‘integrated’ in the definition of E-Health (see Chapter 2) motivated the discussion on cybersecurity (see Chapter 3). On this basis, Chapter 3 investigated E-Health cyber threats and cybersecurity challenges.

Human-related security issues were identified as a reason that healthcare institutions are highly targeted by cyber-attacks. Similarly, links between this human issue and a lack of cybersecurity culture were highlighted as underlying cybersecurity challenges. Given the emphasis on the importance of taking the humans using E-Health into account and the limited amount of research on this topic, Chapter 4 focuses on cybersecurity culture.

E-Health institutions are troubled by people whose actions (be they malicious or non-malicious) are the source of cybersecurity problems (Bulgurcu et al., 2010). Human mistakes cause technical errors in the developed healthcare ICT systems, and the vulnerabilities caused by humans are taken advantage of by cyber-criminals (who are also human). Finally, the employees or management in the organisations frequently fail to develop or to adhere to cybersecurity protocols (both legislative and non-legislative), making it challenging to achieve cybersecurity.

This section briefly discusses threats and challenges related to the cybersecurity culture. As discussed more fully in Chapters 2 and 3, security threats and people-related problems are at the centre of E-Health and cybersecurity challenges. Additionally, the absence of a cybersecurity culture is one of the predominant cybersecurity challenges that confront healthcare organisations. It has been argued that creating a cybersecurity culture is an effective way to tackle these human problems. However, a poor or non-existent security culture has been found to be a frequent problem undermining cybersecurity in E-Health.

It is necessary that, before the specific concept of cybersecurity culture is discussed, the chapter explains the broad concepts of culture, organisational culture and security culture. The next section presents a discussion on culture.

4.3 CULTURE

Culture is an abstract concept, but a culture's influence is clearly evident in the attitudes and behaviours of people (Schein, 2004). Culture has been defined by a variety of researchers over time. Culture is the shared beliefs, assumptions, artefacts, symbols and behaviour of a group that defines the way the group operates (Schein, 2004, 2009). Culture is defined as people's way of life created over time, and it is reflected as evidence in people's behaviours (Schlienger & Teufel, 2003) and in characteristics such as values, beliefs, attitudes, habits, priorities, norms and social habits (Malmedal & Roislien, 2016).

It is "a set of shared attitudes, values, goals and practices that define an institution organisation" (Georgiadou et al., 2020a). Culture is seen as the rules that exist in people's social systems, which are used to change behaviour (Alvarez-Dionisi & Urrego-Baquero, 2019). According to Cameron and Quinn (2011) culture is people's way of life, which impacts the behaviour of both individuals and organisations at large (Cameron & Quinn, 2006).

From the above definitions, it is evident that culture involves groups of people. It has a bi-directional relationship with humans as culture is formed by a group of individuals in a given environment through their accumulated personality and character, and through shared norms and values, but in addition, culture forms, guides and constrains people's behaviour in a group (Schein, 2004). This behaviour can make an individual successful or unsuccessful in each environment. Therefore, Malmedal and Roislien (2016) argue that culture is only evident when loyalty and solidarity exist among the individuals that form a group.

As indicated previously, the issue relating to human behaviour regarding security has been identified as a serious cybersecurity challenge. A discussion of the concept of culture in this section indicates relevance and sets out to develop an understanding of the fundamental relationship between the concepts of culture and people (humans). Culture and people are important as they contribute to the argument underlying the proposals regarding cybersecurity culture in this study.

Creating a culture is fundamental to managing human factors, because culture plays a vital role in people's behaviours and attitudes (van Niekerk & von Solms, 2010). It has been established

that culture affects matters associated with security, including policies, governance and leadership (Ribeiro, 2019). Consequently, creating a security culture has been identified as an essential step towards managing and addressing human factor problems in cybersecurity (Holdsworth & Apeh, 2017; von Solms & van Niekerk, 2013).

Levels of culture: According to Schein (2004, 2010), three different levels exist at which culture can be analysed. These are the beliefs (which are the underlying assumption) that members of the organisation hold, and which form the basis of their shared actions; the values depicting what is considered important by the organisation members; and artefacts (attitude) representing the visible organisational structure, behaviour patterns and processes (Schein, 2004). These levels relate to people's nature, behaviour and beliefs.

Culture plays a significant role in organisations as it contributes to setting priorities and hence what it considers to be 'success' in various ways. For instance, culture can affect an organisation's decision-making related to security-related issues (Chen & Farkas, 2009). It can help in making predictions regarding employees' attitudes on security and privacy-related issues (Halevi et al., 2016). Hence, culture is an underlying and broad notion related to organisational culture.

Exceptional organisations are those that create and maintain a culture of engagement and motivation in the organisation (Deloitte, 2012). The same can be expected to be the case with cybersecurity. Organisations that cultivate a strong cybersecurity culture should be successful in achieving cybersecurity within their organisations. Huang and Pearlson (2019) argue that examining the overall culture of an organisation and its subcultures provides the basis for cybersecurity culture.

Different manifestations of culture include organisational culture, national culture and ethnic culture. The focus of this study is on cybersecurity culture which is a concept that is related to security culture and information security culture. Organisational culture and its subcultures, security culture and information security culture are discussed in **Sections 4.4 to 4.6**, before cybersecurity culture is discussed.

4.4 ORGANISATIONAL CULTURE

In the organisational context, the term organisational culture (OC) specifically refers to the wider concept of culture. As it is evident that culture revolves around people, people should also be considered crucial elements of organisational culture. Corradini (2020) defines OC as

the “collection of people’s ideas, beliefs, behaviours and other elements that ensure the survival of the organisation”.

Therefore, the definition of culture can contribute useful concepts to the definition of organisational culture. Schein’s definition has been widely accepted and adopted as a foundation for definitions of OC (Corradini, 2020; Da Veiga, 2008). Hence, OC has been defined as “a pattern of shared basic assumptions that the group has learned as it tries to solve its problems of external adaptation and internal integration, and that worked well enough to be considered valid, and therefore, to be taught to new members as the correct way to perceive, think and feel in relation to these problems” (Schein, 2004). In a nutshell, the simplest definition of OC is “the way we do things around here” (Lundy & Cowling, 1996).

Notwithstanding the abstract nature of culture, its consequence affects individual and organisational behaviours (Cameron & Quinn, 2006). Some critical roles OC plays within the organisation include: encouraging cooperation among organisation members, defining organisational identity, establishing strategies and goals, and shaping behaviour and attitudes (Corradini, 2020). A strong OC is important, and it is closely associated with successful organisations across the globe (Corradini, 2020).

Layers of organisational culture: The three levels of culture explain the fundamental assumptions, values and artefacts, which are considered the components of culture. These have been used as three core layers in the conceptualisation of OC. Schein’s model of OC also depicts three further levels related to artefacts; these are the visible level, the value depicted at the middle level, and the fundamental assumptions at the deepest level. This can be equated to the metaphor of an iceberg, which has also been used to describe OC.

The visible elements of OC equate to the level of the iceberg visible above the surface. These elements are the tangible aspects of the organisation, for instance, the physical environment, ICT equipment used by employees, as well as behaviours displayed by individual members of the organisation (Schein, 2004, 2010).

The ‘non-visible’ elements of the organisations are found at the middle and lowest iceberg level and include values and basic assumptions. The middle level contains those particular elements in the organisation that improve people's sense of belonging; these are beliefs and norms (Corradini, 2020). The deepest level elements, called fundamental or basic assumptions, are those that constitute the innermost understanding of the essential aspects of the OC. These

untold beliefs are often taken for granted in the organisation, but are the true representation of OC (Schein, 2004, 2010).

In addition, subcultures that have a narrower scope can coexist alongside the main organisational culture. This should not be perceived negatively, because subcultures that are consistent with the leading culture can reinforce it (Corradini, 2020). The subcultures of OC include the security culture.

4.5 SECURITY CULTURE

Security culture is defined as “the unconscious manner in which things are done in the organisation to secure information” (Da Veiga, 2019). It is a culture within the OC, that is, it is a subculture (Da Veiga & Martins, 2017; Schlienger & Teufel, 2003). Therefore, Da Veiga (2019) argue that to understand what influences underlie the security culture, reference should be made to the development of OC, which is rooted in the strategy and mission of the organisation.

A strong security culture is considered to be a behavioural control measure that can be applied to address human-related challenges facing the protection of information (Alhogail, 2015; ENISA, 2017). A really strong security culture is only achieved in situations where information is safeguarded throughout its lifecycle, regardless of its use (Da Veiga & Martins, 2015a)

The term is sometimes used to include both information security culture and cybersecurity culture. At other times, the term is used interchangeably with information security culture; hence, it is explained as the manner in which things are done in the organisation to secure information (Da Veiga, 2019).

The view held in this research is that cybersecurity culture is an umbrella term that includes practices related to other security areas like information security, IT security and operational security. Therefore, cybersecurity culture is used to refer to a culture of security that can exist within and outside a given context. A security culture that exists within an organisational setting is referred to as an information security culture, and a security culture that can exist within an organisational context but extends beyond is referred to as a cybersecurity culture.

The topic of information security culture is explored in **Section 4.6** before the research attention on the cybersecurity culture in **Section 4.8**.

4.6 INFORMATION SECURITY CULTURE

In Chapter 3, it was explained that the term information security (which focuses on organisational security) is not used interchangeably with cybersecurity in this research. Rather, the research maintains the view that cybersecurity is a broader concept that extends beyond the organisational context.

The same applies to the concepts ‘information security culture’ and ‘cybersecurity culture’. Although knowledge of information security culture is important to enhance an understanding of cybersecurity culture, a fundamental difference exists between the two concepts (Huang & Pearlson, 2019). Information security culture emphasises “behaviours that comply with information security policy”, while cybersecurity culture focuses on both policy compliance and also “personal involvement in organisational cyber safety” (Huang & Pearlson, 2019).

An information security culture is defined as “the attitudes, assumptions, beliefs, values and knowledge that employees or stakeholders use to interact with the organisation’s systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour (that is, incidents) evident in artefacts and creations that become part of the way things are done in an organisation to protect its information assets. This information security culture changes over time.” (Da Veiga, 2008: 25).

As information security culture is a subculture of security within the dominant OC, it is widely accepted that the layers of OC form the basis of most information security culture frameworks and models (Reegård et al., 2019; Reid & van Niekerk, 2014a; van Niekerk & von Solms, 2010). And it is reasonable that the same should be the case with a CCSCF (Reegård et al., 2019). However, since this study viewed cybersecurity as a broad concept that encompasses information security and other security, the layers of OC did not form the foundation of the CCSCF proposed in this study.

The discussions provided in **Sections 4.3 to 4.6** assist in an understanding of phenomena related to the concept of a cybersecurity culture. This helps to show the relevance of the cybersecurity culture proposed in this study as a holistic measure to address the human-related cybersecurity problem. The attention is now turned to the concept ‘Cybersecurity Culture’.

4.7 ORDER OF CONCEPTS LEADING TO CYBERSECURITY CULTURE

Figure 4.2 summarises the logical order of concepts leading to the phenomena of cybersecurity culture in this research.

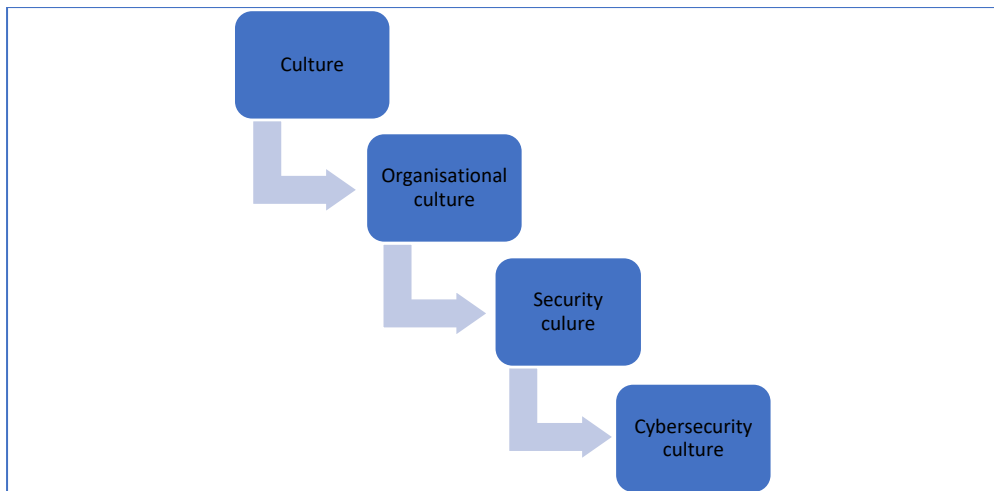


Figure 4.2: Logical Order Leading to the Domain of Cybersecurity Culture (Own source)

It is necessary to change human behaviours as a way to address human factor challenges, and it has been identified that an effective way to facilitate behaviour change is through influencing the culture within which they live. The culture that is established within the organisation can significantly influence performance because it includes many factors that shape human behaviour. Hence, it is important that culture be a positive influence. Culture plays an important role in achieving success within an organisation, as it can help the organisation to obtain the best performance from each individual. This leads to the concept of OC, which is considered an overall culture with security culture as a component. OC's influence on security is significant as it plays a role in protecting the organisation's assets. Security culture contributes substantially by shaping the security posture and behaviour of the organisation and includes both information security culture and cybersecurity culture.

Considering this, it is essential for organisations to invest in the cultivation of their security culture. This research, therefore, focuses on cybersecurity culture. The attention will now turn to the concept of 'Cybersecurity Culture'.

4.8 BACKGROUND OF CYBERSECURITY CULTURE

There is a need for more research to address the pressing problems of cybersecurity facing organisations and nations (Wybourne et al., 2009). The observations already made regarding the human factor have resulted in recommendations to extend this research to apply the human approach and cybersecurity culture to cybersecurity (Gcaza et al., 2015). Research has found that cultivating a security culture among users is the most feasible way to minimise cybersecurity problems (Furnell & Thomson, 2009; Reid & Van Niekerk, 2014a).

This recommendation is also applicable in healthcare, where cybersecurity culture has been identified as one of the independent variables in establishing security effectiveness in health information systems (Shahri et al., 2013). In the absence of a strong security culture, people may be aware of existing and likely threats, but still fail to act appropriately (Shahri et al., 2013). Branley-Bell et al. (2021) argue that developing such a culture in healthcare environments can eradicate noncompliance with security policy and reduce cyber threats arising from behavioural factors.

Since security culture has been identified as being helpful in addressing human factors, information security culture research has become established as a viable approach to reducing the impact of inappropriate human behaviour affecting information security in the organisational context (Alhogail, 2015; Alhogail & Mirza, 2014; Da Veiga & Martins, 2015a, 2015b; Hassan et al., 2017; Schlienger & Teufel, 2002; Thomson et al., 2006). However, given the widespread use of interconnected technologies and the impact of the 4th Industrial Revolution (4IR) in expanding the physical area from which the organisation's employees and users (clients, customers, etc.) operate, security threats have also increased. Under these circumstances, the information security culture, which focuses on a narrow organisational context, falls short in addressing cybersecurity threats and challenges. Hence, the cultivation of a cybersecurity culture is now receiving greater attention as a form of security culture that extends beyond the organisational context (Huang & Pearlson, 2019; Reid & Van Niekerk, 2014a).

The move to Cyber-Physical Systems (CPS) intensifies the importance of cultivating and maintaining a positive, meaningful and easy to comply with cybersecurity culture in organisations. The value of such a culture has also been emphasised as a way to protect employees from both unintentional errors and malicious attacks (Metalidou et al., 2014). As is the case with information security culture, cybersecurity culture has been emphasised as a human-centred approach to the security of information and other assets in cyberspace (Gcaza, et al., 2017).

However, research efforts in the area of human factors have mostly focused on information security and information security culture rather than cybersecurity (Alhogail, 2015; Da Veiga & Eloff, 2010; Da Veiga & Martins, 2015a, 2015b; Hassan et al., 2017; Schlienger & Teufel, 2002; Thomson et al., 2006). Since cybersecurity culture has had little attention, the concept

and its delineating elements are considered to be ill-defined (Gcaza et al., 2017; Gcaza & von Solms, 2017b).

It has become clear that technological solutions alone are unable to achieve cybersecurity, just as technical and procedural controls by themselves were not sufficient to address information security (Gcaza et al., 2017). This is due to them overlooking the human aspects. This has also led to recommendations that awareness of security be established at different levels (international, national, organisational and individual) to achieve a full cybersecurity culture (Da Veiga, 2016).

Understanding the factors that influence and shape the security behaviour of people as they operate in cyberspace, and the associated cybersecurity culture, has become crucial in cybersecurity research. The security chain needs to realise the importance of the human factor in achieving an acceptable cybersecurity level; the cybersecurity process needs to be re-shaped, paying greater attention to human-related issues rather than merely relying on technical controls (Gcaza et al., 2017; Holdsworth & Apeh, 2017).

It is, therefore, not surprising that cultivating a culture of cybersecurity is considered to be an important approach to use when attempting to resolve cybersecurity challenges (Gcaza & von Solms, 2017a; Leenen & Van Vuuren, 2019). Building a cybersecurity culture helps create the human characteristics, values, attitudes and beliefs that shape good cybersecurity behaviours (Marotta & Pearlson, 2019).

In addition to formulating technological solutions for addressing cybersecurity challenges, research has indicated that cultivating a cybersecurity culture contributes meaningfully by addressing human factor problems in cybersecurity (ENISA, 2017; Gcaza et al., 2015; Gcaza & von Solms, 2017b; Holdsworth & Apeh, 2017; Leenen et al., 2018; Leenen & Van Vuuren, 2019; van Niekerk & von Solms, 2010).

4.8.1 CYBERSECURITY CULTURE

Based on the identified challenge. referred to as the human factor, the view in this thesis is that cybersecurity challenges cannot be eradicated by applying technological solutions alone. Therefore, the need for a cybersecurity culture emerged in this study. This study was prompted to employ 'Cybersecurity Culture' as a measure that can help address human factor problems in E-Health.

The fact that research on cybersecurity is beginning to move from a technical approach to a more social-cultural approach supports this decision (Bounas et al., 2020; Da Veiga & Martins, 2015a; ENISA, 2017). Emerging research emphasises the importance of a cybersecurity culture as an essential approach when addressing cybersecurity challenges (Abeyratne, 2016; Bounas et al., 2020; Clark et al., 2017; Corradini, 2020; Saigushev et al., 2020). This is particularly true for challenges emanating from human issues and factors (Gcaza & von Solms, 2017b; Ioannou et al., 2019; Leenen et al., 2018).

Additionally, cybersecurity culture is viewed as a holistic and broad approach that helps address human challenges, while at the same time encouraging the adoption of technological solutions (Alshaikh, 2020; ENISA, 2017; Holdsworth & Apeh, 2017). Therefore, cybersecurity culture research helps bridge the gap between the technical and social-cultural approaches by incorporating elements of both (Bounas et al., 2020). In this research, a perspective that combines aspects of both the personal culture of individual users of E-Health and the organisational security culture of the organisation providing E-Health services is also espoused.

4.8.2 IMPORTANCE OF CYBERSECURITY CULTURE

The importance of cybersecurity culture as a research area is rapidly being recognised. This section discusses the various foci that have been highlighted as important to cybersecurity culture research.

4.8.2.1 A Measure to Counter the Cybersecurity Challenge

Research has argued that promoting, monitoring and making employees aware of the cybersecurity culture within an organisation can contribute immensely towards achieving compliance with cybersecurity policies and regulations (Da Veiga & Martins, 2015a; Holdsworth & Apeh, 2017). Researchers in the area of information and cybersecurity argue that encouraging a cybersecurity culture is one of the best ways to defend and secure organisations against cyber-attacks (Bounas et al., 2020; Ciuperca et al., 2019; Gcaza et al., 2015; International Telecommunication Union (ITU), 2008a).

The ITU considers the presence of a cybersecurity culture as making the most significant contribution to cybersecurity efforts. Supporting this sentiment, researchers argue that the challenges of cybersecurity cannot be addressed unless negligent human behaviour towards security is changed by introducing a new security culture (Corradini, 2020; Holdsworth &

Apeh, 2017). Saigushev et al. (2020) emphasise that an organisation's cybersecurity culture creates a long-term countermeasure that can protect the organisation against both existing and new kinds of cyber-attacks.

The importance of a cybersecurity culture can never be overemphasised. The content analysis conducted by Gcaza and von Solms (2017b) re-affirms the importance of a cybersecurity culture, as all the sources included in the analysis clearly show the importance of cultivating a such a culture as a measure for achieving cybersecurity.

Cybersecurity culture has been recommended and employed as an approach in many business sectors, including finance, education, aviation, military and drinking water utilities, as a way to combat cybersecurity challenges caused by human elements (Abeyratne, 2016; Clark et al., 2017; Da Veiga, 2016; Leenen & Van Vuuren, 2019). In short, developing a cybersecurity culture can be described as a necessary framework for implementing a strong defence programme (Clark et al., 2017).

4.8.2.2 Change of Human Behaviour

Investing in the development of the cybersecurity culture has become an essential part of changing employees' attitudes and perceptions and in building good security behaviours (Da Veiga et al., 2020; Wiley et al., 2020). A cybersecurity culture is key to changing users' behaviours and encouraging positive attitudes towards security (Gcaza et al., 2017).

Instead of being seen as an effort to constrain conduct, the creation and strengthening of cybersecurity culture helps to empower people by helping them achieve a better security outlook, build security mindfulness, reflect on security threats and maintain a uniform culture across all levels of a hierarchy in an organisation or a nation (Ioannou et al., 2019).

A strong cybersecurity culture brings about other positive results as well, such as enhancing efficiencies, improving security, alleviating financial risks, creating a mindset of change in the organisation, providing competitive advantage, and ultimately helping to achieve cybersecurity culture awareness throughout the organisation (ENISA, 2017; Phillips & Tanner, 2019). Encouraging the development of cybersecurity highlights attributes like honesty and willingness to disclose problems (ENISA, 2017; Phillips & Tanner, 2019).

4.8.2.3 Empower People and Support National Cybersecurity

The importance of cybersecurity culture has been formally acknowledged by different countries (Luijff et al., 2013). This is highlighted by the addition of cybersecurity culture as one of the strategic objectives in the countries' cybersecurity strategies (Luijff et al., 2013). Cybersecurity culture has been recognised as an important response and countermeasure to challenges resulting from human factor issues in a cybersecurity environment (Gcaza et al., 2017; International Telecommunication Union (ITU), 2008a; van Niekerk & von Solms, 2010).

According to ISACA (Alvarez-Dionisi & Urrego-Baquero, 2019), a cybersecurity culture is important because it helps:

- empower people with skills (including sociological and psychological skills) required to use cybersecurity technology and follow processes;
- highlight the true meaning of cybersecurity by ensuring a genuine understanding of the three pillars of cybersecurity culture (people, technology and processes);
- define and establish partnership and strengthen collaboration with stakeholders and other role players (employees, managers, government agencies, senior executives, boards of directors, technology providers, consultants, and educators and trainers); and
- provide appropriate education and training programmes that cover the three domains of cybersecurity.

The ITU has identified the creation of a cybersecurity culture as a vital approach to cybersecurity. As a result, there has been growing importance attached to establishing a national cybersecurity culture to support national cybersecurity strategies (Ghernouti-Hélie, 2010; State Security Agency, 2015). Many developed countries, like the United States and the United Kingdom, have started encouraging the development of a cybersecurity culture among their citizens (Kortjan & von Solms, 2014).

In South Africa, the importance of a cybersecurity culture to enhance national security has been acknowledged. This is evident in the development and approval of the National Cybersecurity Policy Framework (NCPF) (State Security Agency, 2015). The purpose of culture, according to the NCPF, is to deal with cybersecurity in society and in the private and public sectors. Government and civil society need to actively strive for the achievement of a cybersecurity culture in South Africa.

Romania's national strategy on cybersecurity also stresses the importance of developing a cybersecurity culture for computer users as a proactive measure to improve cybersecurity (Government decision 271/2013 as cited in Loică, 2017).

Although the need for and importance of the topic 'Cybersecurity Culture' are acknowledged in research (see Sections 5.3.1 and 5.4.1), in the past, no standard solutions have existed for cultivating such a culture. However, this is gradually changing as guidelines, recommendations and frameworks for the development of a cybersecurity culture begin to emerge (ENISA, 2017; Kortjan & von Solms, 2014; Leenen & Van Vuuren, 2019; Malyuk & Miloslavskaya, 2016; Organisation for Economic Co-operation and Development (OECD), 2005, 2015, 2021). However, although these exist, specific research conducted has mainly focused on developing a national cybersecurity culture (Gcaza, 2017; Gcaza & von Solms, 2017a; Malmedal & Roislien, 2016). The emphasis of that research has been on defining the cybersecurity culture domain (Gcaza, 2017; Gcaza et al., 2015; Gcaza & von Solms, 2017b).

As research extends to other levels of cybersecurity culture, work done at the organisation level regarding establishing an organisational cybersecurity culture has predominantly focused on finance and banking institutions, and military organisations (Da Veiga, 2016; Leenen et al., 2018; Leenen & Van Vuuren, 2019; Marotta & Pearlson, 2019). Limited attention has been paid to establishing a cybersecurity culture in E-Health at the organisational level. As discussed in Chapter 1, this creates an opportunity for this study to fill the gap by specifically investigating the cybersecurity culture in E-Health organisations. Therefore, the proposal was to address the human-related problems in achieving cybersecurity in E-Health organisations by cultivating a cybersecurity culture.

4.9 CYBERSECURITY CULTURE LEVELS AND ECOSYSTEM

Unlike information security culture, which is argued to exist only at the organisational level, cybersecurity culture extends beyond the organisational level (Reid & van Niekerk, 2014a). According to Da Veiga (2016), cybersecurity culture includes individuals at work, in private environments, and in national and international contexts. Gupta and Bajramovic (2017) classify security culture roles and responsibilities into three main components: the role of the state, the organisation, and that of individuals. This means that cybersecurity culture can be achieved at the organisational level and at other levels. **Figure 4.3** depicts the four cybersecurity culture levels (Da Veiga, 2016).

Da Veiga (2016) argues that cybersecurity culture should be viewed from the top down. Starting from the top, cybersecurity culture at the international level encompasses devices and people that are globally connected; national cybersecurity culture levels include the security effort of a country in protecting its critical infrastructure; the bottom level of cybersecurity culture includes organisational and individual cybersecurity culture (Da Veiga, 2016). However, looking at **Figure 4.3**, one can argue that to achieve a cybersecurity culture globally, efforts must start at the lower levels, namely, the individual and organisational levels.

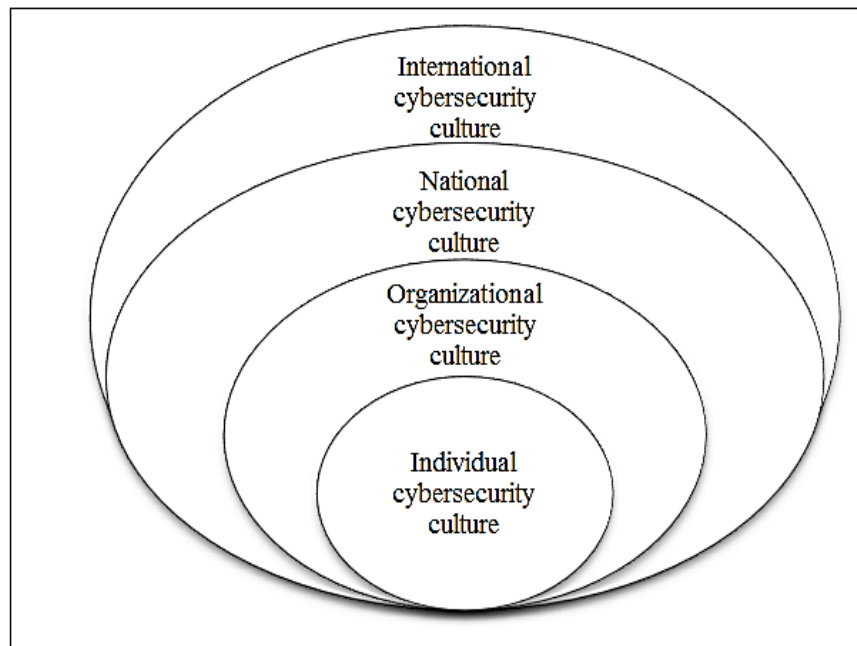


Figure 4.3: Cybersecurity Culture Levels (Da Veiga, 2016)

Based on this, the focus of this research is on achieving a cybersecurity culture at the lower levels, with specific attention being on E-Health organisations and their individual providers and users of E-Health.

Organisational cybersecurity culture is defined as “the beliefs, values, and attitudes in the organisation that drive cyber-secure behaviours. These beliefs, values and attitudes are influenced by both external factors outside the organisation and by mechanisms and actions managers can take inside the organisation” (Huang & Pearlson, 2019). Organisational cybersecurity culture plays an essential role in efforts to secure the organisation’s critical infrastructure and information from cyber threats, for example, in E-Health organisations, which are data sensitive (Leenen & Van Vuuren, 2019). Implementing a cybersecurity culture at the organisational level positions organisations to be proactive rather than reactive in dealing with the cyber threats that confront them (Mills, 2018).

Regardless of the cybersecurity culture level that is implemented, the cybersecurity ecosystem must support the three pillars of cybersecurity (people, technology and process). Alvarez-Dionisi and Urrego-Baquero (2019) depict the cybersecurity ecosystem as having foundations made up of seven blocks representing knowledge, beliefs, perceptions, attitudes, assumptions, norms and values. These foundations support the pillars of cybersecurity, and hence provide a social-psychological environment capable of supporting cybersecurity (Alvarez-Dionisi & Urrego-Baquero, 2019). Together, the cybersecurity pillars and building blocks make up the ecosystem of cybersecurity culture (see **Figure 4.4**).

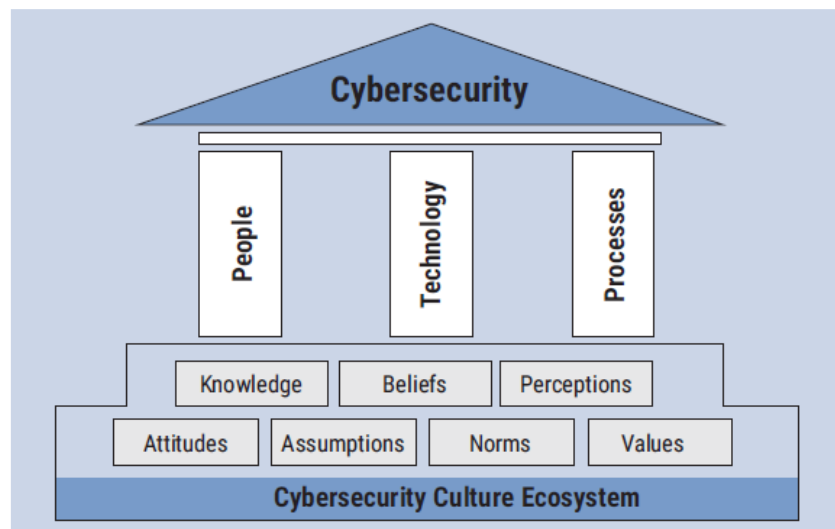


Figure 4.4: Cybersecurity Culture Ecosystem (Adapted from Alvarez-Dionisi & Urrego-Baquero, 2019)

Section 4.10 outlines the phases achieved in the conceptual process adopted as the framework design and development technique for developing cybersecurity culture.

4.10 STEP 1 OF THE CONCEPTUAL PROCESS

A systematic literature review method was followed to achieve the objectives of this chapter, which were: firstly, to identify factors associated with cybersecurity culture in the literature and secondly to identify components from the existing cybersecurity culture frameworks and other frameworks that can stimulate the cultivation of cybersecurity culture in public E-Health institutions. Conducting a systematic literature review in this chapter, the researcher used the first three phases of Jabareen's (2009) framework technique. The strategies followed in the study to achieve these phases and the associated conceptual processes to identify cybersecurity culture factors in developing the proposed contextual framework included using interviews and

questionnaires. **Figure 4.5** shows that Chapter 4 reports on Step 1, which covered the first three phases of the conceptual framework.

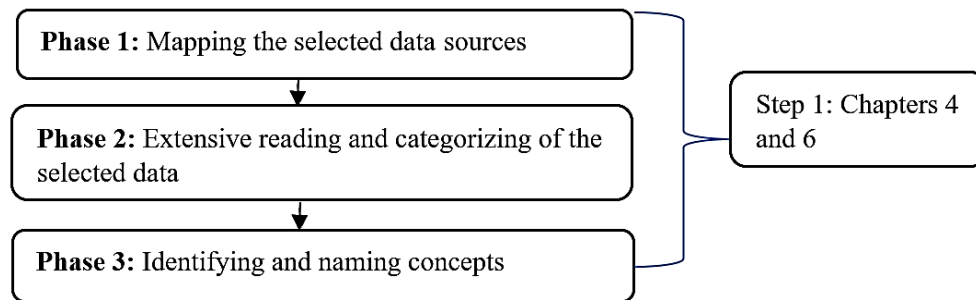


Figure 4.5: Step 1 and Phases 1-3 of the Adapted Conceptual Framework Technique (Adapted from Jabareen, 2009)

The following **Section 4.11** outlines the review protocol steps presented in Chapter 5 to detail how the Xiao and Watson's (2019) review steps (3 - 7) were carried out in this study.

4.11 THE PROTOCOL FOR THE SYSTEMATIC REVIEW

The systematic literature review steps followed to achieve the objectives of this chapter are discussed in detail in Chapter 5. The section presents the phases of the step applied and the outcomes achieved in the step.

The end of this section provides the cybersecurity culture factors identified and the related constructs that contributed to developing cybersecurity culture instruments for data collection and cultivation of cybersecurity culture in E-Health organisations.

4.11.1 SEARCH STRATEGY

Cybersecurity is a broad and multi-disciplinary research area that can be in any organisational sector. To ensure a rigorous search for the systematic review of cybersecurity culture, the literature search included both computing and non-computing databases and focused mainly on peer-reviewed academic publications. However, a few non-academic publications were also included to accommodate industry, business and expert writing on the topic of cybersecurity culture.

Searching the literature achieved the first phase of the conceptual framework, followed by the design and development of cybersecurity culture in the public E-Health institution. The keywords were used to search the titles, abstracts, and keywords of articles. The keywords were utilised to achieve the first phase of the conceptual framework and helped the researcher to

discover the most pertinent and adequate literature pertaining to the cybersecurity culture. Additionally, the keywords obtained research materials that would be interesting for future reading. The search was conducted between December 2020 and March 2021. The lists of keywords used to search the literature are given in **Section 5.5.2**.

An alert was also set on the keywords after completing the initial search to identify important literature published after the search and during the review process. This additional literature was added during the review stage.

The search engines used included the University of South Africa (UNISA) e-reserve, Google Scholar, and normal Google to find the pertinent materials and peer-reviewed literature, and these search engines were used to identify the selected data source. **Figure 4.6** depicts the databases searched by UNISA e-reserve, Google Scholar and normal Google, together with the number of records retrieved.

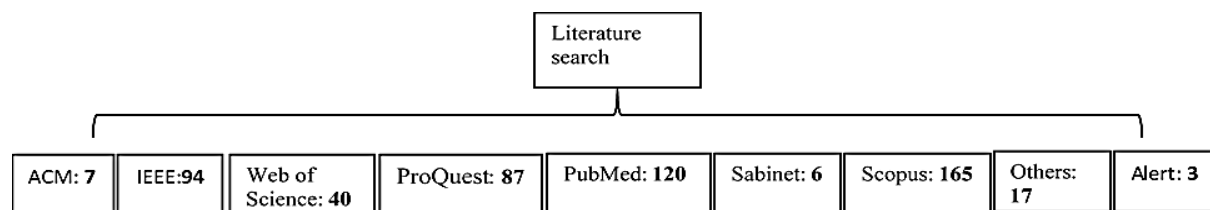


Figure 4.6: Search Database for the First Phase (own source)

To ensure an appropriate data selection process, the retrieved articles were emailed to the researcher or downloaded and saved on the researcher's computer. The researcher then went through the records to remove 39 duplicates. Upon review of the titles and abstracts, a further 423 records were removed because they were either irrelevant or simply editor's notes. Seventy-seven articles were taken in for full-text review. From these 77 records, 19 records were subsequently dropped when the following three further assessment criteria were applied. (a) Was cybersecurity culture the focus of the research, or was the concept only mentioned in passing? (b) Did the study either not consider information security culture, or was the term used interchangeably with cybersecurity culture? (c) Did the study define or discuss factors of cybersecurity culture? Eventually, 58 records were deemed relevant in the review, and to help answer **Research Sub-Question 2 (RSQ 2)** to identify factors that were associated with cybersecurity culture. These 58 records formed part of the data selection source for the first phase of the conceptual framework.

Articles included in the review extend beyond journal and conference publications. This is because cybersecurity culture is considered to be ill-defined. The inclusion criteria were supported by an additional three more explicit assessment criteria:

- a) The year range (between 2010 and 2021)
- b) Only English publications
- c) Publication in the form of journal articles, conference proceedings, policy documents, book chapters and theses
- d) Predominantly cybersecurity culture studies

Cybersecurity culture and E-Health related technologies have evolved rapidly in recent years. The selection of this time range ensured the inclusion of only current cybersecurity culture work to maintain relevance with recent advancements in healthcare cybersecurity culture. Additionally, limiting the papers selected to English publications helped the researcher to avoid the problem of misinterpretation. As a broad and multi-disciplinary research area, widening the publication scope added to the authenticity of the review. In addition, applying the assessment criteria noted above helped to focus the systematic review only on cybersecurity culture so that it did not follow the example of other reviews that used the terms ‘information security’ and ‘cybersecurity culture’ interchangeably. By including cybersecurity culture work occurring at each of the four levels (individual, organisation, national, and international), the review explicitly recognised that the concept was multi-dimensional and could be influenced at various levels.

Figure 4.7 depicts the PRISMA method summarising the inclusion and exclusion process.

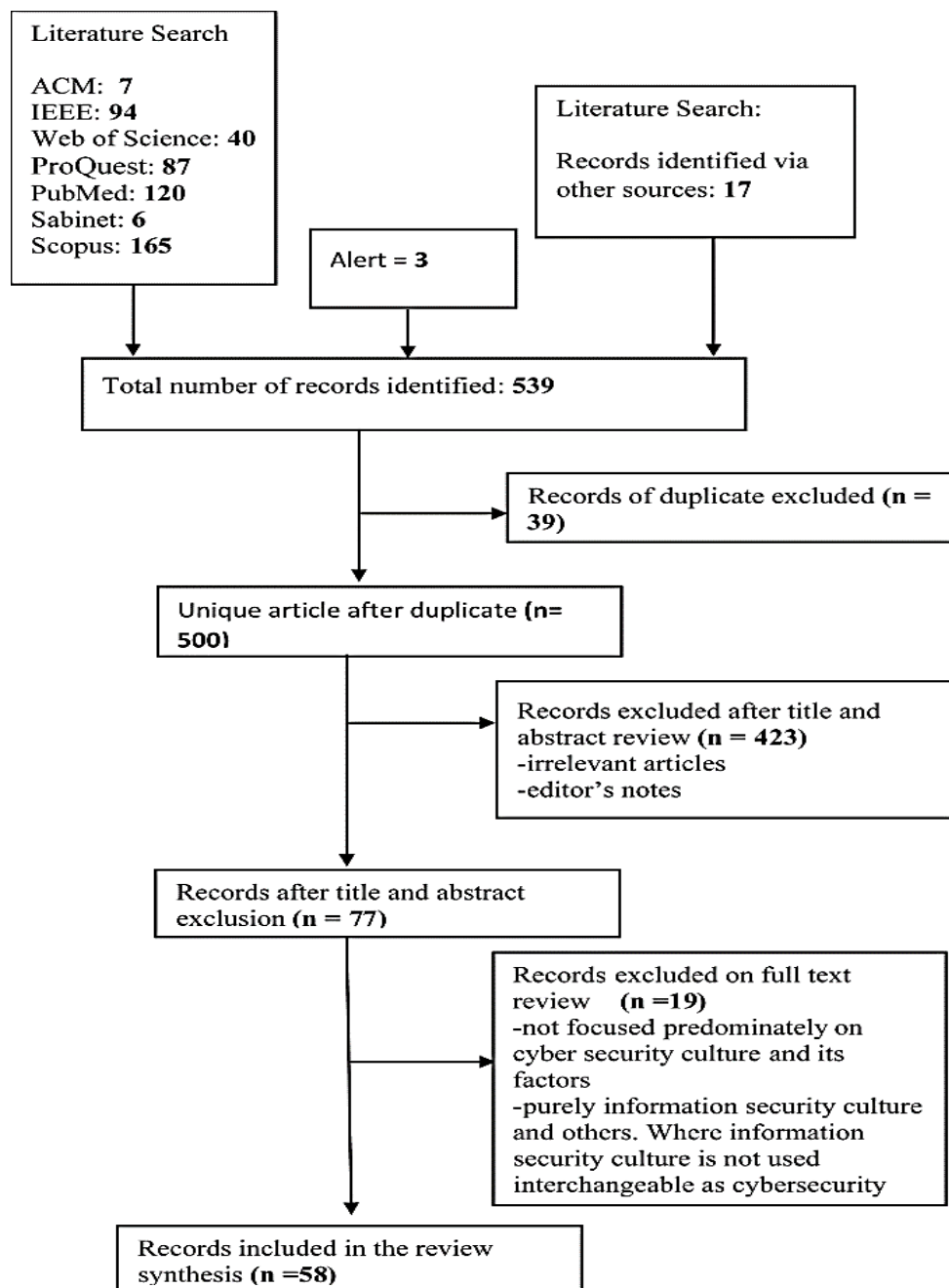


Figure 4.7: PRISMA Method for the Inclusion and Exclusion of the First Phase (Moher et al., 2009)

4.11.2 DATA EXTRACTION

This stage was the start of the second phase of the conceptual framework analysis process adopted for the design and development of the E-Health CCSCF. Phase 2 began with a quality evaluation overview of the data selected in Phase 1. In this phase, it was discovered that data

extracted for the review for the identification of concepts and factors of cybersecurity culture included:

- publications whose titles focused predominantly on cybersecurity culture and with publication dates within the past 12 years;
- mostly journal and conference articles, with only a few other exceptional reports, websites and theses that focused specifically on or had a section dedicated to cybersecurity culture;
- studies conducted in different sectors (healthcare, finance, education, military) across different countries (South Africa, Australia, and America); and
- were published in different countries.

The review focused on extracting data associated with cybersecurity culture as a solution to human factor problems in cybersecurity. It was also discovered that the extracted data included data on:

- Definitions and descriptions of cybersecurity's culture;
- Factors that were fundamental for the development of cybersecurity culture; and
- Different existing frameworks on cybersecurity culture.

4.11.3 REPORTING THE FINDINGS OF THE REVIEW

The second and third phases of the conceptual framework processes were covered by reporting on the findings from the data selected in the first phase. This was done by carefully reading the selected data (second phase). Important elements of cybersecurity culture in the definition and existing framework, and factors associated with the cybersecurity culture were identified and named (third phase). **Sections 4.12** and **4.13** provide the findings of the review on the cybersecurity culture definition, factors, and cybersecurity culture frameworks.

As discussed in Chapter 5, a thematic synthesis approach was followed in the identification and naming of the cybersecurity culture factors. Using ATLAS.ti, some segments of the study were coded. Themes emerging from the codes were obtained by examining the introduction, results, findings, and conclusions of individual studies. These were compared, and meaningful differences were identified, while at the same time remaining close to the text of the primary studies.

Thematic synthesis was followed because through this approach, the researcher was able to integrate the results of many studies on cybersecurity culture and obtain insights on: Important elements of cybersecurity culture (obtained from cybersecurity culture definitions); factors of Cybersecurity Culture; and critical concepts of cybersecurity culture (obtained from existing frameworks). The researcher was able to consolidate the elements from the definition with concepts from the framework.

4.12 DEFINITIONS OF CYBERSECURITY CULTURE

The second phase of the conceptual framework was achieved by carefully reading through the 58 articles and categorising the selected data. From this, it was found that a total of 26 studies contained some form of cybersecurity culture definition. This was the data from which the initial concepts of cybersecurity culture were obtained. In these studies, nearly half of the cybersecurity culture definitions adopted or re-emphasised the definitions of other authors (Aiken, 2019; Alshaikh, 2020; Alvarez-Dionisi & Urrego-Baquero, 2019; Bounas et al., 2020; Corradini, 2020; Da Veiga, 2019; Gundu et al., 2019; Ioannou et al., 2019; Leenen et al., 2018; Leenen & Van Vuuren, 2019; Ogden, 2021; Uchendu et al., 2021).

Among the authors listed above, only a few focused their studies on cybersecurity culture, but credibly replicated definitions of information security culture as being synonymous with cybersecurity culture (Alshaikh, 2020; Gundu et al., 2019; Ioannou et al., 2019; Ogden, 2021). The study by Ioannou et al. (2019) defined cybersecurity culture while also adopting the information security culture definition.

The studies that used information security culture definitions to synonymously define cybersecurity culture have been excluded from the list of cybersecurity culture definitions reviewed in the study. This is because, in this study, cybersecurity culture is considered to be a broad concept that contains information. Therefore, definitions that treat cybersecurity culture as information security culture are treated as incomplete.

The remaining 14 studies came up with unique definitions or explanations of cybersecurity culture (Abeyratne, 2016; Ciuperca et al., 2019; Da Veiga, 2019, 2016; ENISA, 2017; Georgiadou et al., 2020a; Huang & Pearlson, 2019; Ioannou et al., 2019; Leenen & van Vuuren, 2019; Malmedal & Roislien, 2016; Paul & Porche, 2011; Reid & van Niekerk, 2014a; Saigushev et al., 2020; Sousane, 2018). In most of the studies that specifically defined, described or conceptualised cybersecurity culture, the definitions had foundations either in an existing definition or background description of organisational culture, information security

culture or security culture (Da Veiga, 2016; ENISA, 2017; Paul & Porche, 2011; Reid & van Niekerk, 2014a).

Table 4.1 depicts the studies with their corresponding cybersecurity culture definitions.

Table 4.1: Cybersecurity Culture Definitions

Reference	Formal cybersecurity culture Definitions or Description
(Abeyratne, 2016)	“cybersecurity culture - the commitment of people to protecting their organisation. This means a critical part of the cybersecurity programme must be to focus on the human aspects of the organisation - on developing a positive security culture that is grounded in employees’ attitudes, evident in the behaviours people exhibit and which is reinforced by the actions of the leadership”
(Ciuperca et al., 2019)	“cybersecurity culture is a mix of knowledge, skills, values, and ideas that allow the defence of information systems”
(Saigushev et al., 2020)	“cybersecurity culture is “a dedicated set of knowledge and behaviors focused on protecting against intentional and targeted cyber-attacks within informational context.”
(ENISA, 2017)	“cybersecurity culture (CSC) refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms, and values of people regarding cybersecurity and how they manifest themselves in people’s behaviour with information technologies. i.e., cybersecurity culture is the way employees act with regard to cybersecurity, to protect the organisation’s information assets or to achieve the desired level of cybersecurity, as well as their underlying knowledge, beliefs, perceptions, attitudes, assumptions, norms and values.”
(Da Veiga, 2016)	“A cybersecurity culture can be defined as the intentional and unintentional manner in which cyberspace is utilised from an international, national, organisational or individual perspective in the context of the attitudes, assumptions, beliefs, values, and knowledge of the cyber user”. “promotes or inhibits the safety, security, privacy, and civil liberties of individuals, organisations or governments.”
(Georgiadou et al., 2020a)	“Cyber-security culture refers to the set of values, conventions, practices, knowledge, beliefs, and behaviours associated with information security. Therefore, its skeleton is being outlined by the working environment along with the technological infrastructure and security countermeasures that define it”.
(Ioannou et al., 2019)	“A cybersecurity culture refers to the procedures laid down by an organisation to all its employees, directing their course of action in all situations related to data integrity, whenever in the line of duty”.
(Leenen & Van Vuuren, 2019)	cybersecurity culture is a macro-culture found among cyber professionals.
(Sousane, 2018)	A union of people (employees), processes, procedures, symbols, technology, training, awareness, commitment, and actions focused on furthering cybersecurity within organisations.

Reference	Formal cybersecurity culture Definitions or Description
(Da Veiga, 2019)	The cybersecurity culture is therefore described as the way users do things to protect information in cyberspace,
(Reid & van Niekerk, 2014a)	A cybersecurity culture includes all the socio-cultural measures that support technical security methods so that cyber actions become a natural aspect of daily activity at a societal level
(Malmedal & Roislien, 2016)	cybersecurity culture “is the attitudes, assumptions, beliefs, values, and knowledge that people use in their interaction with the information assets. Thus, cybersecurity culture is comprised of behaviour and a set of ideas and attitudes”. It is the action of employees.
(Huang & Pearlson, 2019)	“Underlies the practices, policies and “unwritten rules” that employees use when they carry out their daily activities”.
(Paul & Porche, 2011)	“A pattern of shared basic assumptions that supports information security becoming a natural aspect of the daily activities of all Army personnel who operate in cyberspace.”

During the review, the researcher found that existing definitions of cybersecurity culture showed no consistency. This was evidence that there was no single globally defined and acceptable definition of cybersecurity culture in literature, as is also the case with cybersecurity definitions. This supports the claims of researchers that cybersecurity culture is an emerging research area that lacks deeper study including in its definition (Alvarez-Dionisi & Urrego-Baquero, 2019; Gcaza, 2017).

The following important elements discussed in the next subsection were identified by thoroughly examining the existing definitions of cybersecurity culture.

Important points emerging from the cybersecurity culture definitions: Through extensive reading of the cybersecurity culture definitions found in the 26 articles, individual aspects were identified and named, and the third phase of the conceptual framework (identifying and naming concepts of the framework) was achieved.

The important elements identified include human and human characteristics, context or environment, SETA (security education, training and awareness), technology, and management.

4.12.1 HUMAN CHARACTERISTICS

An element that came out very strongly in most of the definitions reviewed (either in the formal or adapted definitions and descriptions) was the issue of humans and their characteristics,

confirming that cybersecurity culture revolves around people (as is the case with culture). Human characteristics play a significant role in cybersecurity culture in safeguarding national, organisational and individual data from cybercrime.

The following were the human characteristics that appeared in the studies: attitudes, assumptions, beliefs, values, knowledge, behaviour, skills, awareness, perceptions, norms, and training (Abeyratne, 2016; Ciuperca et al., 2019; Da Veiga, 2016; ENISA, 2017; Georgiadou et al., 2020b; Ioannou et al., 2019; Malmedal & Roislien, 2016; Reid & van Niekerk, 2014a; Saigushev et al., 2020; Sousane, 2018).

Human characteristics can be grouped into two categories. The first relates to human characteristics in terms of peoples' competency (awareness and knowledge), while the second relates to behaviours or socio-cultural attributes (attitude, perception, and behaviour).

Unsurprisingly, cybersecurity culture is generally “treated as a behavioural pattern that can be altered and improved,” with the ultimate goal being to add value to organisations, thereby classifying cybersecurity culture as either good or bad (Malmedal & Roislien, 2016).

4.12.2 CONTEXT OR ENVIRONMENT

The second important point that emerged from the definitions related to context or environment. Context (or environment) is the foundation upon which the cybersecurity culture can be built and implemented. Context can be a country (national cybersecurity culture level), an organisation (organisational cybersecurity culture level), an individual (individual level cybersecurity level) or a combination of different levels (Da Veiga, 2016; Gupta & Bajramovic, 2017). Examples of snippets of text from the data: “actions focused on furthering cybersecurity within organisations” (Sousane, 2018); “laid down by an organisation” (Ioannou et al., 2019); “in the context” (Da Veiga, 2016); and “to protect the organisation’s” (ENISA, 2017).

The environment can refer to external issues that affect the design, development, and implementation of the cybersecurity culture. It is often referred to as the environment or as an external factor, for example, “working environment,” as indicated in the definition by Georgiadou et al. 2020a.

4.12.3 SETA (SECURITY EDUCATION, TRAINING AND AWARENESS)

This third point relates to security education, training, and awareness (SETA). In some of the definitions, SETA emerged as an important element of cybersecurity culture. The definitions by Abeyratne (2016) and Sousane (2018) emphasised SETA. SETA has complementary elements that assist with the mitigation of human security threats.

Security education is used to continuously develop the employees' comprehensive knowledge of security over the long term. This informs their behaviours and decisions. Security training provides employees with the specific skills required for their daily operational activities and, in this way, helps to protect the organisation from security incidents. Security training assists employees in acquiring proficiency that is related to specific duties. Security awareness ensures that the employees remain vigilant and aware of security concerns and safety issues.

4.12.4 TECHNOLOGY

Technology was also highlighted in some definitions as an important aspect of cybersecurity culture (Ciuperca et al., 2019; ENISA, 2017; Reid & van Niekerk, 2014a; Sousane, 2018). Although security culture (either information security culture or Cybersecurity Culture) was mostly viewed as a non-technological way of creating a culture of security (Alhogail & Mirza, 2014; Da Veiga & Eloff, 2010; ENISA, 2017), technological aspects cannot be neglected as aspects of technology can influence the nature of the cybersecurity culture that is created. This is because aspects of technology influence the employee's interactions with organisational assets like information, data, systems, people and networks. ENISA (2017) argue that the cybersecurity culture implies focusing on technology, people and their behaviour, awareness, and business processes.

4.12.5 MANAGEMENT

Lastly, aspects of management were identified as essential in some definitions. The terms characterising management that were frequently used in the definitions included policy, procedure, guidelines and leadership (Abeyratne, 2016; Huang & Pearlson, 2019; Ioannou et al., 2019; Sousane, 2018). The term 'organisation' was used to refer to management by some researchers (Ioannou et al., 2019).

In summary, only 14 studies formally defined or described cybersecurity culture. Others either adopted definitions of cybersecurity culture created by other authors or defined the concept as the same as information security by adopting a detailed definition of information security culture.

The major difference between the newly defined cybersecurity culture and the cybersecurity culture definitions adopted or viewed as synonymous to information security culture, was that the new cybersecurity culture definitions were broader in scope. As a result, the focus was not specifically on protecting information assets, as was the case with information security culture. The slight difference in the definitions enforces the view that information security culture and cybersecurity culture are not synonymous but are rather separate parts of a whole (Astakhova, 2014).

Since a deeper study of the definition of cybersecurity culture is lacking, and there is no officially acceptable definition of cybersecurity culture, considering the definitions given in Table 4.1 and identifying essential elements in the definition, this study therefore defines cybersecurity culture as: *a holistic measure that is used as a performance tool by the management of an organisation (guided through policies and procedures), in a specific context, to change human characteristics and their socio-cultural measures (like attitudes, assumptions, beliefs, norms, knowledge, perceptions, skills, behaviours, and practices) to achieve cybersecurity at all levels of cybersecurity culture in order to protect against intentional and unintentional cyber-harms using the available technology.*

4.13 CYBERSECURITY CULTURE FACTORS

This subsection presents the cybersecurity culture factors identified in Phase 3 through the extensive reading of the selected data that relates to the cybersecurity culture factor (first and second phase of the conceptual framework). The ATLAS.ti network diagram (see **Figure 4.8**) was used to summarise the factors associated with cybersecurity culture that had been identified in the literature. These factors had been found to be critical in either the development, recommendations, maintenance, best practices or frameworks of cybersecurity culture (Alshaikh, 2020; Branley-Bell et al., 2021; Cardoso et al., 2017; Corradini, 2020; ENISA, 2017; Gcaza & von Solms, 2017a; Leenen & Van Vuuren, 2019; Ogden, 2021; Reegård et al., 2019).

Therefore, these identified factors are not only constituent factors of cybersecurity culture but also characterise, challenge, influence and are used in the development of cybersecurity culture.

appeared as the top factors associated with cybersecurity culture in research. These factors are consistent across the literature. The factors were considered to be the top factors not due to the number of references to them in the literature, but due to their level of significance in the cultivation, implementation and maintenance of cybersecurity culture, as well as their level of association with other factors.

Other identified factors of cybersecurity culture include information sharing, accountability, cybersecurity hub, national culture, compliance, ethical conduct, security audit, change management, measure of effectiveness, trust, rewards and sanctions, collectivism, physical security, governance and control (legal and regulatory), business continuity plan, interest and communication channel. Table 4.2 depicts the factors identified in the third phase of the conceptual process and the number of literature articles that support the idea.

Table 4.2: Cybersecurity Culture Factors and Their Occurrence in Literature

	Cybersecurity Culture Factors	Number of Papers		Cybersecurity Culture Factors	Number of Papers
1.	Training and education	42	16.	Trust	7
2.	Awareness	34	17.	Communication	6
3.	Top management or leadership support	20	18.	Information sharing	5
4.	Cybersecurity policy and procedures	17	19.	Rewards and sanction	5
5.	Human behaviour	14	20.	Governance and control (legal and regulatory)	5
6.	Knowledge and understanding	14	21.	Compliance	5
7.	Cybersecurity champion or team	13	22.	Measure of effectiveness	4
8.	Organisational culture	11	23.	National culture	4
9.	Engagement, encouragement, cooperation	11	24.	Ethical conduct	4
10.	Budget and resources	11	25.	Business continuity plan	4
11.	Cybersecurity strategy	11	26.	Collectivism	3
12.	Collaboration	10	27.	Cybersecurity hub	3
13.	Commitment	9	28.	Security audit	2
14.	Role and responsibility	8	29.	Physical security	1
15.	Risk and change management	8	30.	Interest	1

	Cybersecurity Culture Factors	Number of Papers		Cybersecurity Culture Factors	Number of Papers
			31	Communication channel	1

The definitions of the cybersecurity culture factors depicted in Table 4.2 are presented in **Section 4.13.1**. The section also provides examples of references in which individual factors were considered. For a detailed table which clearly indicates that the identified cybersecurity culture factors came from the full set of 58 articles as per PRISMA diagram, refer to Appendix A of Mwim and Mtsweni (2022).

4.13.1 DEFINITIONS OF CYBERSECURITY CULTURE FACTORS

Cybersecurity training and education provides members of organisations, communities, and societal groups with essential and appropriate information and skills. Over the years, this has been supported as a factor of cybersecurity culture (Abeyratne, 2016; Alshaikh, 2020; Branley-Bell et al., 2021; Ciuperca et al., 2019; Da Veiga, 2019; ENISA, 2017; Gcaza et al., 2015; Kortjan & von Solms, 2014; Marotta & Pearlson, 2019; Paul & Porche, 2011).

Cybersecurity awareness makes members and employees aware of cybersecurity-related issues and, on a continual basis, maintains their consciousness of cybersecurity obligations within their organisations. Awareness was highlighted overwhelmingly as one of the most essential factors for the cultivation and achievement of cybersecurity culture. Examples of literature referring to this include Alvarez-Dionisi & Urrego-Baquero (2019); Corradini (2020); Gcaza (2017); Georgiadou et al. (2021a); Holdsworth and Apeh (2017); Reid and van Niekerk (2014a, 2014b); Ribeiro (2019); and Trim and Upton (2013).

Top management support is referred to as leadership support as well as executive buy-in. It clarifies the type of support that management needs to provide for the cultivation and implementation of a strong cybersecurity culture. This factor includes the initial development of a cybersecurity policy, defining clear goals for the management of security, endorsement of security requirements, the willingness to commit by providing financial resources to support cybersecurity, and organising cybersecurity activities (such as education, skills and awareness programmes within the organisation). This factor was found to be the third most important factor according to the literature review. Literature that stresses top management support as a

factor in cybersecurity culture includes Alshaikh (2020); Clark et al. (2017); Leenen et al. (2018); Ogden (2021); Reegård et al. (2019); Rinchi (2019); and Wierzynski (2019).

Cybersecurity policy and procedures deal with the definition, clarification and management of the cybersecurity policies and procedures that have been found to be fundamental for achieving cybersecurity culture. Cybersecurity policy is indicated in the literature as a foundational factor for the achievement of cybersecurity culture. Particular references include Branley-Bell et al. (2021); Reegård et al. (2019); Sousane (2018); Uchendu et al. (2021); and Wierzynski (2019).

Human behaviour entails developing an understanding of human attributes. The security culture should reflect people's beliefs, values, perceptions, attitudes and emotions so that adhering to it becomes their natural form of behaviour. Cybersecurity culture should shape and reshape human behaviours. Particular references include . Branley-Bell et al. (2021); Ciuperca et al. (2019); Corradini (2020); ENISA (2017); Malmedal & Roislien (2016); and Van 't Wout (2019)

Knowledge and understanding relates to acquiring facts and information about the organisation, based on which cybersecurity culture will be built. Such knowledge assists in learning about the diversity of groups within the organisation (e.g. educational level, age group, gender group and departmental level) and will assist the security team in making well-informed security-related decisions to accommodate different groups. This factor also relates to equipping the members of the organisation with the necessary cybersecurity knowledge that should inform their actions regarding cybersecurity-related issues. Particular references include Ioannou et al. (2019); Malyuk & Miloslavskaya (2016); and Wierzynski (2019).

Cybersecurity champions or a team refers to the appointment and management of authorities (individuals or teams) that champion cybersecurity, that is, the team or person responsible for ensuring a secure system, and the development of awareness and training activities. Particular references include Corradini (2020); Huang and Pearlson (2019); Leenen et al. (2018); Leenen and van Vuuren (2019); Loică (2017); Uchendu et al. (2021); and Van 't Wout (2019).

Organisational culture comprises belief systems that influence collective action, values that indicate what is considered important, artefacts that are made up of the visible technology, and behavioural patterns that form the basis of cybersecurity culture layers and factors. Particular references include Branley-Bell et al. (2021); ENISA (2017); Loică (2017); Marotta and Pearlson (2019); Pătrascu (2019); Pavlova (2020); and Reegård et al. (2019).

Engagement, encouragement and cooperation addresses and manages how members of an organisation or community who are involved in cybersecurity-related activities, such as decision-making and strategy development, are motivated to adhere to the security regulations and guidelines, and how teams work collaboratively to achieve a security culture. Examples of literature from the review that supported cybersecurity training and education as a factor in cybersecurity culture were . Corradini (2020); ENISA (2017); Malyuk and Miloslavskaya (2016); Marotta and Pearlson (2019); Ramluckan et al. (2020); Uchendu et al. (2021); and Van ‘t Wout (2019).

Budget and resources refers to the financial and non-financial commitment and support provided for the development and maintenance of cybersecurity culture. Particular references include Cardoso et al. (2017); Clark et al. (2017); Corradini (2020); Gcaza et al. (2015); and Huang and Pearlson (2019).

Based on the findings from the systematic review, this section presented the definition and described the top ten cybersecurity culture factors with important references to the literature. For full definitions of all the identified cybersecurity culture factors and all the literature references associated with the factors, see APPENDIX_1A. **Section 4.13.2** discusses the categories of cybersecurity culture factors.

4.13.2 CATEGORIES OF CSC FACTORS

The cybersecurity culture factors depicted in **Figure 4.8** are categorised in **Error! Reference source not found..** The categorisation is based on where the influences of the factor originated from. Some factors’ influence originated from within the organisation, and hence, they were categorised as internal factors (Da Veiga, 2019; Georgiadou et al., 2020b), organisational factors or organisational mechanisms (ENISA, 2017). Where the influence of the factors originated from outside the organisation, they were referred to as external factors or external influences (Da Veiga, 2019; Georgiadou et al., 2020b; Huang & Pearlson, 2019) and non-organisational factors (ENISA, 2017).

There is, however, a discrepancy in how Da Veiga (2019) and ENISA (2017) grouped factors in these two main categories, for example, as human factors or individual characteristics. According to Da Veiga (2019), all human-related factors are categorised as part of internal influence, and they are grouped under the “group tier”, which includes subcultures formed as a result of the demographic composition (age, gender, educational group, and departmental

group). For ENISA (2017), elements constituting the human factor are considered as belonging to both non-organisational factors, such as psychological factors (personality, gender) and organisational factors (attitudes, views, and behaviours).

This study, however, believes that since humans are a significant part of every organisation, their characteristics, which are formed by their culture, change how things are done within the organisation (behaviour). As a result, human factors are regarded as a part of the internal influences or organisational factors of a cybersecurity culture.

Internal influence factors were grouped into three tiers: organisational, group and individual (Da Veiga, 2019). The organisational tier relates to formal structures, participation, knowledge and priority at the managerial level of the organisation. Hence, they are mostly executed by top management or leadership (Da Veiga, 2019; Huang & Pearlson, 2019).

The group tier relates to several compositions of groups, for example, team participation, collaborations between departments, and group norms at the tactical level of the organisation. Group tier factors are executed by groups in the organisation (Da Veiga, 2019; Huang & Pearlson, 2019).

The individual tier relates to employee or individual characteristics (age, attitudes, values, assumptions, norms, personalities, awareness and efficacy) at the operational level of the organisation (Da Veiga, 2019; Huang & Pearlson, 2019).

According to Georgiadou, et al. (2020b), the cybersecurity culture factors are grouped into organisational and individual factors. This, therefore, indicates that internal cybersecurity culture factors can be found both at the organisational and individual levels. **Figure 4.9** summarises the terminologies used to categorise cybersecurity culture by different authors (Da Veiga, 2019; ENISA, 2017; Georgiadou et al., 2020b; Georgiadou et al., 2021a; Huang & Pearlson, 2019).

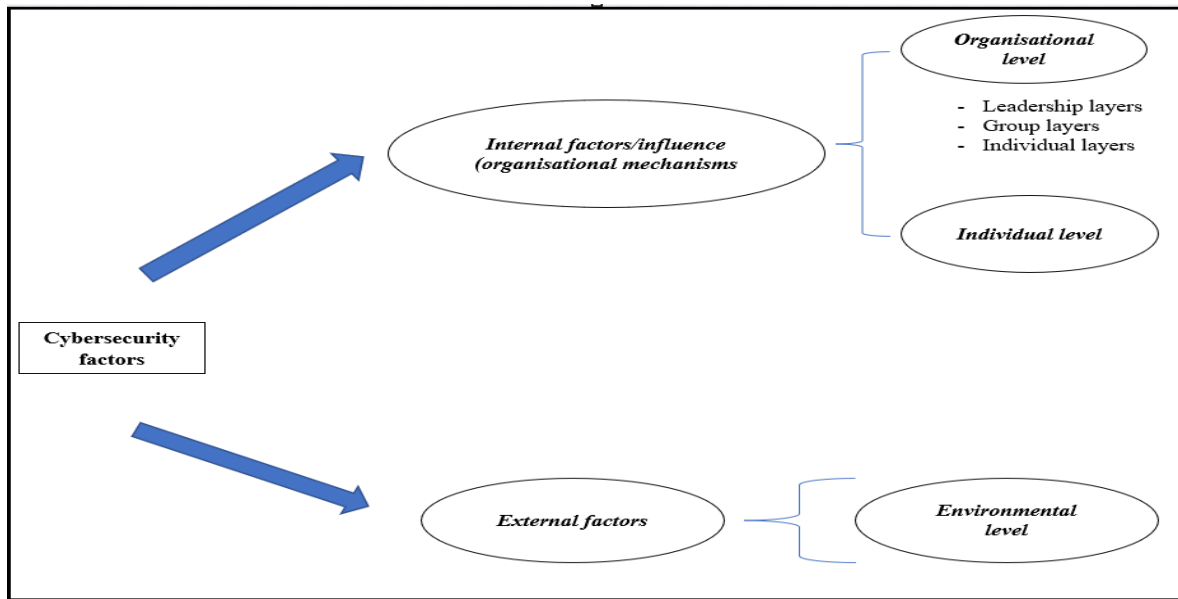


Figure 4.9: Categories of Cybersecurity Culture (own source)

Organisational culture is an organisational factor (or internal influence) which consists of human attributes such as the views, attitudes, and behaviours of organisational members related to the cybersecurity culture and the organisation's cybersecurity strategy. Organisational factors include other human characteristics as well, including psychological attributes (individual personality), age, background, nationality, skill, and competency (Da Veiga, 2019; ENISA, 2017).

Other examples of organisational factors include social environment, compliance, organisational commitment, groups within the organisation (such as departmental groups, groups of committees and age groups), adopted business and employee model, formal roles of top management (the board of directors, executives and senior managers, including security managers) (Da Veiga, 2019; ENISA, 2017).

Non-organisational factors or external influences include national culture, technological innovation, change in the economy, standards, policies, and regulatory requirements (Da Veiga, 2019; ENISA, 2017).

Table 4.3 summarises the factors of cybersecurity culture according to the two broad categories to which cybersecurity culture belongs.

Table 4.3: Cybersecurity Culture According to Category

Internal organisational factors	organisational culture, human factor/behaviour, cybersecurity strategy, cybersecurity policies and procedures, commitments and collaboration (departmental, cross-organisational, and by individual commitments), top management support, knowledge, cybersecurity awareness, knowledge training and education, roles and responsibility, resources, exchange of information, cybersecurity team and hub, trust, accountability, change management, collectivism, compliance, ethical conduct, control measures, security audit, physical security, and continuity plan
External influences or non-organisational factors	national culture, technological innovation, economic change, standards, political, legal and regulatory requirements

Based on the information accumulated through the literature review described in this chapter, the section identified the factors of cybersecurity culture and the two broad categories used to group the factors. Identification of cybersecurity culture forms the basis of this study as it addresses the **Sub-Research Objective 2 (SRO 2)**. Also, using the information gathered through the literature review, the next section discusses the cybersecurity culture frameworks and related frameworks.

4.14 THEORETICAL FRAMEWORK AND RESEARCH MODEL

The discussion of the CCSCF includes additional references to the 58 selected data items (see **Figure 4.7**) that were reviewed to identify important constructs of cybersecurity culture.

As a growing research area, literature on cybersecurity culture is beginning to develop and describe a variety of frameworks or models for cybersecurity culture (Da Veiga, 2019; Georgiadou et al., 2020b; Huang & Pearlson, 2019). The frameworks or models show how cybersecurity culture has been used in different areas to develop a more established and effective Cybersecurity Cultures within organisations. The models help researchers to understand cybersecurity culture, its vital elements, and to visualise a proposed CCSCF.

However, since cybersecurity culture is still a developing area of research, few frameworks exist. Additionally, the research area of cybersecurity is closely linked to a variety of associated research initiatives and their frameworks (human dimension and Strategy, Technology, Organization, People, and Environment (STOPE)) (Alhogail, 2015; Bakry & Bakry, 2005; Bakry, 2003). This research team argues that insight from STOPE and human domain frameworks would assist them in the conceptualisation of components and hence, help with the design and development of the CCSCF in this study.

The cybersecurity culture, STOPE, and human dimension frameworks are discussed below.

4.14.1 CYBER-SECURITY CULTURE THEORETICAL FRAMEWORK (FAOR)

The cybersecurity culture, Theoretical Framework for Assessing Organisational Readiness (FAOR), depicted in **Figure 4.10** was developed by Georgiadou et al. (2020b). The framework emerged as a result of a thorough review of multidisciplinary research into the approaches and principles of information security, information security frameworks, as well as organisational and behavioural theories (Georgiadou et al., 2020b). According to the authors, the framework created a basis upon which essential factors constituting cybersecurity culture can be united (Georgiadou et al., 2020b). The theoretical framework was argued to be a globalised model because its design was based on a combination of “human-centric” elements and characteristics with internal and external organisational parameters (Georgiadou et al., 2020b).

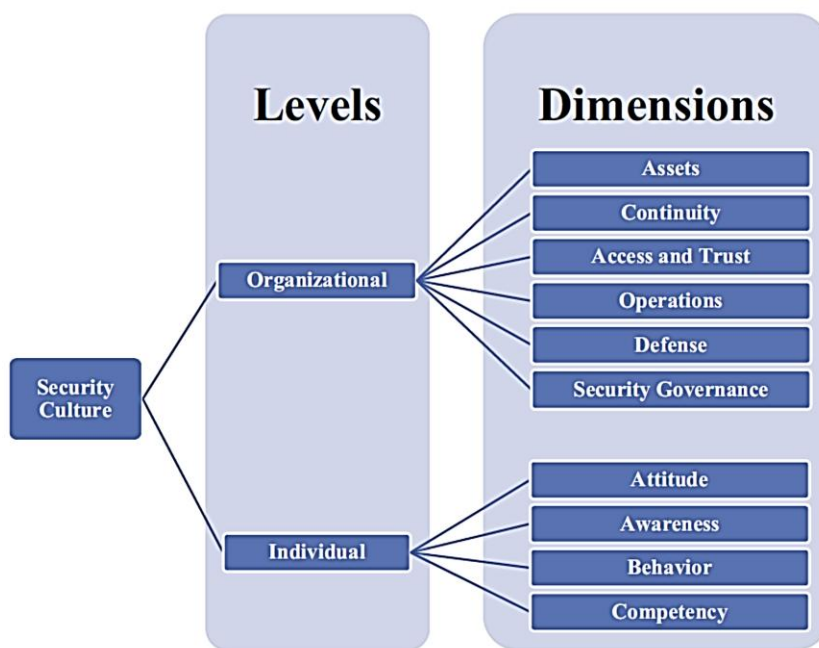


Figure 4.10: Cybersecurity Culture Theoretical Framework (Georgiadou et al., 2020b)

The essential factors that constitute cybersecurity culture in this theoretical framework are represented at two levels, the organisational and individual levels. Each level represents its factors in the form of dimensions (see **Figure 4.10**). The individual level focused on employees’ (human) characteristics and the elements that influence their attitude, awareness, behaviour, and competency as dimensions that are relevant in business domains. The

organisational level relates to the organisation's assets, continuity, access and trust, operations, defence, and security governance as dimensions.

Limitations of the Cyber-Security Culture Theoretical Framework

- The major limitation of this framework is the exclusion of the environment (which can also be regarded as an external level, external influence or external factors) as a component for consideration in developing a CCSCF. The developers of the framework argued that external and internal organisational parameters were considered in the design, but these are not explicitly depicted in the framework. This is a limitation as other work in cybersecurity culture has clearly demarcated between internal factors, external factors, organisational and non-organisational factors of cybersecurity culture (Da Veiga, 2019; ENISA, 2017; Huang & Pearlson, 2019).
- Technology as a component was also not considered in developing the Cyber-Security Culture Theoretical Framework.
- Another limitation of the framework is that its dimensions were not categorised using existing frameworks, for example, the human factor domain (HFD). The organisational level dimensions can be regarded as management, and the individual level dimension can be regarded as preparedness and responsibility according to the HFD framework, but these were not mentioned in the Cyber-Security Culture Theoretical Framework.
- Another limitation of the model includes the fact that no correlation was done as an empirical study. No systematic literature was done using existing search engines such as the Institute of Electrical and Electronics Engineers (IEEE) and Association for Computing Machinery (ACM) to ensure the identification and inclusion of all the cybersecurity culture factors.

4.14.2 SECURITY CULTURE MODEL (SCM)

Da Veiga (2019) developed the Security Culture Model (SCM) depicted in **Figure 4.11** by adapting the model of Da Veiga and Martins, (2017). The SCM embedded cybersecurity culture as a subset of organisational culture (Schlienger & Teufel, 2003; van Niekerk & von Solms, 2006) and included associated dominant or subcultures.

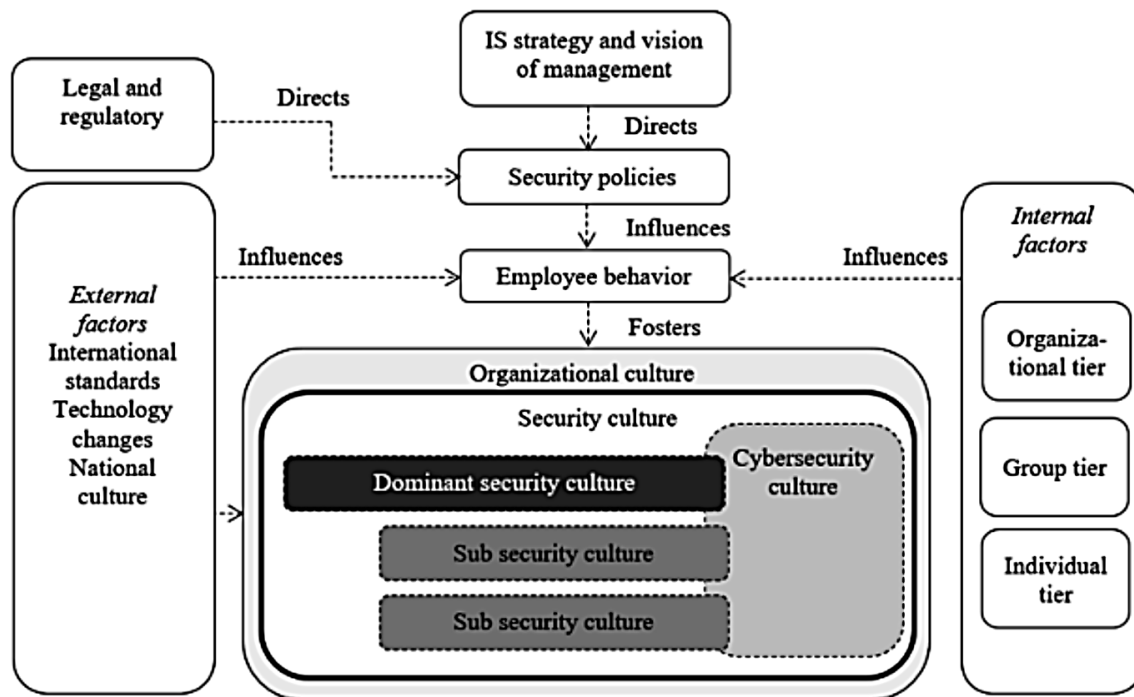


Figure 4.11: Security Culture Model Theoretical Framework (Da Veiga, 2019)

The SCM depicted organisational culture as a means for a better understanding of factors that affect the creation of security culture. To encourage constant compliance in an effective manner, an organisation's security programme needs to consider external and internal factors for a more complete approach (Da Veiga, 2019).

According to the SCM, various external and internal factors influence the security culture and employee behaviour. Employee behaviour is also influenced by security policies, which are in turn directly impacted by legal requirements and regulations, as well as management security strategy and vision. Employee behaviour also fosters an organisational culture of security. External factors include international and industry standards, competitors, technological change and natural culture (Alhogail, 2015; Da Veiga, 2019; ENISA, 2017; Hofstede et al., 2010). Internal factors examples are employee personality and behaviour (Padayachee, 2011).

Limitations of the Security Culture Model

- An aspect that can be considered as a limitation of the SCM is that some factors of the model, which have been grouped as factors of bigger components in other frameworks, were not treated as such in this framework. Instead, the factors were treated independently. For example, “legal and regulatory,” which are factors of external factor components in other frameworks (Alhogail et al., 2015; Corradini,

2020; ENISA, 2017; Huang & Pearlson, 2019), were treated separately in SCM. Management vision and security policies, which elsewhere are elements of internal or organisational factors (Alhogail et al., 2015; Corradini, 2020; ENISA, 2017; Huang & Pearlson, 2019) were separate internal factors in SCM.

- Another limitation is that in SCM, organisational culture and employee behaviour are separate constructs.
- Lastly, there was no inclusion of technology as an explicit component of the framework.

4.14.3 OCYBERSECURITY CULTURE FRAMEWORK

Huang and Pearlson (2019) developed the OCybersecurity Culture Framework by investigating the concepts relating to information security culture, organisational culture and natural culture. Ocyber was developed as “a practical framework for managing the intangible factors of cybersecurity culture ” (Huang & Pearlson, 2019). Hence, the framework offers organisations a way to observe and measure cybersecurity culture. This assists management by giving them a better understanding of decisions that need to be made to help transform their cybersecurity culture.

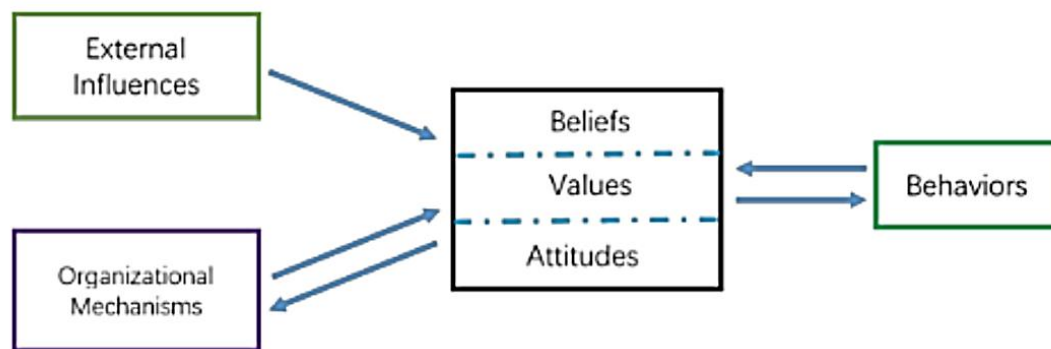


Figure 4.12: Conceptual Framework of OCybersecurity Culture (Huang & Pearlson, 2019)

The authors developed the OCybersecurity Culture Framework based on a strong belief that reducing cybersecurity risk in an organisation requires actions from every member of the organisation. Hence, management has the obligation to comprehend, shape and align their organisational cybersecurity culture with security goals, and individuals have the responsibility to comply with the security practices of their organisation.

The Ocyber framework (see **Figure 4.12**) shows that the way the management of any organisation can achieve cyber secure behaviours is by creating an organisational cybersecurity culture (reflecting beliefs, values and attitudes which are the layers of organisational culture) (Schein, 2004).

Ocyber also shows that organisational cybersecurity culture is directly influenced by a combination of external influence and the organisational mechanisms used by the management. However, the organisational mechanism is also influenced by organisational cybersecurity culture factors, as depicted by the bilateral relationship arrow (Huang & Pearlson, 2019). In some papers, the external factor is also referred to as the environmental or non-organisational factor or influence (Da Veiga, 2019; ENISA, 2017). Organisational mechanisms have been referred to as either management, the organisational factor or level, internal factors or influence elsewhere (Alhogail et al., 2015; Da Veiga, 2019; ENISA, 2017; Georgiadou et al., 2020b).

The OCybersecurity framework components are external influences, organisational mechanisms, organisational culture and behaviours. In the framework, external influences include factors (societal cybersecurity culture and external rules and regulations). The organisational mechanisms were regarded as the manager's six levels for developing cybersecurity expectations, and are comprised of factors (cybersecurity policy, practices, security governance, assets, cybersecurity culture, leadership and communication issues). Organisational culture involves beliefs, values, and attitudes (Reid & van Niekerk, 2014a; Schein, 2004). These can be classified as preparedness and responsibility characteristics (Alhogail, 2015; Alhogail et al., 2015). In the Ocybersecurity culture, behaviour was the actual action of the studied object in the field of research (Madden et al., 1992).

A positive part of this framework is that it was built around the component of organisational culture, which has been considered an essential part of cybersecurity culture (Corradini, 2020). The author argued that cybersecurity culture should be made a vital part of an organisation's culture for it to be effective.

Additionally, the OCybersecurity culture included external influences as a component of the framework (Huang & Pearlson, 2019). This level was missing in the cybersecurity culture FAOR framework (Georgiadou et al., 2020b). This implies that the environment as a component was not treated as part of an organisational factor, as in the HFD framework (Alhogail et al., 2015). Furthermore, the framework did not separate human behaviour, which is seen as culture, from OC (Corradini, 2020; Reid & van Niekerk, 2014a; Schein, 2004;

Schlienger & Teufel, 2003). Additionally, rules and regulations are not treated separately from external influence as in the case of the security culture model (Da Veiga, 2019)

Limitations of the OCybersecurity Culture

- As was the case with the two models discussed in **Section 4.14.1**, the Georgiadou et al. (2020b) Cyber-Security Culture Model and in **Section 4.14.2**, the Da Veiga (2019) Security Culture Model, in the OCybersecurity Culture Framework, technology was missing as an essential component of the framework.
- The model has not been used in the public E-Health hospital setting but only in a financial services firm.

4.14.4 THE HUMAN FACTOR DIAMOND (HFD) FRAMEWORK

Figure 4.13 depicts the human factor diamond (HFD) framework by Alhogail et al. (2015). Although the HFD framework is not a CCSCF, it was considered in this study because of the significance of human elements in understanding and achieving a cybersecurity culture within a context. The reasons for inclusion are firstly that the human factor, which is represented by behaviour, attitude, knowledge, and skill (portrayed by employee and management in an organisation), has an important impact on cybersecurity culture, and the concept has been structured into a comprehensive framework of Human Factor Domain (HFD).

Secondly, limited to no research exists where the HFD framework has been considered in the existing CCSCF. This research argues that it would be necessary to consider the dimensions and domains of the HFD framework for more comprehensive CCSCF development. Thirdly, the framework has been considered by other authors in information security culture studies (Alhogail, 2015). This supports the use of the HFD framework in cybersecurity culture, which is viewed as an umbrella concept that includes information security culture.

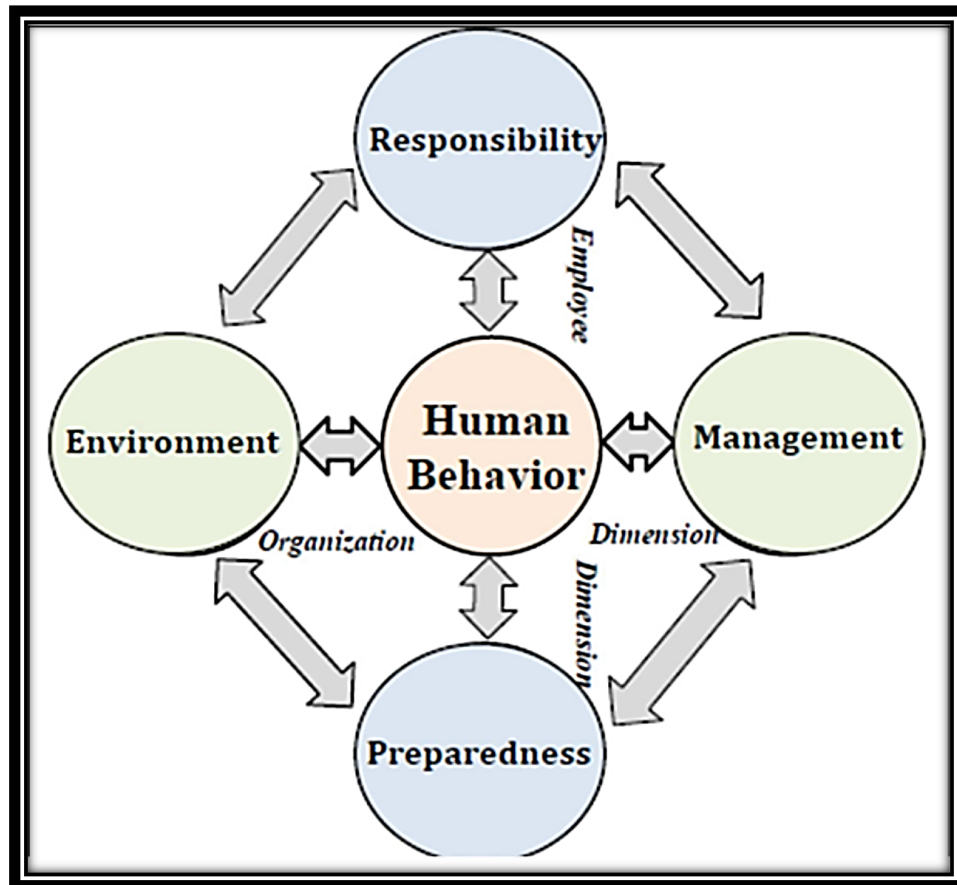


Figure 4.13: The Human Factor Diamond (HFD) Framework (Alhogail, et al., 2015)

The HFD framework's components include preparedness and responsibility, which have been grouped under the employee dimension, and management and environment, grouped under the organisational dimension. Preparedness comprises human individual characteristics, such as awareness, self-efficacy, knowledge, training and change from old practices that are related to cybersecurity culture (Alhogail et al., 2015).

In this theoretical framework, responsibility is related to organisational culture and is comprised of human characteristics (attitudinal factors, monitoring and control, and compliance). Management is classified as an internal cybersecurity culture element. Management focuses on actions and procedures at the organisational level and is associated with cybersecurity culture (Alhogail, 2015; Alhogail et al., 2015). The environment focuses on the external (non-organisational) characteristics of a cybersecurity culture. Although its associated characteristics refer to things outside the organisation, they restrict the way the organisation carries out daily operations that are related to cybersecurity culture. According to the theoretical framework (Alhogail, 2015; Alhogail et al., 2015; Da Veiga, 2019), the

environment is depicted as part of an organisation dimension (see **Figure 4.13**), and human behaviour is referred to as cybersecurity culture.

In this study, the researcher argues that a restriction in the environment can be regarded as a non-organisational dimension (an external factor rather than an internal factor). Technology was not accommodated in the framework, and the dimensions of the framework only focused on internal factors. There was little focus on the restrictions of this framework. This was because it is not a CCSCF, but it was discussed in this study to assist with the conceptualisation of constructs for the proposed framework, since cybersecurity culture draws a lot from human characteristics.

4.14.5 THE TECHNOLOGY, ORGANISATION, PEOPLE AND ENVIRONMENT THEORETICAL FRAMEWORK (STOPE)

The STOPE framework (see **Figure 4.14**) was originally developed by Bakry (2003) as an integrating tool to tackle problems relating to the use of digital technology. This framework has been applied to assist with the development, integration and evaluation of various ICT problems in e-readiness assessment, e-government, ERP, and network security (Alhogail, 2015; Alhogail & Mirza, 2014; Bakry & Bakry, 2005; Bakry, 2002, 2004; Bakry & Bakry, 2001).

The STOPE framework has previously been applied extensively to assist with the development of information security culture frameworks (Ocloo et al., 2021; Alhogail, 2015; Alhogail & Mirza, 2014). In this study, cybersecurity culture and information culture are viewed as separate subsets of security. It is important to note that the researcher is of the view that there is a sound theoretical reason for recognising the important components of STOPE, and that it can be used as a tool in addressing the cybersecurity problem arising from the use of digital technology. Therefore, this study finds it beneficial to consider STOPE as an important framework for the study of a cybersecurity culture. The STOPE framework has been applied in research related to other Internet-enabled applications, such as E-Readiness, E-Assessment, and E-Government. Since this research studied E-Health, STOPE is considered to be a suitable framework.



Figure 4.14: STOPE Theoretical Framework (Bakry, 2003; Bakry & Bakry, 2005)

The STOPE Framework has five core domains: Strategy, Technology, Organization, People and Environment. The strategy domain deals with matters related to ICT leadership and plans for upcoming development. The technology domain relates to non-technical issues of technology, such as ICT infrastructure, services and support (Ocloo et al., 2021). The organisation domain covers regulation, cooperation and management. The people's domain pays particular attention to awareness, education and performance. Lastly, the environment domain relates to issues of economy, overall infrastructure, management and knowledge.

One advantage of this framework is that it explicitly accommodates technology, which was missing in all the frameworks discussed in **Sections 4.14.1 to 4.14.4**. Another advantage of STOPE as a framework is that it also accommodates the other components that are discussed in other frameworks.

The only difference between STOPE and the other frameworks is in the terminology used to refer to the components, the meaning attached to them, and the factors associated with the components. As with HFD (see **Section 4.14.4**), there is no focus on the limitations of STOPE as it is not a CCSCF but is applied to help address the limitations noted in the three existing cybersecurity culture frameworks when undertaking the design and development of the proposed CCSCF.

The information from the frameworks discussed in this section was compared and conceptualised in **Sections 4.15 and 4.16** to achieve the **Research Sub-Objective 4 (SRO 4)**, which aimed to identify components from the existing cybersecurity culture frameworks and other frameworks that can stimulate the cultivation of cybersecurity culture in the public E-Health institutions.

4.15 COMPARISON OF THEORETICAL FRAMEWORKS

Figure 4.10 to **Figure 4.14** depicted the various theoretical frameworks selected to assist with a holistic view of cybersecurity culture and popularly used models in e-government and e-assessment. Context is considered very important in the development of cybersecurity culture. None of the frameworks discussed in **Sections 4.14.1** to **4.14.4** have been developed for or implemented in public E-Health institutions, or in the African context, and this highlights the significance of the framework that was developed in this study.

Table 4.4 shows a comparison of the constructs used in the frameworks discussed in **Sections 4.14.1** to **4.14.5** as well as the final model.

Table 4.4: Theoretical Framework Comparison

Model 1 (Cybersecurity Culture FAOR)	Model 2 (SCM)	Model 3 (Ocyber-security Culture)	Model 4 (HFD)	Model 5 (STOPE)	Final Model
Individual level	Individual tier	Beliefs, values and attitudes	Preparedness and responsibility	People	Preparedness and Responsibility (Organisational Culture)
	External factor	External influences (external factors)	Environment (Internal factors)	Environment	External Environment Non-Organisational Management
Organisational level	Internal Factors	Organisa-tional mechanisms	Management	Organisa-tional Strategy	Internal Organisational Management
	Technology			Technology	Technology
Cybersecurity culture	Human behaviour	Behaviours	Human behaviour		Cybersecurity Culture/Human behaviour

It is evident from Table 4.4 that there is confusion in the names of the constructs. What the constructs mean and include as elements in the theoretical frameworks and associated work of several researchers differs. Hence, there is a lack of standardised ways to define and measure specific constructs in and between previous studies.

For example, in some frameworks like the Cybersecurity Culture-FAOR theoretical framework, organisational factor is argued to consist of external and internal factors (as in Georgiadou et al. (2020b)). However, in the OCybersecurity Culture Framework, an organisational factor (known as an organisational mechanism in that framework) was used to refer to the management responsibility in the organisation, and external factors were treated as separate constructs outside the organisation (Huang & Pearlson, 2019). No single decision variable was found to be defined or used consistently across the frameworks.

There is no clear definition of terms such as domain, dimension and level; hence, there is inconsistency in the terms in the framework. The comparison provided in Table 4.4 shows that technology has not been considered as a construct in any of the three existing theoretical frameworks discussed, which are intended for cybersecurity culture and appear only in the STOPE framework. This highlights the need for an improved CCSCF, as is proposed in this research. Regarding the HFD framework, the environment is part of an organisation dimension, a view which is rejected in this research as a limitation because the environment can be regarded as a non-organisational dimension.

The concept of a cybersecurity culture is still emerging. Therefore, not many empirical studies have been carried out yet, and as a result, the existing theoretical frameworks have not had sufficient empirical testing and evaluation. This makes it difficult for the researcher to compare them empirically. Further studies are expected to incorporate theoretical comparisons of frameworks.

In this study, cybersecurity culture looks at human behaviour.

4.16 CONCEPTUALISATION OF E-HEALTH CSC COMPONENTS

This section shows how the different theoretical frameworks (discussed in Sections 4.14.1 to 4.14.4 and compared in Section 4.15) were conceptualised in the context of this cybersecurity culture study. This led to the identification of the constructs depicted in Table 4.5 as associated with cybersecurity culture.

Table 4.5: The Research Constructs

Constructs
Preparedness (P) and Responsibility (R)
External Environment and Non-Organisational Management (EENOM)
Internal Organisational Management (IOM)
Technology
Cybersecurity Culture

The constructs depicted in Table 4.5 are discussed below.

4.16.1 PREPAREDNESS (P) AND RESPONSIBILITY (R) (ORGANISATIONAL CULTURE)

These constructs relate to about people. The constructs relate to characteristics of individuals (also used interchangeably with people, humans, or employees), within the organisation that makes use of the organisation's own ICT systems. Preparedness and responsibility both represent people's characteristics (particularly their attitudes and behaviour), hence the components are used to represent organisational culture in this study.

The constructs also represent the people element of the E-Health ecosystem defined in Chapter 2. This is consistent with the cybersecurity culture definition (in **Section 4.12**) which found humans, their characteristics, and SETA to be important elements of cybersecurity culture. Therefore, the constructs of preparedness (P) and responsibility (R) relate to the elements of humans, their characteristics and SETA.

The research found that employees' interactions with the critical ICT infrastructure of an organisation are what demonstrate security behaviour, hence, a culture of maintaining security is needed to manage human-related factors and to improve the behaviour of the user (Alhogail & Mirza, 2014; Caballero, 2014). Examples of factors associated with the constructs of preparedness and responsibility are employee awareness, competency, skills, knowledge, attitude, perception, behaviour and belief in cybersecurity.

As a result, preparedness (P) and responsibility (R) (Organisational Culture) are expected to have a relationship with cybersecurity culture, as well as with other constructs that constituted the frameworks of this study.

Several names have been used in other theoretical frameworks to refer to this construct. In this study, the terms ‘individual level’, ‘individual tier’, ‘belief’, ‘values and attitudes’, ‘preparedness’, and ‘responsibility’, as well as ‘people’, are shown in Table 4.4, are referred to as preparedness (P) and responsibility (R) (Organisational culture).

4.16.2 EXTERNAL ENVIRONMENT AND NON-ORGANISATIONAL MANAGEMENT (EENOM)

External Environment and Non-Organisational Management (EENOM) is related to context or environment as identified in **Section 4.12**. The construct is also related to the policymaker element of the E-Health ecosystem (identified in Chapter 2). The component pertains to the external, that is, non-organisational elements, that are associated with cybersecurity culture.

This construct covers the external environment variables over which the healthcare institution has limited to no control. Hence, legal and regulatory requirements, competition from other institutions, and national or cultural culture are examples of environmental factors. EENOM has a relationship with organisational culture, which ultimately influences cybersecurity culture.

In this study, different names are used to refer to this component in other theoretical frameworks, as depicted in Table 4.4, have been combined to come up with the name (*EENOM*) that this component would be referred to in the context of this study. Therefore, in this study, components related to external factors, external influence, and environment (internal factor) are going to be regarded as external environment and non-organisational management. External Environment and Non-Organisational Management (EENOM) can also be used interchangeably in this study as External Environment (EE).

4.16.3 INTERNAL ORGANISATIONAL MANAGEMENT (IOM)

Internal organisational management (IOM) refers to actions taken or decisions made by the internal management of the organisation in relation to cybersecurity practices. This means that factors pertaining to this construct include all the actions that are performed at the managerial level internally and are under the control and authority of the organisation management.

The construct IOM includes factors such as cybersecurity policy, practices, security governance, organisational learning, assets, cybersecurity culture, leadership and

communication issues. IOM is related to the management factor identified in **Section 4.12**. The construct can also be said to have a similarity with E-Health institutions, which was defined as an element of the E-Health ecosystem in Chapter 2.

IOM has a bilateral relationship with organisational culture, meaning that actions, decisions, and the established practices of the internal organisation management can influence employee behaviours and can also be influenced by employee behaviours.

Due to the inconsistency in the use of the construct in other theoretical frameworks, in this study, the organisational level, internal components, organisational mechanism, and strategy are going to be regarded as Internal Organisational Management (IOM).

Internal Organisational Management (IOM) can also be referred to as Management Cybersecurity Practices (MCP) or Management (M).

4.16.4 TECHNOLOGY (TECH)

Technology (TECH) in this study means E-Health technology or systems, such as patient registration systems, and is inclusive of ICT infrastructure, frequency of change in ICT (emerging technologies), and outsources of ICT systems. The construct of technology (TECH) correlates with the element of technology identified from the cybersecurity culture definition in **Section 4.12** and in Chapter 2 as an element of the E-Health ecosystem.

The construct of technology has retained the same familiar name in this study, as it has not been explicitly discussed by other cybersecurity culture theoretical frameworks as a construct to be considered in the development and implementation of cybersecurity culture. The importance of technology as a construct of cybersecurity culture was highlighted during the review of cybersecurity culture definitions in **Section 4.12**. The technology construct in this research can be argued to have a relationship with preparedness and responsibility, internal organisation management, and external environmental and non-organisational management constructs.

4.16.5 CYBERSECURITY CULTURE

Cybersecurity culture, as defined in this study, is used as a performance tool by the management (guided through policies and procedures) to change human characteristics and their socio-cultural attributes like attitudes, assumptions, beliefs, norms, knowledge,

perceptions, skill, behaviours and practices to achieve cybersecurity at all levels of organisations and national and social structures to protect against damages from intentional and unintentional cybersecurity incidents.

The terms, cybersecurity culture, human behaviour, behaviour and people, are used by other theoretical frameworks in relation to this component. The term cybersecurity culture is maintained in the context of this study, and all these constructs discussed in this section were considered as cybersecurity culture.

4.16.6 SUMMARY OF THE CYBERSECURITY CULTURE CONSTRUCTS

Based on the review of the cybersecurity culture definitions in **Section 4.12** and the discussion of the framework in this section 4.14 and 4.16, Table 4.6 summarises the cybersecurity culture constructs that have emerged from the literature.

Table 4.6: Contributions of Literature on the Cybersecurity Culture Constructs

Cybersecurity Culture Constructs Studies	Preparedness	Responsibility	IOM	EENOM	Technology
Abeyratne (2016)	-	x	x	-	-
Ciuperca et al. (2019)	x	x	-	-	-
Da Veiga (2016)	x	x	-	x	-
Da Veiga (2019)	x	x	x	x	x
ENISA (2017)	x	x	-	x	-
Georgiadou et al. (2020b)	x	x	-	x	-
Ioannou et al. (2019)	-	x	x	x	-
Leenen & van Vuuren (2019)	-	-	-	-	-
Reid & van Niekerk (2014a)	-	x	-	-	x
Malmedal & Roislien (2016)	x	x	-	-	-
Huang & Pearlson (2019)	x	x	x	x	-
Paul & Porche (2012)	-	-	-	-	-
Saigushev et al. (2020)	x	x	-	-	-
Sousane (2018)	x	x	x	-	-
Alhogail et al., (2015)	x	x	x	x	-

Cybersecurity Culture Constructs Studies	Preparedness	Responsibility	IOM	EENOM	Technology
Bakry (2003) and Bakry & Bakry (2005)	x	-	x	x	x

The summary provided in Table 4.6 is convincing evidence that the constructs identified in this study have a theoretical grounding for an investigation of cybersecurity culture factors. The constructs form an important building block towards the design and development of a contextual framework for establishing a cybersecurity culture in public E-Health institutions.

4.16.7 CSC FACTORS MAPPED TO THE CONSTRUCTS

Using the cybersecurity culture constructs identified and discussed in **Section 4.16**, Table 4.7 maps the factors of cybersecurity culture according to the constructs it relates to.

Table 4.7: Mapping Cybersecurity Culture Factors to Identified Constructs

Cybersecurity Culture constructs Cybersecurity Culture Factors	Preparedness	Responsibility	IOM	EENOM	Technology
Training and education	x				
Awareness	x				
Top management or leadership support		x			
Cybersecurity policy and procedures		x			
Human behaviour		x			
Knowledge and understanding	x				
Cybersecurity champion or team			x		
Organisational culture		x			
Engagement, encouragement, cooperation	x		x		
Budget and resources			x		
Cybersecurity strategy			x		
Collaboration			x		
Commitment			x		

Cybersecurity Culture constructs Cybersecurity Culture Factors	Preparedness	Responsibility	IOM	EENOM	Technology
Role and responsibility	x		x		
Risk and change management			x		
Trust			x		
Communication	x				
information sharing	x		x		
Rewards and sanction			x		
Governance and control (legal and regulatory)				x	
Compliance			x		
Measure of effectiveness			x		
National culture				x	
Ethical conduct				x	
Business continuity plan			x		
Collectivism				x	
Cybersecurity hub			x		
Security audit			x		
Physical security			x		
Interest			x		
Communication channel			x		

The factors which are not mapping to the cybersecurity culture constructs (see Table 4.7) indicate the research gap. For example, top management or leadership support is not shown to be a factor of IOM.

4.17 CONCLUSION

In this chapter, a framework was articulated based on the results of the literature reviews described in (Chapter 2 and 3, which laid a foundation for the systematic review of cybersecurity culture presented in this chapter. *People*, with the support of *Technology* and *Processes*, are essential pillars in cybersecurity systems. The concepts of *Culture* and *Organisational Culture* as super-cultures that underpin cybersecurity culture were also discussed, with core cultural components identified as creating a foundation for the organisation, information, and CCSCF levels.

This chapter set out to answer the following research sub-question.

Research Sub-Question 2 (RSQ 2): *“What essential factors associated with cybersecurity culture are identified in existing literature that should be considered in developing a Cybersecurity Culture Framework for public E-Health institutions?”*

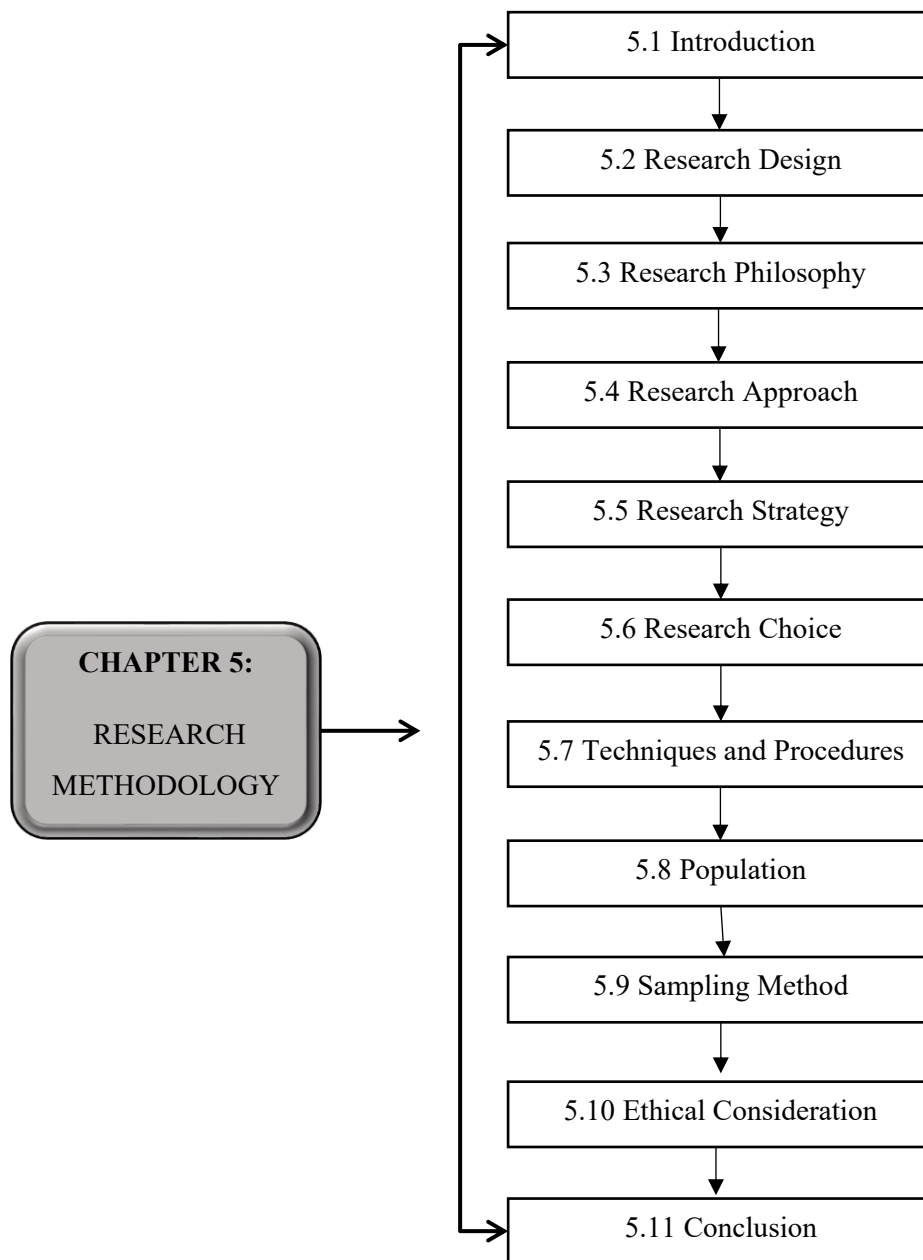
Research Sub-Question 4 (RSQ 4): *“What constructs from existing cybersecurity culture frameworks and other relevant frameworks can inform the design of a Contextual Cybersecurity Culture Framework for public E-Health institutions?”*

To achieve this, an extended systematic literature review was conducted to identify the factors associated with the creation, implementation, and management of cybersecurity culture. A total of 31 cybersecurity culture factors were identified. The majority of these are related to or can be linked to the elements and factors of cybersecurity culture that have been identified. These are, in return, equivalent to the four domains of the human factor framework.

Hence, each of the identified factors has been tentatively grouped according to the four domains of the human factor framework to facilitate understanding of that factor before cybersecurity culture theoretical frameworks are reviewed. Through the systematic review, cybersecurity culture theoretical frameworks have been identified, discussed, and conceptualised in the context of this study. As indicated at the beginning of the chapter, conducting the systematic review of this chapter assisted in accomplishing the first step (phases 1 to 3) of the conceptual framework analysis process.

Chapters 6 and 7 continue with the identification of cybersecurity culture factors, but from the E-Health context, using a combination of quantitative and qualitative methods. Activities described in these chapters still form part of phases 1 to 3 of Step 1. However, the next Chapter 5 presents the method followed in achieving the different chapters of the study.

CHAPTER 5: RESEARCH METHODOLOGY



5.1 INTRODUCTION

Research projects set out to address a central issue. The issue can be resolved through asking and answering research questions and by testing hypotheses in relation to the problem. Doing this requires a systematic approach that allows the researcher to journey from the main question of the problem to the solution. The research questions this study sets out to answer and the objectives it plans to achieve towards addressing the problem related to the CCSCF were summarised in Chapter 1. Chapters 2 and 3 laid a foundation for understanding E-Health and cybersecurity, including their benefits and challenges.

The objective of this chapter is to outline the methodological processes followed in different chapters of the study to answer the research questions and achieve the research objectives.

Section 5.2 presents the research design. Thereafter, discussions and justifications of the chosen research philosophy (see **Section 5.3**), research approach (see **Section 5.4**), research strategy (see **Section 5.5**), research choice (see **Section 5.6**), and techniques and procedures (see **Section 5.7**) are articulated. **Sections 5.8** and **5.9** presented the population and sampling method. The ethical considerations and the conclusion of the chapter are discussed in **Sections 5.9.5** and **5.10**.

5.2 RESEARCH DESIGN

A research design is the overall plan and blueprint employed to answer the research questions and achieve the research objectives (du Toit, 2015; Polit & Beck, 2008; Saunders et al., 2016). The research study was conducted using a combination of systematic literature review, conceptual framework analysis and research process onion.

Systematic literature review as a method was used to answer the **Research Sub-Question 2 (RSQ 2)** and **Research Sub-Question 4 (RSQ 4)**. Conceptual framework analysis assisted by articulating the processes and steps followed to achieve the research's main objective: *“To show and explain the processes and steps followed in the research to develop a contextual framework for establishing a cybersecurity culture in public E-Health institutions.”*

The research process onion, developed by Saunders et al. (2016), has been adopted as the methodology for conducting the empirical part of this research. The research process depicts research methodology as an onion with different layers. The layers of the onion demonstrate various aspects of research methodologies. The aim of the research onion of Saunders et al.

(2016) was to ensure the clarity and trustworthiness of an empirical research procedure. **Figure 5.1** illustrates the research onion as depicted by the authors.

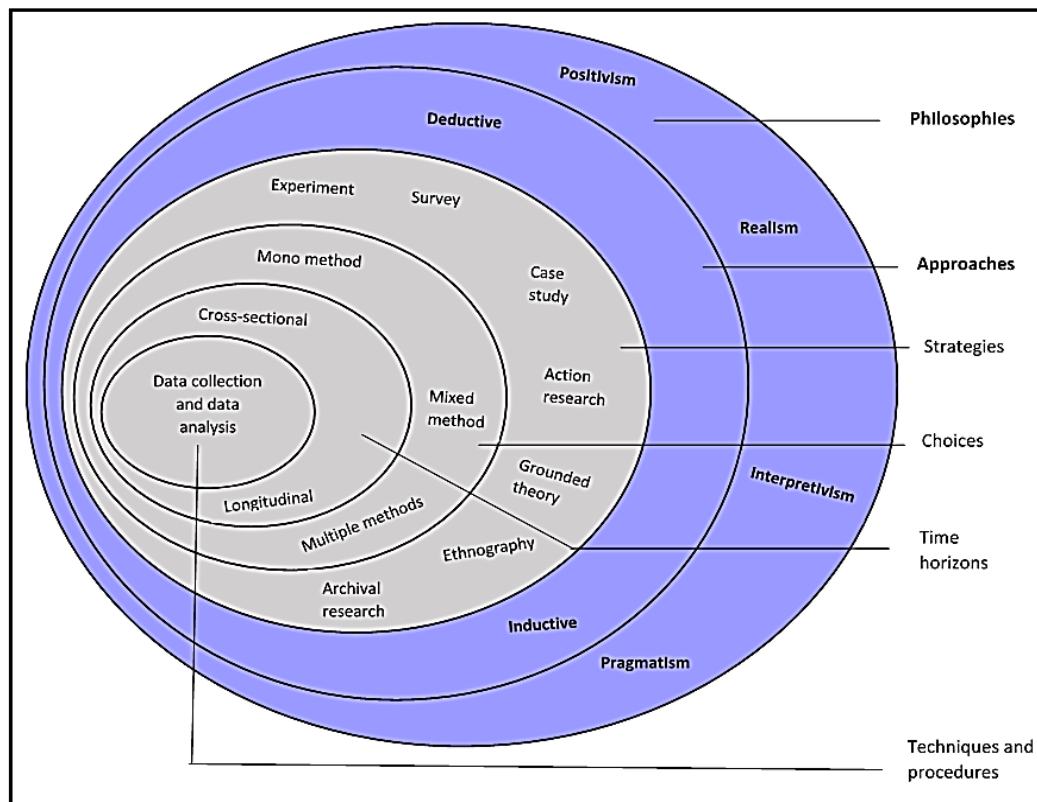


Figure 5.1: Research Process Onion (Adapted from Saunders et al., 2016)

Although various alternative research approaches could have been used in this research, such as the research process model (Oates, 2006; Oates et al., 2022) or a framework for research (Creswell & Creswell, 2018, 2023), the research approach adopted in this study followed the research process onion (Saunders et al., 2016). This is because the process enabled a systematic and logical presentation of all the research processes undertaken in this study. The research process model (Oates, 2006; Oates et al., 2022) and research framework (Creswell & Creswell, 2018) fail to present aspects of the research methodology that were detailed systematically by Saunders et al. (2016).

In addition to the systematic and logical presentations of research processes, the research process onion has been adopted as a rational framework for summarising research methodology. Also, the research onion has been successfully adopted as a methodological framework in cybersecurity culture and E-Health research (Da Veiga, 2016; Gcaza, 2017; Munyaradzi, 2018). This study followed those examples by adopting the same framework to present its methodology. **Figure 5.2** depicts the research process onion as it relates to this study.

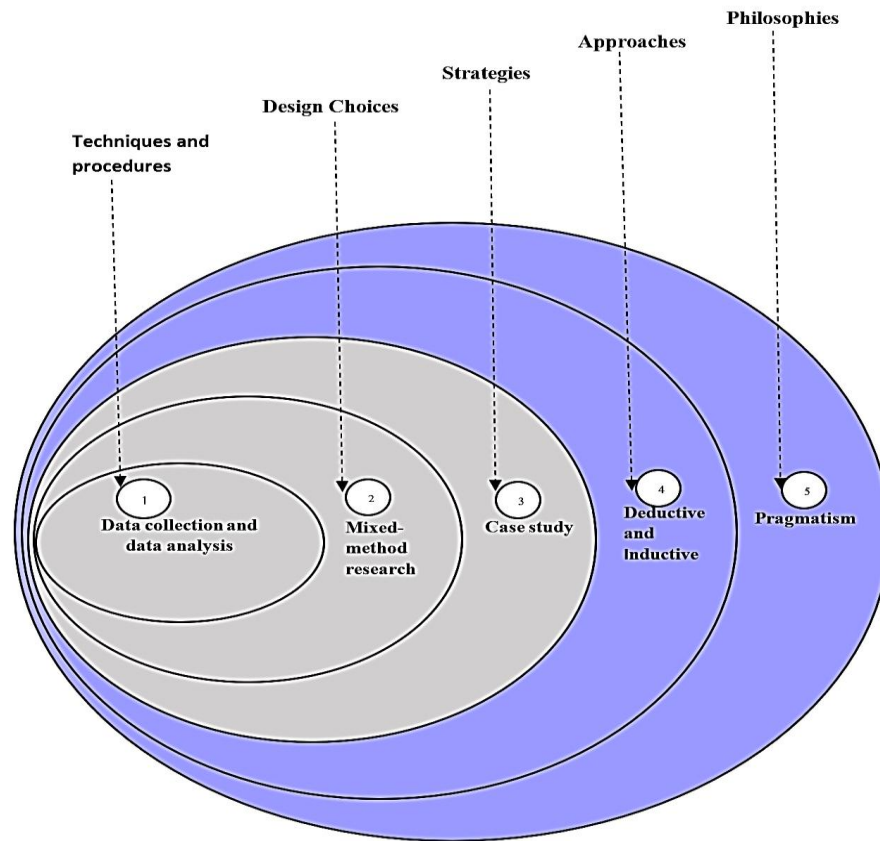


Figure 5.2: Research Process Model (Adapted from Saunders et al., 2016)

According to Saunders et al. (2016), a researcher's decision regarding the choice of a data generation method and data analysis is found at the centre of the research onion. However, before arriving at the centre of the research onion, the researcher needs to reflect upon the outer layers of the onion, which include making decisions regarding the research philosophy, approaches, strategies, choices, and time horizons that will apply (Saunders et al., 2016).

The following sections will provide an explanation of various aspects of the research process as it relates to this study, starting with the philosophical assumptions of the researcher.

5.3 RESEARCH PHILOSOPHY

Research philosophy relates to the development of new knowledge and how knowledge is generated (Saunders et al., 2016). The philosophy adopted in research depends on significant assumptions hidden in the researcher's worldview. A philosophical worldview is a general set of ideas and beliefs about the world that the researcher brings to a study (Creswell, 2014; Creswell & Creswell, 2023). Revealing the associated philosophical assumptions is essential in a research project as this guides the researcher's choice of strategy, methods and analysis

while conducting research (Creswell, 2014; Oates, 2006; Oates et al., 2022; Saunders et al., 2016).

The research process onion depicted in **Figure 5.1** identifies four research philosophies (positivism, realism, interpretivism, and pragmatism). These align with those described by Lee (2004), who argued that all research efforts adopt one of the aforementioned philosophical orientations.

The most fitting research philosophy in relation to this research is pragmatism. The philosophy and the rationale behind adopting it are presented in bullet.

The study adopts a pragmatic worldview which is appropriate given the research objectives of examining both measurable patterns and context-specific perspectives within public E-Health institutions. The pragmatic view recognises that no single methodological tradition is sufficient for capturing social-technical phenomena. Therefore, according to this worldview, the research question should guide the choice of method.

Mixed Method Research (MMR) was employed in this study to integrate the quantitative and qualitative findings and thereby to strengthen the investigation on cybersecurity culture. Quantitative research identifies associations, and qualitative research identifies insight and explains underlying meaning and contextual factors. The integration of these two approaches helps to deepen our understanding of cybersecurity culture and hence facilitates the effective development of a cybersecurity culture framework. As a result, the integration of the data obtained from the two methods allowed the study to address the what and the why of cybersecurity culture development.

- **PRAGMATISM**

Pragmatism is argued by this researcher to be the worldview that most closely matches research intended to develop a contextual framework for establishing a cybersecurity culture in public E-Health institutions in South Africa.

Pragmatism bases its principles on the practical consequences that flow from acceptance of belief (Rylander, 2012). Other research concurs with this view by indicating that the main concern with pragmatism is putting the solution of the problem into practice (Patton, 1990), and answering the research question (Saunders et al., 2016). This means that for the pragmatist, getting to the end (research question answered) and having a practical use of what was done are the ultimate goals.

Saunders et al. (2016) argued that the research question is the most important determinant of the epistemology, ontology and axiology adopted in research. Research questions are crucial in any research and are closely linked to the objectives the research intends to achieve. With the pragmatist worldview, researchers should choose the methods, techniques, and procedures that best answer their research questions (Creswell, 2014).

This research indicated in **Section 1.2** that cybersecurity culture was viewed as an ill-defined research problem. As such, following a methodological perspective that requires the researcher to be totally objective or totally subjective throughout the entire study will put limitations on answering the main research question:

“How can a contextual framework for establishing cybersecurity culture in the public E-Health institution in South Africa be developed and evaluated”?

Therefore, as a start before developing the proposed framework for this research, the researcher came from a perspective of pragmatism. This worldview permitted the researcher to be objective in a situation that requires objectivity and subjective in a circumstance that needs a subjective approach. The framework was expected to articulate and document a validated shared assumption that underpins how cybersecurity is viewed and how to respond to cybercrime and threats in the E-Health institutions among E-Health system users.

This researcher argued, therefore, that unless the elements that constitute the CCSCF in the E-Health institutions were derived from the practical experiences of social actors in E-Health institutions, the developed framework might become ineffective as it would, in some circumstances, fail to assist with the establishment of cybersecurity culture when put into practice.

In this research, the researcher was in search of ‘the truth’ on the issue of cybersecurity culture and was aware that ‘the truth’ can vary depending on who the participants are. Hence, following the pragmatist philosophy allowed the researcher the opportunity to adopt a method, technique and procedures that were best at a given moment to get the truth.

The major disadvantages of pragmatism include its ambiguity and vagueness at times. This is tied to the fact that pragmatism is not clearly committed to positivism or interpretivism. To address this problem, the current research was strategic in its choice of approaches and data collection methods. Data collection methods were selected to accommodate the two research approaches that underpin pragmatism.

Section 5.4 unpacks the approaches the researcher follows to answer the research questions and achieve the research objectives.

5.4 RESEARCH APPROACH

The two research approaches in the research onion are deductive and inductive. (Saunders et al., 2016). These are also the two main research approaches described by Dahlberg & Mccaig (2010). The different research approaches are discussed below, followed by a justification of the approaches chosen for this study.

5.4.1 DEDUCTIVE RESEARCH APPROACH

Deduction is a research approach that is dominant in natural science research. The deductive approach is top-down, using theory as a starting point (Dahlberg & Mccaig, 2010). The approach generally tests existing theory through formulating hypotheses and setting out to prove or disprove these using quantitative data collected in a controlled environment using a structured method (Saunders et al., 2016).

Therefore, the deductive approach is generally used to test existing theories rather than to develop new perspectives that might challenge already existing ideas (O'Reilly, 2009). This presents a significant drawback of the deductive approach because the focus of the research will be restricted, and perception distorted if data are collected solely based on existing theories. This limitation was overcome in this study by not adopting or basing the development of a quantitative instrument on pre-existing theoretical instruments. Instead, instruments were freely developed and categorised under the identified constructs.

Section 5.4.2 describes the inductive research approach.

5.4.2 INDUCTIVE RESEARCH APPROACH

The inductive research approach enables the researcher to start with limited preconceptions and allows theory to emerge from the empirical data collected and analysed (O'Reilly, 2009). This approach focuses on understanding the way in which humans interpret their social world.

In the case of this research, the researcher argues that research on cybersecurity culture views people as humans whose actions (intentional and unintentional), education, and awareness are a result of the meaning they attach to the phenomenon, cybersecurity. The inductive research approach begins with a research question, which guides the researcher's collection of empirical

data about the social world, followed by analysis, which assists the researcher to obtain and share an understanding of reality, and lastly, a theory is developed.

The inductive approach is a bottom-up approach (Dahlberg & Mccaig, 2010). According to Dahlberg and Mccaig (2010), a research study conducted on the grounds of an inductive approach starts with an empirical data collection process that is flexible. The inductive approach can allow changes to the original research question or the introduction of a new question at any time until the researcher becomes familiar with the research context and the phenomenon under study.

Creswell (2014), and Creswell and Creswell (2018) suggested that there should be an emphasis on research and the nature of the research topic as these are the most important criteria for selecting a research approach. It may be appropriate to use the inductive approach for a new research topic with limited existing literature (Creswell, 2014). The approach enables the researcher to generate data, analyse it, and reflect upon the theoretical themes the data suggest.

5.4.3 APPLYING DEDUCTIVE AND INDUCTIVE APPROACHES

This study applied a combination of the deductive and inductive approaches. This accommodated the principle of pragmatism as a research philosophy with no static set of perspectives or techniques limiting the exploration of the research problem.

This study did not test existing theories, and no predefined hypothesis was deduced from existing theories. Therefore, the deductive approach was ruled out as the sole approach for this research study. However, a deductive approach was applied for the analysis of the Round 2 data collection (using questionnaires). The deductive approach was applied at this stage of data analysis because the researcher had already identified core constructs from the initial round of data collection, the systematic literature review. Therefore, the researcher approached the analysis already having preliminary constructs that were intended to be triangulated for verification and validation purposes. The deductive approach was also partly applied in the Round 3 data analysis (qualitative) at Stage 3 of thematic analysis in Chapter 7. This was done during theme creation by linking the categorised codes with pre-existing cybersecurity culture terms from literature.

Justifying the choice of inductive approach in this research relied on the fact that cybersecurity culture is a new research topic in the area of E-Health. It is considered an ill-defined problem as limited literature exists in the area. Therefore, approaching the research from an inductive

viewpoint afforded the researcher the opportunity of having a flexible structure to permit changes as the research progressed. The inductive approach's flexibility also ties in with that of pragmatism, which was the adopted research philosophy for the current research.

Qualitatively, an inductive approach was achieved in Stage 2 of the thematic analysis method through open coding as described in Chapter 7. The coding of data chunks was not approached with pre-defined names. Instead, meaningful names were given to data segments to help develop a better understanding of cybersecurity culture. Also, in Stage 3 of the thematic method, an inductive approach was applied for code categories that did not fit existing cybersecurity culture terms. For such code categories, the researcher allowed themes to emerge based on the categorisations or the meaning attached to them.

An inductive approach was adopted in this research to get a feel of what was going on in the E-Health institutions and to understand the nature of their cybersecurity problems and the cybersecurity culture in the sector. The researcher wanted to understand the meaning humans (in the case of this research, E-Health system users and ICT staff) attached to incidents related to cyber threats and cybersecurity by asking research questions that led to the collection of empirical data from the social actors.

This approach enabled the researcher to focus on understanding cybersecurity culture in the context of E-Health institutions where the research took place. By analysing collected data, the approach contributed to understanding the reality concerning cybersecurity culture in E-Health institutions through the identification of factors associated with cybersecurity culture. Ultimately, this led to the development of a contextual cybersecurity framework.

The next section explores the research strategies for the research study.

5.5 RESEARCH STRATEGY

A research strategy is the researcher's overall approach to answering research questions (Oates, 2006; Oates et al., 2022). Research strategy is a technique that guides the whole research process, so that research questions can be answered (Yin, 2014).

What is important in selecting a research strategy is deciding whether it would enable the researcher to answer research questions and meet research objectives. Hence, the choice of research strategy should be guided by the research questions and objectives, the extent of existing knowledge, the amount of time and other resources available, as well as the researcher's philosophical beliefs (Saunders et al., 2016)

The choice of the research strategy should be guided by the research purpose, irrespective of whether the research is exploratory, descriptive, explanatory or a combination of purposes. This research employed a combination of exploratory and descriptive studies. The exploratory research approach enabled the researcher to find out what was happening in the field to obtain insights into cybersecurity culture in the E-Health environment and to ask questions in this data-sensitive environment.

The research extended the exploratory work that was already done by adding a descriptive view. This allowed the researcher to present a multifaceted and realistic profile of the phenomenon of cybersecurity culture in the context of public E-Health institutions. According to Saunders et al. (2016), an essential practice when conducting descriptive research is to have a good knowledge of the phenomenon of interest before data collection. This is the case in this research, where the systematic literature review was conducted first, and later quantitative and qualitative data were collected to get a clear picture of the phenomenon of cybersecurity.

Table 5.1 highlights seven research strategies (experiment, survey, case study, action research, grounded theory, ethnography and archival research) (Saunders et al., 2016). These strategies are not tied to a specific research purpose; any research purpose can employ any strategy (Yin, 2003). The purposes of the strategies and their applicability in this research study are summarised in Table 5.1 in no particular order.

Table 5.1: Summary of Research Strategies and Their Applicability in this Research

Research strategy	Purpose/ description	Applied in this research?
Experiment	Study causal links between a factor and an observed outcome (Oates, 2006). It investigates if a change in an independent variable will have an effect on another dependent variable.	No: the current research will not be conducted in a controlled environment like a laboratory. As a result, this strategy will not be employed.
Survey	This is a strategy that usually uses questionnaires to collect quantitative data from a large number of people (Saunders et al., 2016). The focus is on collecting the same kind of data from a large group of people with the purpose of generalising to larger groups (Oates, 2006).	No: Although part of the Round 2 data collection in this study was achieved using a survey strategy, namely a questionnaire, to collect quantitative data, the data was not collected from a large number of participants. As a result, this research does not employ a survey strategy as it failed to meet the major requirement of the survey (collecting data from a large number of people).

Research strategy	Purpose/ description	Applied in this research?
Case study	Empirical investigation of a phenomenon of interest within its real-life context (Robson, 2002).	Yes: cybersecurity is studied within the context of public E-Health institutions. This strategy helped generate answers to the “what” questions asked in the research.
Action research	Participative and democratic research strategies are used by professionals to investigate and improve their own working practices (Oates, 2006).	No: The aim of the research was to develop and evaluate a framework that could potentially be of practical use by public E-Health institutions when addressing cybersecurity challenges. The researcher was not working with the participants to implement the framework. The researcher is not a practitioner in the health sector. As a result, she was not directly involved in taking any practical operational actions to address the challenge of cybersecurity using the developed framework.
Grounded theory	Participants' views are the ground upon which general, abstract theories of a process, action or interactions are derived (Creswell, 2014). Grounded theory is an inductive and deductive approach.	No: The research did not develop any new theory. Instead, a contextual framework was developed from data generated through various rounds and methods of data collection.
Ethnography	“studies shared patterns of behaviours, languages, and actions of an intact cultural group in a natural setting over a prolonged period of time” (Creswell, 2014).	No: Ethnographers take part in the life of the people in the field, meaning they carry out participant observation. Firstly, this research did not do that. Secondly, data collection in this research will not be done over a prolonged period.
Archival research	Evidence and data are collected primarily from administrative records and documents (Saunders et al., 2016).	No: document analysis would not be used as a research strategy but rather as a means of secondary data collection.

Sections 5.5.1 to 5.5.3 elaborate further on the case study, systematic literature review and conceptual framework analysis research strategies.

5.5.1 CASE STUDY

Yin (2014), in the first part of the two-fold definitions, defined a case study as a research strategy that investigates a contemporary phenomenon in its real-world context. This is usually done in situations where the boundaries between the phenomenon and context may not be clearly evident (Yin, 2014). A case study is defined as a strategy for doing research that

involves an empirical investigation of a particular contemporary phenomenon within its real-life context using multiple sources of evidence (Robson, 2002). It is evident that a case study emphasises the importance of context and contemporary phenomena (Robson, 2002; Yin, 2003, 2014).

Since the main objective of this research was to *develop a contextual framework for establishing cybersecurity culture in public E-Health institutions in South Africa*, a case study was deemed the appropriate strategy.

Saunders et al. (2016) argue that a case study offers the opportunity to explore and understand the research context and is not limited to predefined variables for data collection. Following the case study strategy helped the researcher to gain a rich understanding of the phenomenon of cybersecurity culture in the context of public E-Health institutions. The case study strategy also afforded the researcher the opportunity to identify cybersecurity culture concepts to be used in the contextual framework. A good result could be achieved by having exposure to the natural settings of the case being studied and by engaging directly with participants working in that organisation.

In addition to focusing on the real-world context of a research phenomenon, the choice of the case study strategy is dependent on the research question, the extent of the researcher's control over behavioural events, and the degree of focus on contemporary historical events (Yin, 2014).

The main question of this research was, "*How can a contextual framework for establishing cybersecurity culture in the public E-Health institution in South Africa be developed and evaluated?*" This prompted the researcher to reveal the prevailing circumstances and operations in terms of the culture of cybersecurity in the public E-Health institutions, and from there to develop a contextual framework for cybersecurity culture.

The focus of the research question was on "How", and Yin (2014) argued that a case study is the preferred strategy in research with such a question. Since this research was expected to collect data using various data collection methods, the researcher knew that she would have no control over the behaviour of participants or events, and this strengthened the choice of the strategy for this research. Lastly, the phenomenon of cybersecurity culture, which was to be studied, was not being studied from a historical position; it was considered to be a contemporary phenomenon.

Criticisms of the case study strategy include difficulties in generalising results, lack of rigour, and bias. However, the quality of case-study research can be enhanced by the researcher ensuring its validity and reliability (Wedawatta et al., 2011; Yin, 2014).

The study collected data from more than one hospital as the inclusion of multiple cases increases confidence in the research findings (Yin, 2014). An embedded approach was followed because different groups (ICT staff, medical professionals, and administrative staff) were selected from the public E-Health institutions that were examined. The next section describes the selected cases. In the qualitative data collection, there were five employees from a single district-level hospital (Carolina) and four employees from a provincial or tertiary hospital (Witbank). Quantitative data was collected from 53 participants from the Witbank provincial hospital and 46 participants from the Carolina district hospital.

However, the researcher realised during the qualitative data collection that the major ICT function was centralised at the provincial level in Mpumalanga. This means that no ICT department was located at any of the provincial hospitals (other than limited technical support, which was located at the district level). The ICT department was made up of the following sections: support, system, server, governance (this section was dormant), and client service.

The case study strategy was selected as it facilitates an in-depth examination of real-world organisations' practice, ensuring methodological triangulation. This study followed a convergent parallel mixed method, as indicated in Chapter 4, for empirical data collection and analysis. With this approach, multiple data sources, such as quantitative survey response (Chapter 6), qualitative interview (Chapter 7) and the systematic literature review (Chapter 5), were used to collect data which was analysed separately to ensure triangulated results (Dawadi et al., 2021). Triangulation enhances credibility by enabling convergence and comprehension across data types.

5.5.1.1 Defining the Cases

Section 5.9 gives details regarding the three sampling techniques employed in this research; these were convenience sampling, judgment (also known as purposive sampling), and snowball sampling. For convenience, the research focused on the Mpumalanga province located in the North-East of South Africa. Mpumalanga is one of the nine provinces of South Africa. In the province, two categories of hospitals (district and tertiary hospitals), located in the rural and urban areas, were selected.

Mpumalanga has a single Department of Health, which manages all the healthcare facilities within the province. ICT services are centralised in the province, meaning that all ICT-related matters, including cybersecurity, are handled at the provincial level. The province has three districts: Ehlanzeni, Nkangala and Gert Sibande. Each of these has 5 or 6 sub-districts. Each district contains at least one and no more than three healthcare facilities in the form of hospitals and clinics. The hospitals vary between district (small, medium or large) hospitals, provincial tertiary hospitals, and regional specialised TB hospitals.

5.5.1.2 Case Study 1: Carolina Hospital

Figure 5.3 shows the entrance to the Carolina hospital.

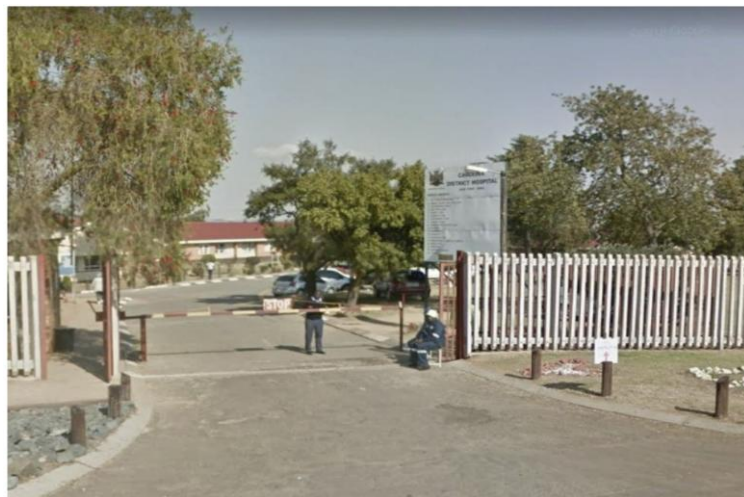


Figure 5.3: Carolina Hospital (Internet)

Carolina Hospital is a public healthcare hospital located in Mpumalanga Province in South Africa. According to the National Health Act (2003), which gives the regulations relating to categories of public hospitals, Carolina is a Small District Hospital. The healthcare institution is in the District Municipality (DM) of Gert Sibande, which is a sub-district in Albert Luthuli Local Municipality (LM) (Department of Health, 2012b).

5.5.1.3 Case Study 2: Witbank Provincial Tertiary Hospital

Figure 5.4 shows some of the buildings of the Witbank hospital.



Figure 5.4: Witbank Hospital (Internet)

Witbank Hospital is a public healthcare hospital located in Mpumalanga Province in South Africa. According to the same National Health Act (2003), Witbank is a tertiary Hospital. The hospital is found in the sub-district of Emalahleni Municipality (LM), which falls under Nkangala Municipality (DM) (Department of Health, 2012b).

The study is now understood to be a case study, and the cases are defined. The next section discusses systematic literature review as the methodological strategy followed to understand related research available covering the topic of cybersecurity culture.

5.5.2 SYSTEMATIC LITERATURE REVIEW

A literature review is an important aspect of all academic research, and it is used to establish the foundation of academic inquiries (Xiao & Watson, 2019). Various types of literature reviews exist (Okoli & Schabram, 2010). In this research, a type of literature review known as a systematic literature review (also known as a stand-alone literature review) was followed.

“A research literature review is a systematic, explicit, and reproducible method for identifying, evaluating and synthesising the existing body of completed and recorded work produced by researchers, scholars, and practitioners”(Fink, 2014).

A systematic literature review is defined as *“a means of identifying, evaluating and interpreting all available research relevant to a particular research question, topic and area or phenomenon of interest”* (Kitchenham & Charters, 2007).

Many other definitions of systematic literature review exist. Since the Fink (2014) definition accommodates many characteristics of a systematic literature review, namely, explicit,

repeatable, systematic, complete, rigorous and synthesising, this research will adopt the definition as that of a systematic literature review. In this study, the phenomenon of cybersecurity culture was systematically reviewed to explicitly identify, evaluate and synthesise existing research in the area.

5.5.2.1 Why Was a Systematic Literature Review Carried Out?

Research has indicated that a literature review is an important starting point for any research project (Hart, 2018; Xiao & Watson, 2019). However, some researchers argue that unless a literature review is thorough, fair and scientifically rigorous, it is of little scientific value (Kitchenham & Charters, 2007; Okoli & Schabram, 2010).

A systematic review synthesises existing work in a way that is seen to be fair (explicit), reliable and repeatable. This is achieved by conducting the review using a predefined search strategy and by using a rigorous and auditable methodology that has been defined before the start of the review process (Kitchenham & Charters, 2007). Lavalley et al. (2014) added that the review must be complete and repeatable.

To ensure that the major contribution of this study, developing a contextual framework for establishing cybersecurity culture for public E-Health institutions, was of scientific value to the academic communities, a systematic literature review was conducted in the research area of “Cybersecurity Culture”.

Although the purpose of a systematic literature review is not considered to be a step in the formal research process (see Subsection 5.5.3) adopted in this research, it is an essential step in other research processes (Kitchenham & Charters, 2007; Okoli & Schabram, 2010). As a result, this research deemed it important to highlight the purpose of the review before proceeding by explaining the systematic review process of this research.

The purpose of the systematic literature review was threefold. Firstly, it provided the researcher with a theoretical background (through aggregation, interpretation and explanation) of previous work done in the area of cybersecurity culture in the context of E-Health. Thereby strengthening the researcher's understanding of the research domain. Secondly, it identified gaps that existed in the literature in the area of CCSCF that the current research intended to fill. Thirdly, it assisted the researcher in developing a framework to position cybersecurity culture in the E-Health domain.

Various systematic literature review processes exist (Fink, 2014; Kitchenham & Charters, 2007; Levy & Ellis, 2006; Okoli & Schabram, 2010; Xiao & Watson, 2019). For this research, the researcher used the systematic literature review process by Xiao and Watson (2019). However, to ensure the inclusion of various other aspects of a systematic literature review, where necessary, reference was made to the best practices of other authors.

The review process by Xiao and Watson (2019) was used because those authors clearly described the best practices from various literature review processes. Xiao and Watson (2019) achieved this by conducting a systematic search on the literature review methodology to develop their own steps for conducting a systematic literature review. The review process followed by Xiao and Watson (2019), like many systematic literature review processes, was based on three basic steps (plan, conduct and report the review) and their sub-steps.

Xiao and Watson (2019) indicate that despite the existence of various approaches to carrying out a literature review, the majority of reviews are conducted by following eight simple processes (see Table 5.2).

Table 5.2: Eight Step Process for Systematic Literature Review

Systematic Literature Review Steps	
1. Formulate the research problem	5. Assess quality
2. Develop and validate the review protocol	6. Extract data
3. Search the literature	7. Analyse and synthesise
4. Screen for inclusion	8. Report the finding

These eight steps, grouped into three processes, formed the basis of the systematic literature review conducted in this study. **Figure 5.5** summarises the review process and steps followed, and how they were applied in this study.

The process depicted in **Figure 5.5** was iterative, as are many other review processes (Lavallée et al., 2014). While conducting the review, issues that require changes to the previous steps may arise (Xiao & Watson, 2019). The iterative process is depicted in **Figure 5.5** with the arrow going backwards from conducting the review to planning the review.

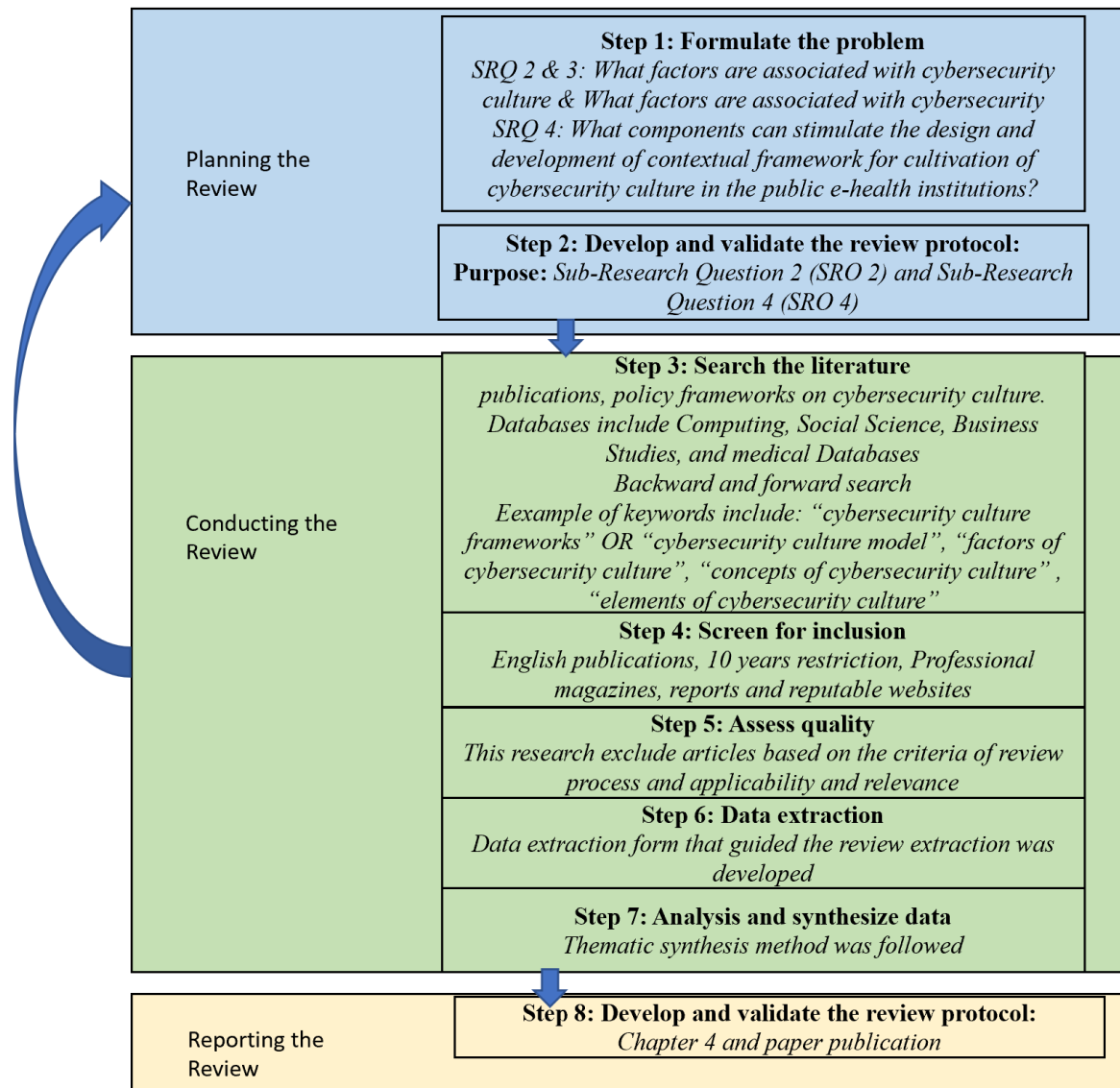


Figure 5.5: Systematic Literature Review Process (Xiao & Watson, 2019)

The following sections explain how the processes and steps were adopted in this research.

5.5.2.2 Formulating the Review Question

Developing and specifying the research questions is the first and arguably the most important part of any systematic literature review, as it provides a framework that drives the development and conduct of the entire review (Kitchenham & Charters, 2007). The systematic review methodology is based on the following three requirements:

- The search process must identify primary studies that speak to the research questions.
- The data extraction process must extract the data needed to attend to the research questions.

- The data analysis process must synthesise data in a way that answers the research questions.

Once the research questions have been formulated, search inclusion and exclusion criteria can be developed by focusing on the concepts identified in the research questions. Having precise, well-defined, and focused research questions clearly identifies the data the reviewer needs to look for to arrive at a credible conclusion.

The researcher revisited the main research questions and sub-questions formulated in Chapter 1 to help guide the systematic literature review process. However, other questions also emerged as the review process progressed.

The main research question:

“How can a contextual framework for establishing cybersecurity culture in the public E-Health institution in South Africa be developed and evaluated”?

The sub-questions that assisted in answering the main research question and the guiding questions related specifically to the search for relevant literature are presented below:

RSQ 2: *What factors are associated with cybersecurity culture in the literature?*

- What work has been done in the area of cybersecurity culture in literature?
- What factors were considered in the discussions and development of Cybersecurity Culture?

RSQ 4: *What components from existing cybersecurity culture frameworks can stimulate the design and development of a contextual framework for establishing cybersecurity culture in public E-Health institutions?*

- What components were considered in the development of the existing CCSCF?
- What are the factors that can be considered to develop a cybersecurity culture in E-Health institutions?

5.5.2.3 Develop and Validate the Review Protocol

A review protocol is a plan that stipulates the method the researcher will use in conducting the review (Okoli & Schabram, 2010). Planning and documenting the review methods in advance can improve the quality of the resulting review and increase its reliability. In addition, it

addresses the possibility of researchers introducing bias in the review. In this research, the review protocol outlined the strategy for each step of the systematic review process.

The elements of the review protocol as they relate to this study are purpose, search strategy, inclusion criteria, quality assessment, data extraction and data synthesis.

- Purpose

The purpose of conducting a systematic literature review was to identify factors that were associated with cybersecurity culture and to identify components in the literature that could be used in the CCSCF. Achieving these objectives assisted in answering *Research Sub-Question 2 (RSQ 2)* and *Research Sub-Question 4 (RSQ 4)*.

- Search strategy

The systematic review search process was limited to obtaining publications that were peer-reviewed and official documents. Publications searched included peer-reviewed conference papers, peer-reviewed journal publications, policy frameworks on cybersecurity culture and credible information based on reports regarding cybersecurity and cybersecurity culture from reputable professional magazines. Basing the systematic review on peer-reviewed publications and official documents (for example, policy documents) gave the researcher confidence to use the work of others as a stepping-stone in order to advance insight into cybersecurity culture in the E-Health sector.

Table 5.3 provides the list of databases and other sources that were searched to ensure the inclusion of relevant articles in the areas of interest.

Table 5.3: List of Databases Searched for the Literature Review

Computing, Social Science and Business Studies Databases
IEEE (Comp Soc & Xplore) ACM (Digital lib) ProQuest (ABI/INFORM) Elsevier (ScienceDirect) EBSCOhost INFORMS Scopus AiSeL Web of Science Computing: https://libguides.unisa.ac.za/c.php?g=355509&p=2399881 Business databases: https://libguides.unisa.ac.za/c.php?g=355705&p=7722082 Social Science database:
Medical Database
PUBMED Other Medical and Health related databases: https://libguides.unisa.ac.za/c.php?g=355612&p=2398423 https://libguides.unisa.ac.za/c.php?g=355427&p=2400122
Open Access to Thesis and Dissertation (OATD)

Cybersecurity is a multi-disciplinary research phenomenon, and therefore, the databases that needed to be searched covered several disciplines. A search including several different databases helped the researcher to gather a comprehensive list of peer-reviewed articles and relevant materials from various publishers.

With the assistance of a research librarian and the thesis supervisor's guidance, the following keywords were used during the initial search to retrieve literature useful for answering the research questions.

“cybersecurity culture frameworks” OR “cybersecurity culture model”, OR “cybersecurity cult*”, “Cybersecurity Culture” “aspects of cybersecurity” OR “factors of Cybersecurity Culture”, “concepts of Cybersecurity Culture”, “elements of Cybersecurity Culture”.

Conducting a meaningful keyword search is the first technique to master when conducting a literature search (Levy & Ellis, 2006). Using the keywords listed above assisted the researcher in retrieving the most relevant articles for inclusion in the review. The search process went through various iterations until the researcher was satisfied that sufficient literature had been selected. The keywords produced a high volume of literature that had “Cybersecurity Culture” in the title, abstract or in the body of the literature. The researcher reviewed the titles and abstracts to select articles that seemed likely to help answer the research questions. After this preliminary assessment of the titles and abstracts, the full text of the selected articles also needed to be assessed for relevance and applicability to the research topic.

Information system literature is diverse and multidisciplinary in nature. Hence, to consult all literature sources and obtain a wide variety of literature on the phenomenon of cybersecurity culture, the researcher utilised three techniques (Levy & Ellis, 2006). As a result, the research strategy involved not only a keyword search but also a subsequent search for articles from the reference sections of the articles retrieved initially.

A backward and forward search helped ensure the rigour of the search process and avoided publication bias to ensure that high-impact articles were included. The backward search included reviewing references used by the articles selected during the keyword search, reviewing what the authors had published before the current article, and reviewing keywords used in the articles yielded from the initial keyword search. The forward search included reviewing research articles published more recently that referenced the paper and reviewing the author’s publications following the paper under review.

The bibliographic details of the articles selected during the literature search were saved on Mendeley, and the full text was downloaded onto the CD drive of the researcher. The literature was managed using Mendeley Library Manager. (Mendeley is a reference management software that enables the researcher to organise a personal document library and text references.) Thereafter, the articles saved on the CD drive were transferred to ATLAS.ti.

ATLAS.ti. is a software application that assists the researcher in analysing and reviewing the identified articles during the data extraction and synthesis stages. The Preferred Reporting Items for Systematic Review and Meta-Analyses (PRISMA) flow diagram was used to depict

the processes followed to arrive at the selected literature for inclusion and synthesis in the research.

- Inclusion criteria

Since the term ‘cybersecurity culture’ was considered ill-defined, the inclusion criteria for the systematic review were not limited to journal articles and conference papers. Professional magazines, reports and reputable websites were also selected for review, provided they were published or made available in English. Cybersecurity culture is a relatively new research area, and a fairly limited amount of research literature exists, particularly in the area of E-Health. Therefore, a fairly generous 10-year restriction was placed on the publication year of research articles that were selected for review.

Since peer-reviewed papers from high-impact journals formed a major part of the systematic review, the researcher assumed that English versions of high-impact papers on the topic “Cybersecurity Culture”, translated from papers published in other languages, were also available. Hence, no important literature was excluded from the review due to language.

- Quality assessment

Quality assessment, a method for screening for inclusion, enabled the reviewer to state explicitly the criteria used to justify the inclusion of articles that were of sufficiently high quality (Okoli & Schabram, 2010). Levy and Ellis (2006) warned that not all published materials are of a high quality. These authors indicated that researchers should make special efforts to avoid papers that are not peer-reviewed or practitioner-oriented. Other researchers have also emphasised the importance of making use of peer-reviewed publications as a cornerstone for identifying new concepts and for advancing new insight (Davison et al., 2005).

This stresses the point made earlier that a systematic literature review has to be rigorous, explicit and not biased. To achieve these qualities, assessments of the literature that underpinned the review in this research were considered essential.

To ensure the quality of the literature reviewed, this research excluded articles based on:

Review process: Special care was taken to ensure that articles selected for the systematic review did not include or included only a limited number of works that were not peer-reviewed or practitioner-based. However, unless the non-peer-reviewed documents (from magazines and

newspapers) were endorsed by reliable sources (cybersecurity associations or professional bodies) and contained factual information, they were not selected.

The literature search included searching all the databases that house highly ranked IS journals and conference publications, in addition to other sources, so as to ensure the inclusion of all relevant articles. Moreover, IS articles that were not from the top-ranked IS journals or conferences or were from sources that were not endorsed by reputable research or professional associations were excluded.

Applicability and relevance of selected literature were other important inclusion factors that were considered. Each item of literature retrieved was evaluated regarding its relevance and applicability for the current research. Studies were applicable if they were in the field of ‘cybersecurity culture’ and could conceivably contribute to answering the research questions.

The literature contains various frameworks and checklists for assessing the quality of research to be selected for systematic review (Fink, 2014; Gough, 2007; Pawson et al., 2003; Petticrew & Roberts, 2006; Thomas et al., 2012). However, since this research emphasised the importance of focusing on peer-reviewed articles published in top accredited journals, the researcher accepted that the selected articles had already been reviewed based on the criteria given in those quality frameworks and checklists. Hence, in this research, the researcher did not follow any specific framework or checklist. Instead, the quality of the selected articles was assessed based on their relevance to the current research argument, the review processes the papers went through, and the published journals.

- **Data extraction**

Data extraction is a process that involves identifying essential characteristics of the appraised studies and coding them (Stanley, 2001). Gough et al. (2017) define data extraction as noting from each article in the literature review a description of how the study was conducted and the findings of the study. Xiao and Watson (2019) also say that coding is part of the data extraction process.

Codes are assigned to sections of text by researchers to categorise the underlying literature (Miles et al., 2019). The way in which the selected studies are coded will have a direct impact on the outcome of a systematic review (Xiao & Watson, 2019). It is important that researchers establish whether the coding will be based only on the data itself (inductive) or on pre-existing

concepts (deductive) (Suri & Clarke, 2009) and also decide between manual or computer-aided coding (Massaro et al., 2016).

In the data extraction stage of the systematic review a data extraction form must be designed to assist researchers to scan the selected studies and to collect specific information needed to answer the review questions (Kitchenham & Charters, 2007). Designing data extraction forms at the start of the review protocol helps reduce errors and biases in the review process.

Table 5.4 depicts the data extraction form designed for this research. The form listed the categories that were to be used to classify each selected study. The studies were assigned different codes depending on whether they were defining cybersecurity culture, discussing its concepts, or developing a framework for use in other contexts. Other articles were classified based on the issues discussed in the articles.

Detailed information and the characteristics (using the relevant codes) of the selected studies were captured electronically using the data extraction form. A combination of inductive and deductive coding approaches was employed. This enabled the researcher to accommodate both predetermined coding categories as well as codes that emerged during the data extraction process and synthesis. Examples of the predetermined coding categories that were used are CCSCF, definition, and factor or component. The data extraction process and synthesis of this research were achieved using ATLAS.ti software. ATLAS.ti is a qualitative data analysis tool. The software helped the researcher arrange, reassemble and manage data in the selected studies in a creative yet systematic way.

Table 5.4: Data Extraction Form

General information of the study
Title, author, publication year
Type of publication (journal, conference, etc.), publication country
Studied countries, and citation (database)
Study characteristics
Purpose/aim/objectives of the study
Study strategy (survey, literature review, case study, quantitative modelling, etc.)
Data collection method (questionnaire, interview, experiment, observation, focus group, literature review, etc.)
Data analysis (quantitative, qualitative or mixed method).
Inclusion and exclusion criteria

General information of the study
Participants characteristics
Individual, organisation, national or international level
Participant job title/positions in the organisation
Other descriptions of the participants
Industry/Sector
Health, Financial, Defence/Military, Education, others
Topics/classification schemes// Research activities
Cybersecurity Culture: definition, framework, components, and aspects/factors
Articles identified will be classified based on their content
Outcomes/findings/results
Relevant and domain-related outcome

- Data synthesis

Synthesis combines elements or sets of items to generate new knowledge grounded in the findings or results of multiple research studies (Thomas et al., 2012). Hence, synthesis describes the findings of a collection of studies to facilitate conceptual innovation. Although grounded in the studies, synthesis can go beyond the content of those studies.

Dixon-Woods et al. (2004) discussed integration and interpretation as two primary aims of synthesis. According to Thomas et al. (2012), the two broad modes of synthesis are configuration and aggregation. A synthesis that configures the findings of a collection of studies generates new theories or builds hypotheses, while a synthesis that aggregates the findings from a collection of studies tests the theory or hypothesis (Thomas et al., 2012).

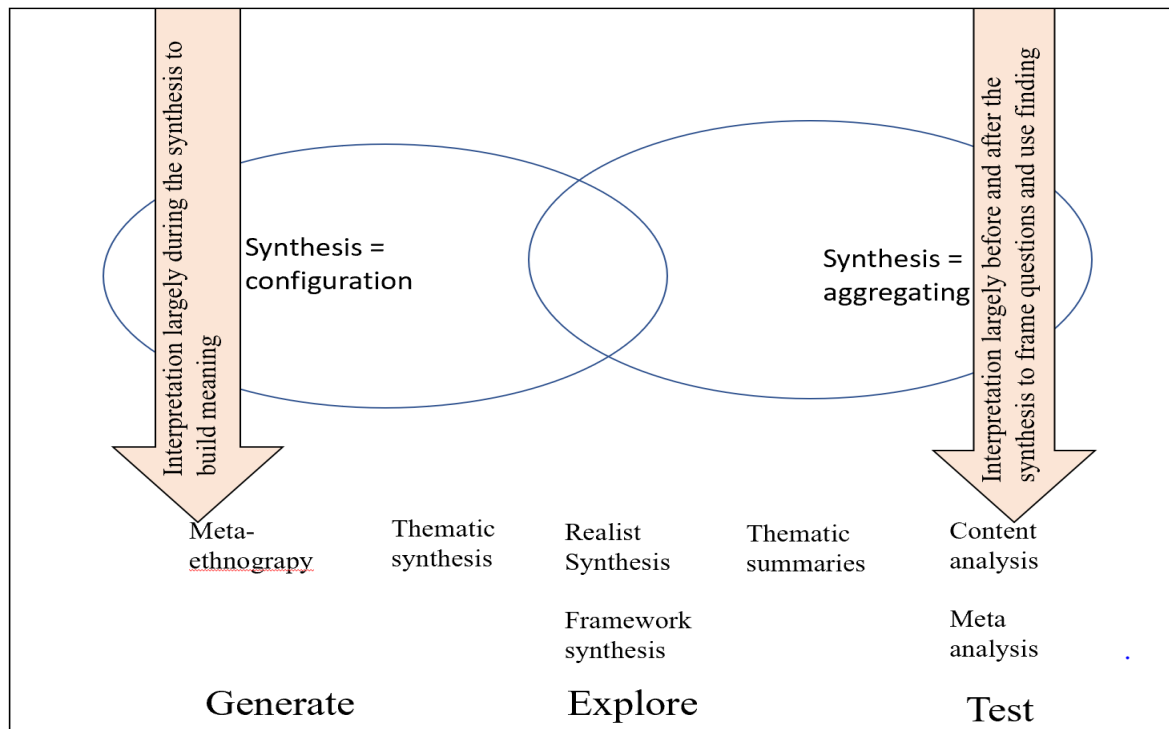


Figure 5.6: Synthesis Conceptualisation (Snilstveit et al., 2012; Thomas et al., 2012)

The modes of synthesis correspond to varying extents with the aims of the synthesis and are linked to the synthesis methods (see **Figure 5.6**). Different methods of synthesis mentioned in the literature are meta-ethnography, thematic synthesis, framework synthesis, thematic summaries and content analysis (Snilstveit et al., 2012; Thomas et al., 2012)

Based on the conceptualisation of synthesis depicted in **Figure 5.6**, thematic synthesis was employed in this research, and was used to identify, summarise and integrate the findings of different studies, creating analytical themes through a process of codification (Cruzes & Dybå, 2011; Thomas et al., 2012; Thomas & Harden, 2008). This method was chosen firstly because it was suitable for analysing multidisciplinary datasets (Thomas et al., 2012; Thomas & Harden, 2008). Secondly, as the method applies to different types of reviews, it assisted the researchers to conduct a synthesis that was grounded in the context of the study under review. And thirdly, the method was consistent with the thematic analysis method followed in the qualitative analysis. Finally, the flexibility of the thematic method supported the researcher's philosophical viewpoint of pragmatics.

Various other factors were also considered in selecting the synthesis method for the systematic review of this research. These included the type or aim of the synthesis, mode of synthesis and

the fact that the conceptual framework analysis process by Jabareen (2019) was followed in building the contextual framework of the study.

The thematic method of synthesis was used to identify recurring concepts, themes and patterns across the collection of studies used in the systematic review. The main concept of thematic synthesis is translation, which is the process of examining concepts that emerge from individual studies and identifying common themes among them, although the themes might be stated differently in diverse studies (Thomas et al., 2012).

A three-stage process of thematic synthesis was followed that involved coding text, developing descriptive themes and generating analytical themes (Thomas et al., 2012). Identification of the ‘finding’ is a challenge when undertaking a review using thematic synthesis, as it is not easy to decide what constitutes the primary research finding. To address this problem, this research took a broad perspective by understanding a primary study’s findings to include all sections where the concept of cybersecurity culture was discussed. This could include the introduction, results, findings and conclusions of the primary study paper. The conclusion is included as a reflection of the findings because it helps the researcher understand the original perspectives and priorities of the authors, since the reporting of all studies is mediated by the study’s author (Thomas et al., 2012).

ATLAS.ti, was the software used for the review, as it supports thematic analysis and synthesis. During the review, the three-stage process was applied to the final articles selected for the review. Initially, the definitions of cybersecurity culture were reviewed and coded to identify essential points in the definition. This was followed by reviewing the findings of the identified articles for the identification (coding) of the cybersecurity culture factors. Finally, the theoretical frameworks were reviewed for the development of descriptive and analytical themes (constructs) that were used for the categorisation of the identified factors.

Figure 4.7 of Chapter 4 depicts the PRISMA method and is revisited here to emphasise the inclusion and exclusion process.

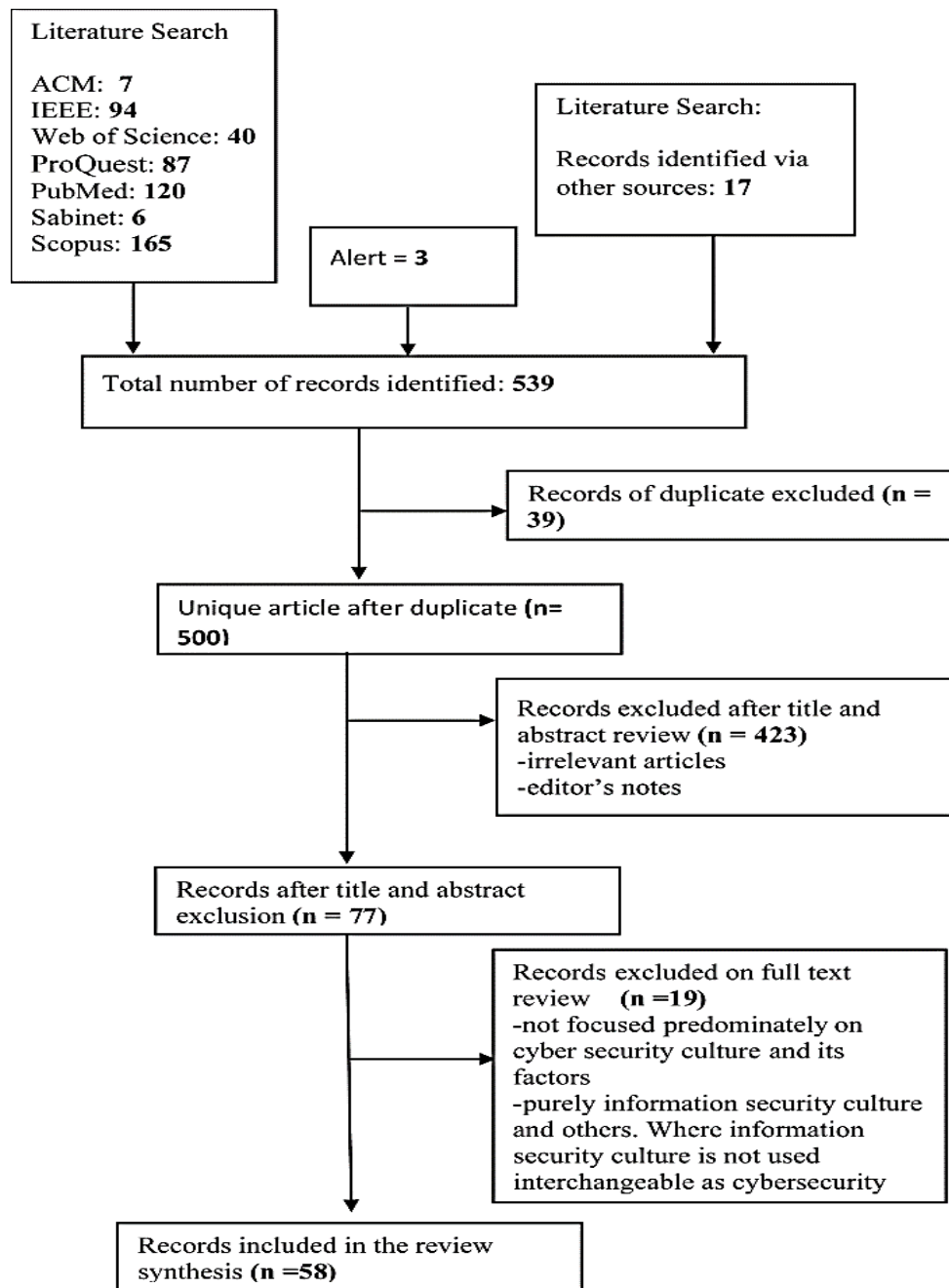


Figure 5.7: PRISMA Method for the Inclusion and Exclusion of the First Phase (Revisited) (Adapted from Moher et al., 2009)

The literature selection process was guided by the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework, thereby ensuring a rigorous and transparent methodology for identifying, screening and including studies relevant to building a cybersecurity culture. An initial literature search was conducted across multiple databases, including ACM (7 records), IEEE (94 records), Web of Science (40 records), ProQuest (87

records), PubMed (120 records), Sabinet (6 records), and Scopus (165 records), supplemented by alerts (3 records) and other sources (17 records), yielding a total of 539 records.

Duplicates ($n = 39$) were removed, leaving 500 unique articles for further evaluation. Title and abstract screening were then conducted to assess relevance to the study's focus. This process resulted in excluding 423 records due to irrelevance or because they were simply editors' notes. This resulted in 77 articles for full-text review.

During further full-text assessment, 19 articles were excluded based on content criteria: either they did not predominantly focus on cybersecurity culture and its factors, or they addressed general information security culture where the terms "information security culture" and "cybersecurity culture" were used interchangeably. Ultimately, 58 studies met all inclusion criteria and were included in the synthesis phase of the review.

This systematic approach ensured that the selected studies were highly relevant, focused specifically on cybersecurity culture, and provided a strong empirical and theoretical foundation for the subsequent analysis and framework development.

The last strategy followed in this research is the conceptual framework analysis presented in the next section.

5.5.3 CONCEPTUAL FRAMEWORK ANALYSIS

Cybersecurity and cybersecurity culture are topics studied in various disciplines. However, since cybersecurity culture is still an emerging topic, a limited amount of published research exists. Therefore, this study aimed to develop a contextual framework that would highlight concepts based on identified themes and elements to promote an understanding of cybersecurity culture. The concepts related to cybersecurity culture, from a variety of sectors and disciplines, emerged from a combination of systematic literature review and data obtained using other research instruments.

From a methodological perspective, the construction of the contextual framework of this study was achieved by following the conceptual framework process method of Jabareen (2009) as its strategy.

This strategy was followed to help answer the **Research Sub-Question 5 (RSQ 5)**: *"How can the identified factors associated with cybersecurity culture in E-Health institutions be used to*

design and develop a contextual framework for establishing cybersecurity culture in the public E-Health institutions in South Africa?”

This was one of the sub-research questions that contributed to the **Research Main Question:** *“How can a contextual framework for establishing cybersecurity culture in the public E-Health institution in South Africa be developed and evaluated?”*

Conceptual framework analysis is an iterative process that provides a procedure for building conceptual frameworks that are based on the grounded theory method (Jabareen, 2009).

Jabareen (2009) defined conceptual framework analysis as *“a grounded theory technique, or tactic, which aims to generate, identify, and trace a phenomenon’s major concepts, which together constitute its theoretical framework”*.

Putting this definition into the context of this research, conceptual framework analysis techniques were applied to identify and generate essential points, concepts and factors that constitute cybersecurity culture in public E-Health institutions.

According to Jabareen (2009), conceptual framework analysis is a process of building a conceptual framework for multidisciplinary phenomena. Conceptual framework analysis has been undertaken in many studies (Eizenberg & Jabareen, 2017; Mäenpää, 2021), including cyber-related studies (Hidayati et al., 2021). These assist by showing the process followed in identifying concepts related to multidisciplinary phenomena. Framework analysis was applied in this study as a strategy assisting in the development of a contextual framework of cybersecurity culture. Since limited research existed in this research area, the conceptual framework technique contributed to constructing the major concepts that constitute cybersecurity culture.

5.5.3.1 Phases of the Conceptual Framework Analysis

Jabareen (2009) proposed eight phases of the conceptual framework analysis methodology that need to be followed. **Figure 5.8** depicts the eight phases as adopted in this study, and the chapter references show where they were achieved.

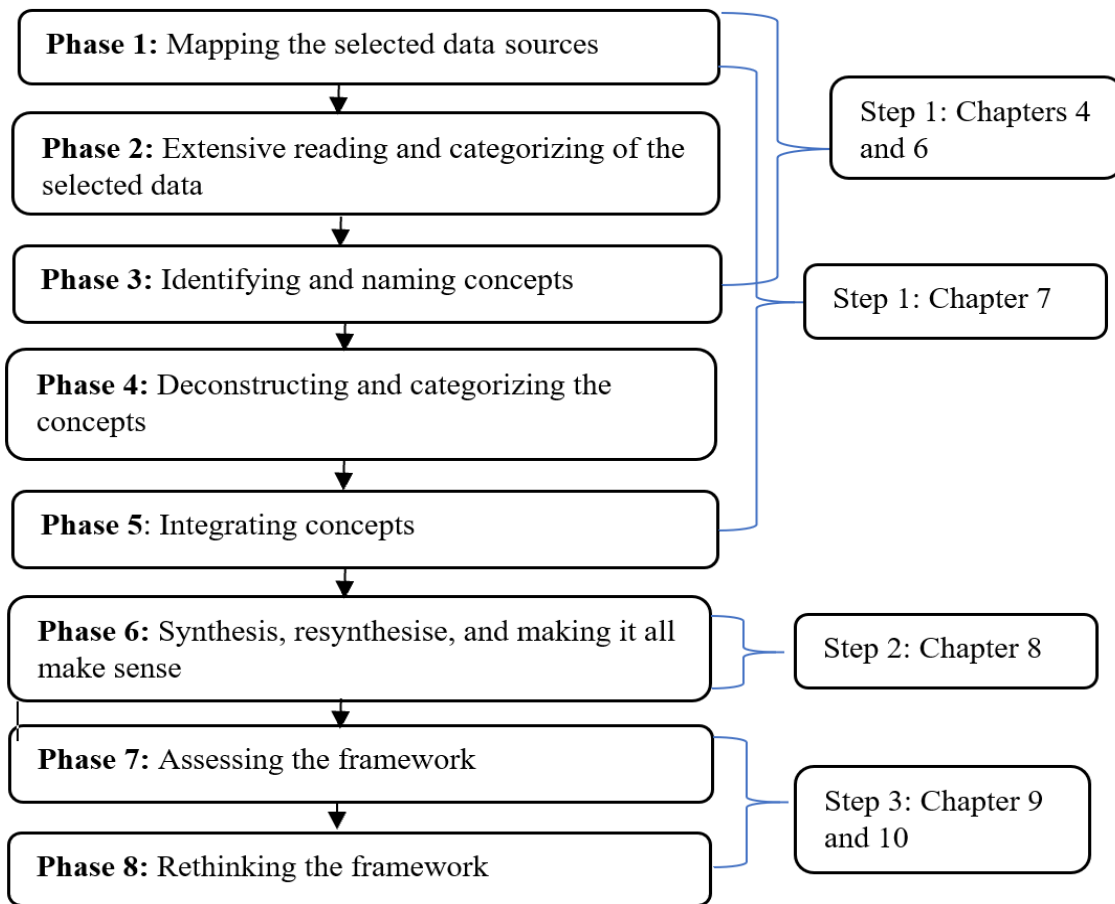


Figure 5.8: Conceptual Framework Analysis Phases (Adapted from Jabareen, 2009)

The aim of the conceptual framework analysis that was undertaken was to help with the identification of concepts and to link the concepts together to form a framework (Jabareen, 2009).

In light of this, conceptual framework analysis was adopted in this study by following three steps:

- **Step 1:** Identify, categorise, and integrate factors of cybersecurity culture empirically and non-empirically (presented in Chapters 4, 6 and 7). Step 1 involves the first five phases of the framework.
- **Step 2:** Link (through synthesis and resynthesise) the factors to develop a CCSCF in E-Health. Step 2 is described in Chapter 8 and is made up of Phase 6.
- **Step 3:** Assess the proposed framework to confirm it meets the intended principles and objectives. Step 3 contains Phases 7 and 8. Phase 7 is covered in Chapter 9. Phase 8 will be carried out as part of further work (see Chapter 10).

Chapters 2 and 3 of this study laid the foundation for a study of E-Health and developed an understanding of critical issues regarding cybersecurity in the E-Health context. The understanding gained from these chapters led to the systematic review of the main phenomenon of this study, namely, cybersecurity culture (see Chapter 4). Since neither cybersecurity culture nor the identification of cybersecurity culture factors were covered in Chapters 2 and 3, those two chapters were not included in any of the conceptual framework steps.

The eight phases of the conceptual framework analysis (depicted in **Figure 5.8**) followed in this study are explained below:

Phase 1. Mapping the selected data source: This phase involved identifying various disciplines that had explicitly addressed or used the topic and concepts of cybersecurity culture. Phase 1 also entailed identifying categories of sources and additional sources of data. The sectors identified that used or addressed cybersecurity culture as a topic, or its concepts included finance, aviation, water and education (Abeyratne, 2016; Clark et al., 2017; Da Veiga, 2016). The sources used to collect data included textual data via the literature review, interview data and questionnaires. This phase is reported in Chapters 4, 6 and 7 of this thesis.

Phase 2. Extensive reading and development of categories used to group the selected data: Phase 2 entailed a thorough reading of the data selected in Phase 1, categorising the data according to disciplines, creating and using scales of importance with representative power within the disciplines. As depicted in **Figure 5.8**, this phase is reported in Chapters 4, 6 and 7.

Phase 3. Identifying and naming concepts: The conceptual framework analysis method allows concepts about the phenomena being studied to emerge from the review of literature. This phase continued with the reading of the selected data that was begun in Phase 2, to discover concepts (Strauss & Corbin, 1990). The output of this phase was a list of competing and possibly contradictory concepts (Jabareen, 2009). As in Phases 1 and 2, the activities of Phase 3 are reported in Chapters 4, 6 and 7.

Phase 4. Deconstructing and categorising concepts: In this phase, the identified concepts were deconstructed to identify their main attributes, features, assumptions and roles. Phase 4 also involved organising and categorising the concepts according to their ontological, epistemological and methodological roles.

The results of this phase were presented as a table that summarised the concepts, their descriptions, categories according to their roles, and references for each concept. Phase 4 of Jabareen's (2009) framework is reported in Chapter 7 of this thesis, as shown in **Figure 5.8**.

Phase 5. Integrating concepts: This phase helped reduce the number of concepts identified to a reasonable number by integrating and grouping similar concepts. Chapter 7 of this study covers the activities of this phase.

Phase 6. Synthesis, re-synthesis, and making it all make sense: Concepts were synthesised into a theoretical framework. This was achieved by an iterative process of synthesising and re-synthesising until a point was reached where the framework made sense. **Figure 5.8** shows that Phase 6 is covered in Chapter 8.

Phase 7. Assessing the framework: After the conceptual framework was developed, the researcher asked questions like: Is the framework and its composed concepts sensible to the researcher, practitioners and academic community? This assessment was done by having the framework validated by experts to receive inputs and criticisms. As depicted in **Figure 5.8**, Phase 7 is covered in Chapter 9 of this study.

Phase 8. Rethinking the framework: This phase will form part of the further work proposed in Chapter 10. Future work undertaken after this study will seek more insight into the framework, revise it or make it more appropriate for another discipline or topic.

5.5.3.2 Trade-offs and Justification of the Conceptual Framework Analysis

The drawback of the conceptual framework is the subjectivity of the researchers' choice of categorisation. This drawback was minimised by applying a deductive approach in the categorisation of code items and in the definition and naming of themes during stages 3 and 4 of thematic analysis. Notwithstanding the drawbacks, the framework technique offers many advantages. The technique was followed in developing the framework of this thesis due to its numerous advantages. One major advantage is its flexibility, which ties in with the philosophical worldview of pragmatism adopted in this study.

Through the eight phases of the conceptual framework, the flexibility of this technique offered interpretation, adjustment and alteration opportunities with the adoption and adaptation of related concepts as fresh ideas and information were developed (Jabareen, 2009).

Other advantages of the conceptual framework analysis that contributed to the reasons it was chosen as a technique for developing the contextual framework of this study include:

- It helps with the development of a conceptual framework for a research phenomenon where limited or no academic literature exists currently. Cybersecurity culture is still an emerging research area, and limited literature exists. Therefore, conceptual framework analysis was considered to be an appropriate research strategy for the development of the contextual framework of this study.
- It is a technique that allows the development of a framework using concepts and factors from multidisciplinary perspectives and sources. Cybersecurity culture is of interest across sectors and disciplines. Consequently, following the framework analysis steps was considered appropriate for the development of the CCSCF, which is expected to serve as a theoretical framework for representing cybersecurity culture as a multidisciplinary phenomenon.
- The framework technique helps with the understanding of the phenomenon instead of predicting the working of the phenomenon. This study aimed to propose a framework for understanding cybersecurity culture for use in future studies. Hence, the use of conceptual framework analysis offered an opportunity in the process of developing the CCSCF.

5.6 RESEARCH CHOICE

According to the research process onion (see **Figure 5.1**), the three methodological choices a researcher may choose from are the mono method, mixed method, and multiple method (Saunders et al., 2016). The proposed research used a mixed-methods research approach because both quantitative and qualitative data collection techniques and analysis procedures were applied (Saunders et al., 2016). Creswell (2014) depicted quantitative, qualitative, and mixed methods at the centre of the research framework as the three research approaches that are influenced by other components.

5.6.1 QUALITATIVE AND QUANTITATIVE RESEARCH METHODS

Qualitative research is an approach that is used to learn and understand the meaning that participants, both individuals and groups, assign to a social or human problem (Creswell & Creswell, 2018). The authors argued that the primary focus of the qualitative approach is on individual (participant) meaning; hence, the researcher is the key instrument in the data

collection process, and data is collected in the participants' setting. In addition, this approach enables multiple sources of data collection and structural flexibility.

The quantitative research approach tests theories by examining the relationship that exists among variables (Creswell & Creswell, 2018). The approach is used to collect numerical data that is analysed by applying statistical procedures. Unlike the qualitative approach, the quantitative approach has a set structure, and theories are tested deductively to generalise the findings.

5.6.2 MIXED METHOD RESEARCH (MMR)

Mixed Method Research (MMR) is a research approach that allows using both qualitative and quantitative data collection and analysis in a single study (Creswell, 2014; Shorten & Smith, 2017). Shorten and Smith (2017) argue that with a mixed method approach, the collection, analysis and interpretation of data are mixed and can be integrated.

A combination of qualitative and quantitative research approaches, known as MMR, was employed in the research reported on in this thesis. As was indicated in **Section 5.3**, pragmatism was the research philosophy adopted in this research. As a paradigm, pragmatism has been proposed as a philosophical underpinning for MMR (Creswell & Plano Clark, 2018; Morgan, 2007; Edmonds & Kennedy, 2017; Hall, 2013; Leavy, 2017). One major advantage of employing mixed method research offered in this research is that it helps address the weakness associated with a single data collection (Kohlbacher, 2006).

The openness of pragmatism allows for combinations of approaches and methods, and this was beneficial to this research. As the research philosophy, pragmatism allowed a combination of qualitative and quantitative data collection (mixed method) to be used to obtain a rich and comprehensive understanding of cybersecurity culture factors in the public E-Health institutions. mixed method research helped the researcher identify the integrated cybersecurity culture factors used for achieving **Research Sub-Question 3 (RSQ 3)**, which contributed to the main research question, *“How can the contextual framework for establishing cybersecurity culture in the public E-Health institutions be developed and evaluated?”*. This was done by approaching the question from more than one methodological angle. This further confirms the suitability of the choice of pragmatism as the appropriate philosophical underpinning of this study.

Table 5.5 presents a summary of the different types MMR. Detailed descriptions and the applicability of the research choice of MMR type are explained in **Section 5.6.3**.

Table 5.5: Summary of the Types of Mixed Method Research (MMR)

Type of MMR	Description
Convergent Parallel Mixed method	This is a method that allows both quantitative and qualitative data to be collected concurrently, but the data are analysed independently using different approaches (Creswell & Plano Clark, 2018; Dawadi et al., 2021; Shorten & Smith, 2017).
Explanatory Sequential method	The explanatory sequential method is a two-phase study process. The method starts with the collection and analysis of quantitative data and subsequently uses qualitative data collection and analysis to aid with the explanation of the quantitative data (Creswell & Plano Clark, 2018; Dawadi et al., 2021; Shorten & Smith, 2017).
Exploratory Sequential method	This method is regarded as a three-phase study process. Qualitative data is collected and analysed first. Thereafter, quantitative data is collected and analysed to test the empirical findings of the qualitative method (Creswell & Plano Clark, 2018; Dawadi et al., 2021; Shorten & Smith, 2017).

5.6.3 CONVERGENT PARALLEL MIXED METHOD

In this research, the combination of quantitative and qualitative research was achieved through convergent parallel mixed methods, as depicted in Table 5.5. This means that the quantitative and qualitative data collection took place concurrently, and the analysis happened separately (Creswell & Plano Clark, 2018; Dawadi et al., 2021; Shorten & Smith, 2017). The convergent parallel mixed method allows a combination of dual data sets for a more comprehensive picture of the problem being explored and for validation of the findings of each method (Creswell & Plano Clark, 2018).

A convergent parallel mixed method design was followed in this research because its theoretical assumption is underpinned by pragmatism (Creswell & Plano Clark, 2018), and that is in alignment with the philosophical viewpoint of this study. In addition, the method enabled triangulation of results in Chapter 7. Triangulation, which involves the use of more than one data collection method, was used to increase the credibility, validity and accuracy of the research findings (Cohen et al., 2007; Dawadi et al., 2021; Noble & Heale, 2019). The convergent mixed method allowed the researcher to triangulate the results of quantitative and qualitative methods together with the findings of the systematic literature review in identifying the factors of cybersecurity culture.

In this study, the theoretical data was collected using a systematic literature review. This was followed by the concurrent collection of quantitative and qualitative data. Quantitative data were collected through surveys from system users (medical and administrative staff), while qualitative data was collected via interviews with ICT staff. Thereafter, the findings from the diverse data sets were integrated before the building of a CCSCF. The various methods of data collection used in this study resulted in the construction of legitimate and reliable realities, as triangulation enriches research, as it offers a range to explain several factors of cybersecurity culture (Cohen et al., 2007; Noble & Heale, 2019). **Figure 5.9** depicts the convergent parallel mixed method followed in this study.

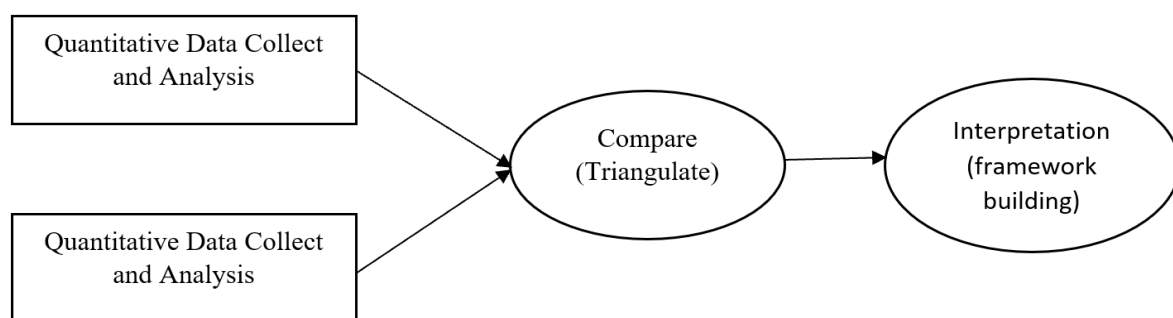


Figure 5.9: Convergent Parallel Mixed Method (Adapted from Creswell & Creswell, 2023)

5.7 TECHNIQUES AND PROCEDURES

Data collection and data analysis are the last layer of the research process onion. Research by McNiff and Whitehead (2002) indicate that various sources of data collection exist. However, these authors indicate that the selected data collection methods should be appropriate at all times for the research project under investigation (McNiff & Whitehead, 2002).

The study followed a combination of theoretical and empirical research approaches. This was because data was collected using various methods. The theoretical part of the research was achieved by conducting a systematic literature review. This assisted the researcher in identifying factors and concepts that contributed to developing the Contextual Framework of Cybersecurity Culture in an E-Health institution. The aim of the empirical part of the research was to enable the researcher to also derive knowledge from the experiences of E-Health stakeholders regarding factors that constitute cybersecurity culture in E-Health institutions.

The aim of the empirical part was also to derive knowledge relating to the factors that needed to be considered for the development of the framework, and to evaluate and validate the

developed framework using measurement instruments, interviews, and expert review questions. The research data collection methods are discussed in the next section.

5.7.1 DATA COLLECTION PROCESS

In this study, a questionnaire was used as part of a survey to carry out quantitative data collection. In addition to that, a semi-structured interview protocol was used for interviews as part of qualitative data collection. Data was collected in three rounds. In round one, a systematic literature review was used to collect data that contributed to answering:

Research Sub-Question 2: “What factors are associated with cybersecurity culture in literature?”

Round two used quantitative and qualitative methods to extract information from the participants that assisted with:

Research Sub-Question 3: “What factors are associated with cybersecurity culture in the public E-Health institutions in South Africa?”

Figure 5.10 was used to model the data collection process that was followed during the different rounds of data collection and analysis in this research.

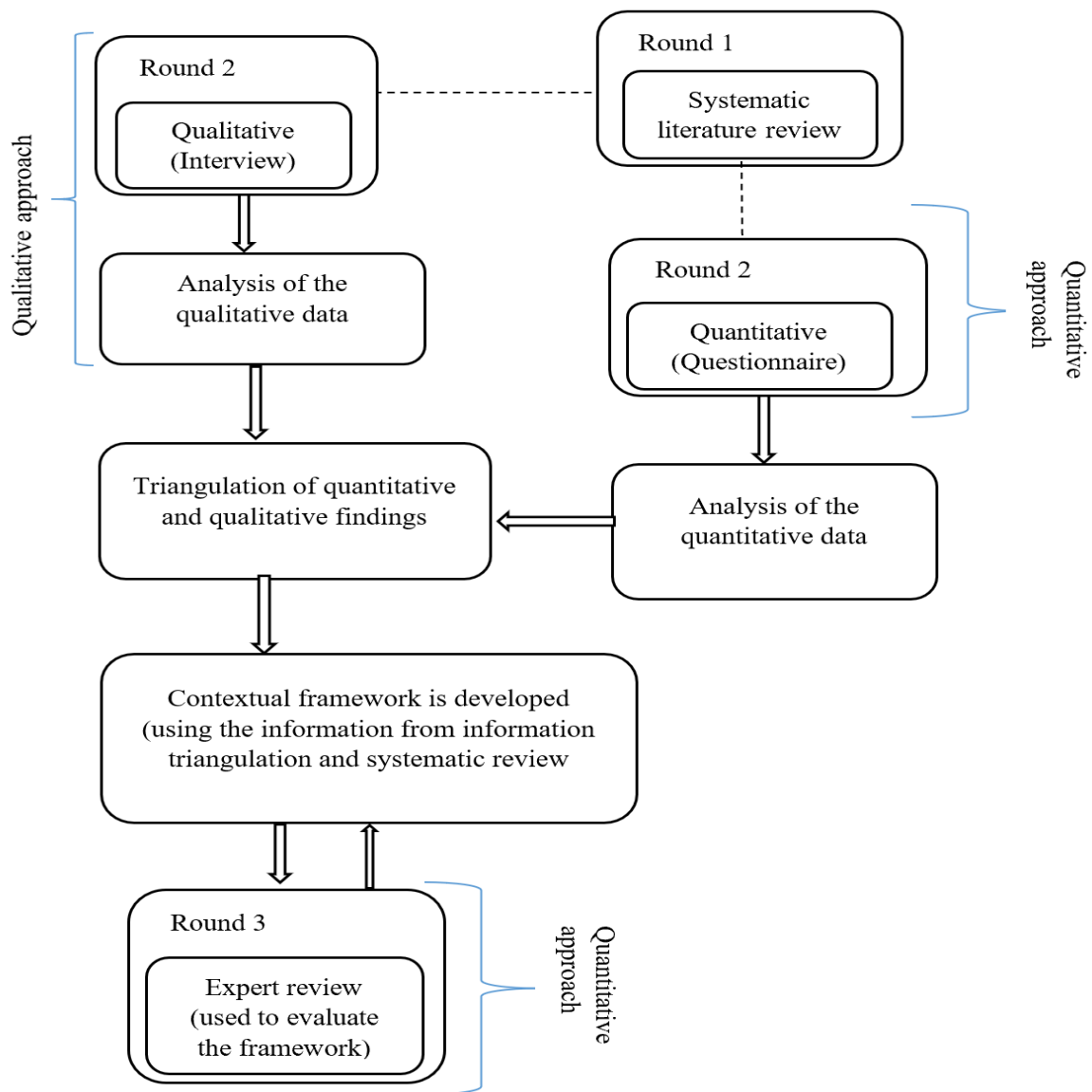


Figure 5.10: Model of the Data Collection Process (own source)

The aim of Round 1 of data collection was to identify factors associated with cybersecurity culture in the existing literature through a systematic review. The objective of round two was to gather data on cybersecurity culture factors in public E-Health institutions from ICT users through individual questionnaires and via interviews with ICT staff.

Data collected via quantitative and qualitative methods was initially triangulated to derive reliable and validated final factors of cybersecurity culture in the public E-Health institutions. The findings of the empirical data was then integrated with the factors identified from the systematic literature review to create a consolidated list of factors to be used to develop a contextual framework for this study.

The three rounds of data collection were aimed at the evaluation and validation of the contextual framework for establishing cybersecurity culture.

Using MMR in this study helped with the development of a research solution, “contextual framework of Cybersecurity Culture” that may be put to a more practical use, thereby adhering to the fundamental principle of pragmatism. This was the case because the basis of the contextual framework was not solely on abstract reality but was also derived from direct interaction with the participants in their context and within their natural settings. Using the MMR method helped with the triangulation of data collected via various collection methods.

Applying the mixed method research approach counteracted the vulnerability associated with being restricted to only one form of data collection. The instruments employed in the study for the collection of multiple forms of data included document analysis (systematic literature review), questionnaire, individual interview and expert review. These instruments were discussed in **Section 5.7.2..**

5.7.2 DATA COLLECTION INSTRUMENTS

This study collected data using the following techniques:

- Systematic review (Documents)

In this study, the document data collection method followed the form of a normal literature review in Chapters 2 and 3, as well as a systematic literature review in Chapter 4. The reviews in Chapters 2 and 3 were used mainly for foundational knowledge in the area of E-Health and cybersecurity. The understanding gained in those chapters led to the systematic review of the main phenomenon of this study, namely, cybersecurity culture, in Chapter 4.

The researcher systematically reviewed the literature to provide information on cybersecurity culture and to demonstrate that the proposed research could contribute to the body of knowledge in the field of Information Systems. As discussed in **Section 5.5.2**, Xiao and Watson's (2019) systematic literature review process was followed. According to Oates (2006), documents are divided into found and researcher-generated documents. The research reviewed documents that already existed in the research field. Examples of documents that were reviewed are journal articles, conference proceedings and textbooks.

- Questionnaires

A questionnaire is a pre-defined set of questions, assembled in a pre-determined order, and are either self-administered or researcher-administered (Oates, 2006). Questionnaires were used to collect data from system users on the factors associated with cybersecurity culture. The data obtained was triangulated with qualitative data to ensure the identification of reliable and validated cybersecurity culture factors in the public E-Health institutions in South Africa.

The study employed structured questionnaires where the participants were given predefined questions and answers. The design of the questionnaire research instrument was done using the five constructs of cybersecurity culture identified and explained in Chapter 4. The questionnaire consisted of a cover letter, participant consent letter, and six Sections (A to F). Section A contained questions that were used to collect demographic information of the participants, such as age, gender, and education level. Using a five-point scale, Sections B to F covered questions on the five research constructs of cybersecurity culture, namely, preparedness (P), responsibility (R), internal organisational management (IOM), also referred to as management, external environment and non-organisational management (EENOM), also known as external environment, and technology (TECH).

The answers to the questions were in an agreement legend of 1 to 5, with 1 indicating “strongly disagree” and 5 “strongly agree”. The questionnaires focused on the medical and administrative staff from the public E-Health institutions, such as the Doctors, Nurses, and support staff. See APPENDIX_3A for the questionnaire. Table 5.6 provides a summary of the questionnaire sections.

Table 5.6: Summary of the Questionnaire Sections

Section	Title	Question
A	Demographic information	Q1 to Q7
B	Preparedness (P)	Q8 (8.1 to 8.15), Q9 - Q12
C	Responsibility (R)	Q13 (13.1 to 13.19)
D	Internal Organisation Management (IOM)	Q14 (14.1 - 14.16)
E	External Environment and Non-Organisational Management (EENOM)	Q15 (15.1 - 15.6)
F	Technology (TECH)	Q16 (16.1 - 16.2)

- Interview

Is a planned and purposeful discussion by the researcher with the intention to obtain information from the interviewee (Oates, 2006; Saunders et al., 2016). A semi-structured interview was used to help the researcher gather valid and reliable data that are relevant to the research questions and objectives. The focus of the interview was on the ICT personnel's understanding of factors to be considered in the South African context when developing a CCSCF in the public E-Health institutions.

As a non-standardised interview method, semi-structured interviews offered the researcher the opportunity to probe for detailed answers where the researcher wanted the interviewees to explain or build on their responses. It offered the ICT staff the opportunity to explain their answers to the questions asked. By conducting the interview in a semi-structured way, the researcher could change the order of the interview questions depending on the flow of the conversation. The interview was conducted via Microsoft Teams with ICT personnel.

The interview design consisted of three sections. Section A was used to meet ethical norms. Section B covered biographic information and ICT background information questions, and Section C contained the twenty interview questions (see APPENDIX_4A).

- Expert review

An expert review is a data collection or evaluation method that involves engaging independent and qualified content experts on the phenomenon being studied to provide a critical and consultative evaluation of the merits of a research product (Ron, 2008). Several authors support the use of expert review as an evaluation criterion to assess the feasibility of a research framework or any other artifact (Peffer et al., 2012, 2014; Sonnenberg & vom Brocke, 2012). Expert reviews were used in this research to evaluate the contextual framework developed for establishing cybersecurity culture in public E-Health institutions.

The expert reviews provided the researcher with objective views from sources who are familiar with the research area of cybersecurity and cybersecurity culture. The expert reviews aimed to gain knowledge and opinions of the cybersecurity or cybersecurity culture experts to evaluate the CCSCF developed as an artefact in this study. After expert evaluation, recommendations were recorded and used for the improvement of the framework.

The data collected via expert review was used to address **Research Sub-Question 6: “How can the Cybersecurity Culture Framework be evaluated?”**

The researcher consulted academic research peers and industry personnel with expertise in cybersecurity and cybersecurity culture for their views on:

- 1) The extent to which the contextual framework of this study meets the objectives and principles the framework was set to achieve
- 2) The comprehensiveness of the framework
- 3) The relevance and applicability of the framework
- 4) Their suggestion on how the framework could be improved

A set of interview questions was used to help the researcher gather data from the evaluation of the framework. These were grouped to highlight five aspects, namely, principles, objectives, comprehensiveness, relevance and applicability. This excludes the last question, which was used to collect general comments on how the framework could be improved¹. The five aspects consisted of a minimum of one and a maximum of four questions.

The interview questions were designed using the Google Form application. The researcher shared the Google link together with other information with the interviewee at the start of the interview.

The method of analysis applied for the expert review data was content analysis, and offered the researcher the opportunity to deduce genuine and authentic meaning from text data in the context where the text is being used (Krippendorff, 2004). Quantitative and qualitative content analysis are two forms of content analysis (Bengtsson, 2016). Qualitative content analysis was applied in this study because the researcher sought to derive meaningful interpretations from the textual data collected via the expert review.

The knowledge gained through these data collection processes and instruments assisted in answering the research questions summarised in Table 5.7.

¹ https://docs.google.com/forms/d/1_P7Y-1LViPPF2nZbD6uqaclbeY1eVeFmO5aqlzAihz0/viewform?edit_requested=true#responses

Table 5.7: Research Sub-Questions Addressed by the Data Collection Instrument

Research sub-questions
Research Sub-Question 2 (RSQ 2): What essential factors associated with cybersecurity culture are identified in existing literature that should be considered in developing a Cybersecurity Culture Framework for public E-Health institutions?
Research Sub-Question 3 (RSQ 3): What factors are associated with cybersecurity culture in the E-Health environment in South Africa?
Research Sub-Question 4 (RSQ 4): What constructs from existing cybersecurity culture frameworks and other relevant frameworks can inform the design of a contextual Cybersecurity Culture Framework for public E-Health institutions?
Research Sub-Question 6 (RSQ 6): How can the contextual Cybersecurity Culture Framework be evaluated?

Figure 5.11 depicts the data collection instruments employed in the study, together with the participants and documents from which the researcher collected the data.

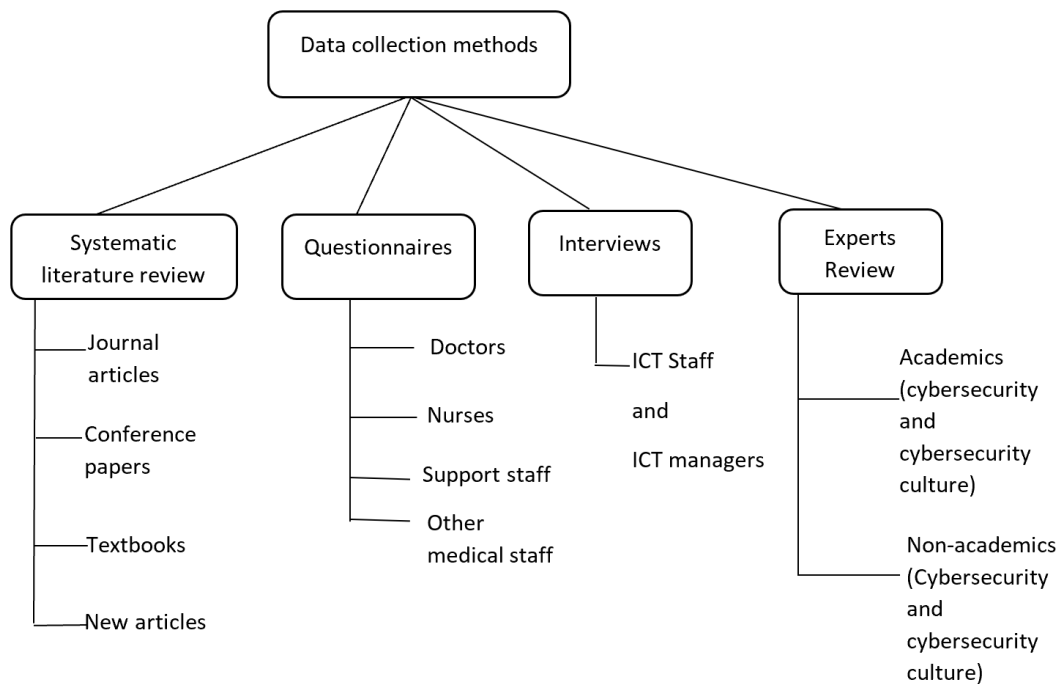


Figure 5.11: Data Collection Method (own source)

5.7.3 RESEARCH QUESTIONS AND DATA COLLECTION INSTRUMENTS

The main research question of this study was, “*How can a contextual framework for establishing cybersecurity culture in the public E-Health institution in South Africa be developed?*”

To address this question, sub-research questions were outlined as described in Chapter 1. Various methods followed in answering the sub-research questions were discussed in this chapter. Table 5.8 summarises the research sub-research questions together with the methodology and techniques that were followed in addressing them.

Table 5.8: Summary of Research Questions and Associated Data Collection

No.	Sub-Research Question (RSQ)	Methodology and data collection instruments
2 and 4	What essential factors associated with cybersecurity culture are identified in existing literature that should be considered in developing a Cybersecurity Culture Framework for public E-Health institutions? and What constructs from existing cybersecurity culture frameworks and other relevant frameworks can inform the design of a contextual Cybersecurity Culture Framework for public E-Health institutions?	A systematic literature review (Document analysis) on cybersecurity culture was used to identify factors and components of cybersecurity culture in the literature.
3.	What factors are associated with cybersecurity culture in public E-Health institutions?	i) Questionnaires were used for system users, which included medical and administrative staff. ii) An interview was carried out with ICT staff, including ICT managers, in a semi-structured way to gather more detailed data on cybersecurity culture factors.
5	How can the factors identified through this research be applied to design and develop a contextual framework for establishing cybersecurity culture in public E-Health institutions?	The eight 8 phases of conceptual framework analysis were followed as the methodology to achieve the development of the proposed contextual framework developed in this study.
6.	How can the Contextual Cybersecurity Culture Framework (CCSCF) be evaluated and validated?	Expert review questionnaires were used with cybersecurity experts, including academic and non-academic experts for their views and inputs on how the developed framework could be improved.

5.7.4 DATA ANALYSIS

Data analysis looks for patterns in the collected data and draws conclusions (Oates, 2006). The purpose of the analysis for this study was to organise the findings in such a way as to allow the

researcher to identify essential factors that can assist with developing a cybersecurity culture in the public E-Health institution in South Africa.

It was noted in a previous section that this research followed a pragmatic research philosophy, achieved through the choice of a mixed methods approach. In light of these choices, the study employed quantitative and qualitative data analysis methods for the analysis of the data collected. Various stages of a research project follow a proactive and thorough analysis process to obtain findings that transform collected data into fresh insights (De Villiers, 2012).

Reliability and validity test were reported; however, further interpretative explanation was necessary beyond the statistical result. The reported Cronbach's values and factor loading were classified in terms of how they reflected the strength and consistency of the measurement scale. The discussion also showed how these measures aligned with and accurately represented the underlying constructs in the study. The interpretation strengthened confidence that the quantitative findings were meaningful and theoretically grounded rather than simply statistically adequate.

5.7.4.1 Quantitative Analysis

Quantitative processes were followed to analyse the quantitative data collected in this study. The quantitative analysis is covered in Chapter 6 and was performed using Statistical Package for Social Sciences (SPSS) and Analysis of Moment Structures (AMOS) version 28.0. The quantitative data were analysed using frequency tables, Cronbach's alpha, Exploratory Factor Analysis (EFA), descriptive statistics and Pearson Correlation.

The demographic data of the participants (gender, age, education level, and job title) was analysed for visualisation and understanding of the participants' characteristics using frequency tables (see Table 6.2 to Table 6.5).

The reliability of the study was assessed using Cronbach's alpha. A threshold value of 0.6 would be acceptable (Cossío-Silva et al., 2016). Reliability assessment is covered in **Section 6.5.4**.

The validity of the research instrument was assessed using Exploratory Factor Analysis (EFA). As will be seen in **Section 6.5.5** the research instrument of this study did not have issues regarding validity. The EFA used to assess the research instrument included Kaiser-Meyer-Olkin (KMO) and Barlett's Commonalities, Total Variance Explained (TVE), Scree plot, and

Component Matrix to validate. **Section 6.5.5** provides a detailed discussion and statistical analysis of EFA.

Quantitative analysis, including reliability testing, EFA and correlation were not only statistically executed but were strengthened by linking the results to the underlying theoretical construct of cybersecurity culture to ensure meaningful interpretation. To enhance the qualitative components, the thematic analysis was used, and themes were formulated when data saturation was enriched. The process of triangulation was elaborated to show how quantitative findings, qualitative themes, and documentary evidence were compared to identify areas of convergence and divergence. Finally, the quantitative - qualitative integration was classified by outlining the specific procedural steps used to merge and interpret both data sets, ensuring a coherent and transparent mixed-method analytical pathway.

Descriptive statistics were used to find the mean per construct. In addition, descriptive statistics were used to find the standard deviation of each decision variable, such as preparedness (P) and responsibility (R) (see **Section 6.5.6**).

Pearson Correlation was used to measure the relationships between variables using R-value and P-value. The R-value ranges from -1 to 1, and the P-value chosen for this research study was 0.05 (Pallant, 2020). Significant constructs were selected to derive a model of cybersecurity culture. Discussion on the Pearson Correlation analysis and findings are presented in **Section 6.5.7**.

5.7.4.2 Qualitative Analysis

Multi-method qualitative analysis is an appropriate research choice for interpretivist (subjective) research. It allows the researcher to collect data using various methods and to conduct analysis using a qualitative procedure (Saunders et al., 2016). The qualitative data collected via interviews were analysed using a thematic analysis process.

This section discusses thematic analysis as used in analysing the interview data. Qualitative analysis is also covered in Chapter 7; ATLAS.ti version 9 was the software used to achieve the thematic process. This section discusses the coding process, network diagram, table, Groundedness, and density as the thematic and ATLAS.ti features applied during the analysis.

- Thematic analysis

Thematic analysis is a qualitative data analysis process described as a “way of seeing” or “making sense” and “analysing” (Boyatzis, 1998). Boyatzis (1998) referred to thematic analysis this way because the data, information and circumstances can appear to make sense or be analysed differently by different people. Thematic analysis is commonly used to search through qualitative data to identify, analyse and report recurring patterns of meaning in the data (Attride-Stirling, 2001; Boyatzis, 1998; Braun & Clarke, 2006; Cruzes & Dybå, 2011; Thomas & Harden, 2008). Thematic analysis at an unsophisticated level helps to organise and describe data in detail and, at the most ambitious level, assists with interpreting various aspects of the phenomenon under discussion (Boyatzis, 1998; Braun & Clarke, 2006).

The benefits of thematic analysis include its flexibility, which allows inductive analysis, deductive analysis or a combination of these to generate themes (Braun & Clarke, 2006). It systematically handles diverse types of data and information (Boyatzis, 1998). The flexibility allowed made the thematic approach of Braun and Clark (2006) attractive for this research, and it was achieved using the qualitative data analysis software ATLAS.ti version 9.

The flexibility of thematic analysis supports pragmatism, which is the philosophy considered most suitable for this study. The choice of thematic analysis was also consistent with the thematic synthesis applied in the systematic literature review (see **Section 5.5.2.3**). **Figure 5.12** shows the thematic stages of Braun and Clark (2006) as applied in this study. For a detailed discussion of how these stages were applied during the analysis process, see **Section 7.4**.

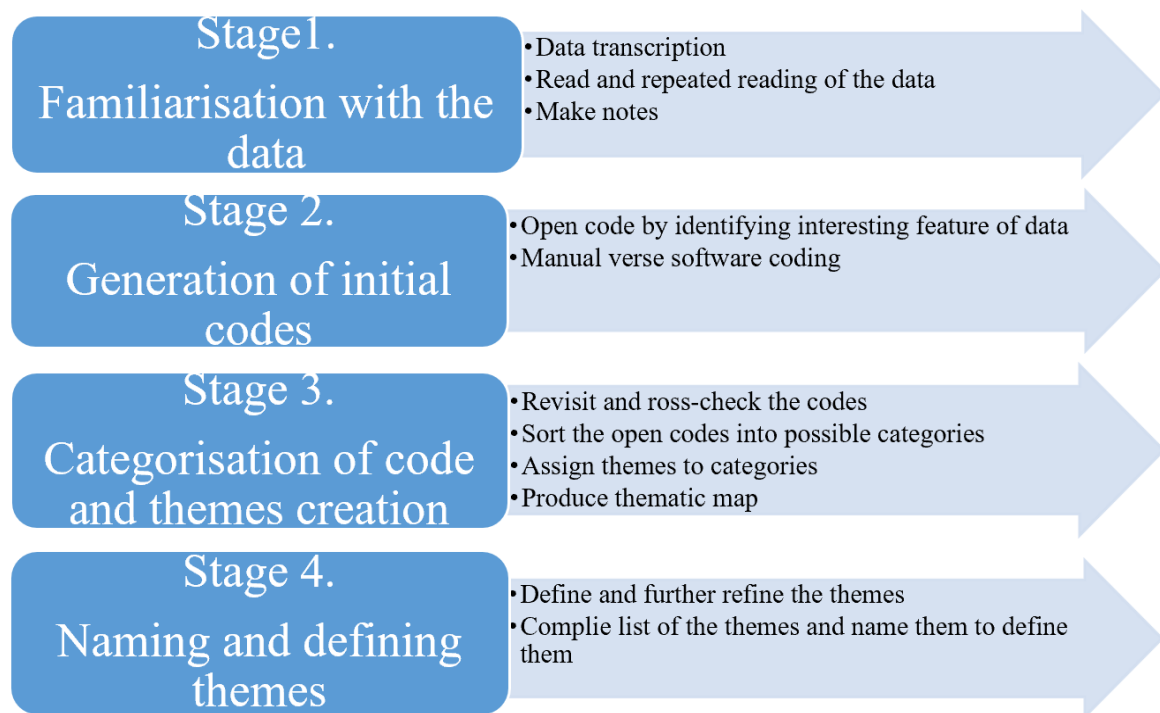


Figure 5.12: Stages of Qualitative Analysis (Adapted from Braun & Clarke, 2006)

The thematic analysis followed in this study focused on identifying recurring codes and sub-themes to obtain a deeper understanding of cybersecurity culture. The thematic analysis enabled the researcher to compile comprehensive and structured tables and diagrams of factors associated with cybersecurity culture.

Coding attaches meaningful labels to data segments (excerpts) and shows what the short extracted piece of text represents (Charmaz, 2014). It is used to organise qualitative data to make it clear what the data is about (Richards & Morse, 2013). The coding process, particularly open coding, was employed to identify patterns and trends within the qualitative primary data. The coding done in this study ensured a thorough and nuanced exploration of the participants' narratives. After coding the responses (see **Section 7.4.2**), the codes were grouped into meaningful sub-themes (see **Section 7.4.3**), and the sub-themes were categorised into higher-order themes categorised (see **Section 7.4.4**).

In this study, network diagrams and tables were used to visualise themes by showing associations between the themes and concepts. The tables show the Groundedness and density linking the codes and their associated themes. The network and table visualisation link to the higher-order themes of the study, namely, preparedness (P), responsibility (R), internal

organisation management (IOM), technology (TECH), and external environment and non-organisational management (EENOM).

Grounding is the observed connection between the themes or codes, and when frequent, to the point of interest (Rambaree, 2018). “It shows how many quotation codes are linked to a code” (ATLAS.ti, 2024). Grounding was used in this study to ensure that the analysis remains glued together, promoting authenticity and good findings.

Density is the association of occurrences within a particular theme of a field of interest (Passonneau & Coffey, 2011). It indicates the “Number of linkages to other codes” (ATLAS.ti, 2024). In this study, density refers to which themes are connected. A higher density illustrates a greater number of connections.

5.7.4.3 Trustworthiness of Qualitative Enquiry

Researchers have argued that qualitative research needs to be concerned with validity and reliability (Creswell & Creswell, 2018; Grosseohme, 2014). In qualitative research, validity refers to the authentic and credible representation of the participant's voice and the researcher's involvement in the data creation (Mac Naughton & Hughes, 2008). According to Creswell and Creswell (2018), validity in qualitative research means the researcher employs strategies to check the accuracy of the research findings. Reliability ensures consistency across researchers and projects in interpreting research findings obtained via qualitative research methods like interviews (Grosseohme, 2014).

Validity and reliability were achieved in this study by giving detailed and careful attention to the collection, analysis of results, interpretation of data, and presentation of findings. Doing this fulfilled the essence of validity and reliability (Golafshani, 2003).

The measures used to ensure the qualitative trustworthiness of this study include credibility, transferability, dependability, confirmability and triangulation. These terms are discussed below.

- **Credibility**

According to Oates (2006), credibility relates to internal validity. This implies that participants understand the question asked and can provide informed answers in a given context. Credibility ensures that participants' perceptions are compatible with the research findings. Oates (2006) argued that credibility tried to answer the question, “*Is the inquiry carried out in a way that*

ensured that the subject of the inquiry was accurately identified and described, and that the research findings are credible?”

The following strategies discussed by Creswell and Creswell (2018) were applied in this research to ensure credibility:

Prolonged time: After the prospective respondent was referred to the researcher and before the interview, the researcher spent time engaging with the respondents to get to know them better. It also allowed the participants to get to know the researcher and become accustomed to her. This helped establish a relationship between the researcher and the participants. Likewise, after the interview, the researcher remained in the interview as the respondents said other general things and asked non-research-related questions. Additionally, the researcher drove to the province of data collection to visit the case hospitals to understand their environment and develop a relationship with them before the data collection commenced.

Interview process: During the interview, the researcher asked some of the interview questions in different ways, reframing them for better understanding by the participants. Questions were repeated occasionally when the participants failed to hear or understand the researcher.

Peer debriefing: also known as expert review and independent scientific review (Ron, 2008), is used to improve the correctness of the account (Creswell & Creswell, 2018). Peer debriefing entailed asking an independent person to review and query the study, so that the account would resonate with others and not just the researcher. The research was conducted under the supervision of two supervisors who monitored the research processes and asked questions about them, starting from the systematic literature review, research design, data collection, analysis and interpretation. A peer review was also carried out as there were blind reviews of the research work published in conference proceedings and journals. Furthermore, an expert review was performed on the final framework (CCSCF) developed for the study, which was developed using the data collected.

Member checking: This was performed to check the accuracy of the findings and was achieved by partially reporting back or following up with participants to determine the participants' feelings about data accuracy (Creswell & Creswell, 2018). In this research, to ensure transcription words were accurately reflected during data cleaning, follow-up communication occurred with specific participants for clarification of some transcribed words whose meanings were not well understood.

- Confirmability

Confirmability is a qualitative strategy used to establish the extent to which the researcher's results can be confirmed and hence be supported by other researchers. According to Oates (2006), the question to answer with confirmability is, *“Have we been told enough about the study to judge whether the findings flow from the data and the experience in the setting?”* Auditors assess confirmability via an ‘audit trail’ (Oates, 2006). The main ‘auditors’ used to achieve confirmability in this study were the supervisors. The study also documented the processes followed in conducting the research in various chapters, which will give the reader sufficient information to make an informed judgment.

- Dependability

Dependability assesses the consistency of the research findings across researchers and methods. It checks how well the research process is recorded and data documented (Oates, 2006). With dependability, Oates (2006) expects researchers to answer the question, *“Is it possible for others to carry out an audit trail to trace the whole process?”* Qualitative analysis software ATLAS.ti was used to analyse the qualitative data in this study. This made the detailed documentation of analysis reports and the retrieval of such reports when needed possible and relatively easy. Google software was also used to document the responses of expert reviewers for easy retrieval at any given point. Triangulation also assisted with dependability as it addressed individual biases.

- Transferability

Transferability is concerned with how generalisable the findings of the research are from one case to another (Oates, 2006). Transferability is achieved by providing a rich and sufficiently thick description of the research setting, which enables readers to make informed judgments as to whether their situation is similar to the research setting and that findings can be applied to their specific context (Oates, 2006). Rich description was also discussed by Creswell and Creswell (2018) as among the strategies for achieving qualitative validity and reliability. In various sections of this methodology chapter (Chapter 5), data collection, and analysis (see Chapter 7), the researcher provided detailed and sufficient descriptions of the context and participants that can provide the readers with sufficient information.

- Triangulation

Triangulation is the use of multiple data collection sources in a study of human behaviour to gather compatible evidence. It increases the credibility and validity of the results (Cohen et al., 2007; Noble & Heale, 2019). Triangulation is based on the logic that multiple data collection and analysis methods are capable of solving problems more completely than a single method, because each method discloses unique aspects of empirical evidence (Patton, 1999). Hence, numerous methods provide more materials for researchers (Patton, 1999). Triangulation offered multiple benefits to this research. For example, it enhanced the trustworthiness of research results (Kohlbacher, 2006) and assured the consistency of data collected via different methods and sources (Yin, 2014).

Four different kinds of triangulations have been discussed: data, investigator, theory, and methodological triangulation (Denzin & Lincoln, 2005). Types of triangulations also include triangulation of source, theory/perspective, analyst, and method triangulations (Oates, 2006; Patton, 1999).

The two kinds of triangulation adopted in this study were data and methodological triangulation. Data triangulation was achieved by comparing and integrating the findings of data collected and analysed via multiple methods. Methodological triangulation was achieved by following several data collection methods such as a systematic literature review in Chapter 4, the quantitative method in Chapter 6, and the qualitative method in Chapter 7.

Achieving triangulation using systematic literature review, qualitative and quantitative data collection, and analysis helped avoid weaknesses like biases that are sometimes found in studies that employ a single method. Collecting empirical data related to the factors associated with cybersecurity culture, using multiple methods, helped confirm the consistency of the factors identified. Furthermore, triangulation is assisted by facilitating the creation of a well-integrated list of cybersecurity culture factors from empirical and systematic literature review findings. The integrated list was the final factor in developing the proposed CCSCF.

Patton (1999) argued that it is important to identify and acknowledge inconsistencies in the findings derived from analysis of data obtained from data of different types as this provides opportunities for a better understanding of the research phenomenon. This holds true in this study, because identifying the factors of cybersecurity culture using systematic review, questionnaires, and interviews yielded a few factors specific to a different method and data type. However, this allowed the CCSCF to be developed based on comprehensive and diverse factors identified through the triangulation of methods.

Triangulation in the study of human behaviour involves using more than one data collection method to increase the credibility and the validity of the results (Cohen et al., 2007; Noble & Heale, 2019). This allowed the researcher to identify factors associated with cybersecurity culture in the selected public E-Health institution using two different data collection methods, qualitative and quantitative. It also helped identify cybersecurity culture factors from the literature. Triangulation is the best way to reduce bias stemming from quantitative and qualitative analysis when these are handled separately.

This section presents a triangulation of the findings of the two research methods to ensure the credibility and validity of the research results obtained from empirical data. Doing this helped produce an accurate picture of the phenomenon of cybersecurity culture (Gillham, 2000). According to Gillham, an accurate representation of a phenomenon emerges when there is an indication that the data collection methods and sources jointly produced the results. The absence of such convergences should result in the researcher being cautious about any conclusions put forward regarding the phenomenon (Gillham, 2000).

To achieve triangulation in this study, the two models obtained as a result of the separate qualitative and quantitative findings were compared, and then the similarities and differences were discussed. This was followed by the integration or consolidation of factors from the two methods. Finally, the results from the triangulation of the two empirical data sets were compared with the data from the systematic literature review to produce the final list of cybersecurity culture factors for the contextual framework presented in Chapter 8.

5.8 POPULATION

A research population is the full set of possible cases from which a research sample is taken (Saunders et al., 2016). According to Oates (2006), a research population, also referred to as a sampling frame, refers to an aspect of the entire population of people that could be included in the data collection from which a sample can be chosen.

The population for this study consisted of:

- ICT staff with knowledge of operations in the Mpumalanga medical facilities.
- E-Health system users, that is, medical and administrative staff who use any Internet-based electronic system for their work.
- Cybersecurity culture experts working in the industry or academic sectors.

The study population indicated above is small. These groups were selected because of their knowledge and experience in the use or maintenance of electronic healthcare systems in the context of Mpumalanga province, or their knowledge and experience in development, supervision, grading, evaluation, implementation, and management of frameworks in the area of cybersecurity or cybersecurity culture.

The population of this study with regard to the quantitative study was 99. Furthermore, the population of the qualitative study was nine.

5.9 SAMPLING METHOD

According to Marshall (1996), choosing a study sample is a crucial step in any research project, since studying the whole population is not practical, efficient or ethical.

Choosing an appropriate sample method depends on the study's aim (Marshall, 1996). Quantitative research sampling approaches aim to draw a representative sample from the population and to test pre-determined hypotheses so that the results of the study sample can be generalised back to the population (Marshall, 1996).

Sampling methods are grouped into probability and non-probability sampling types (Creswell & Plano Clark, 2018). Probability sampling is a statistical technique whereby each unit in the target population has an equal chance of being selected in the sample (Etikan et al., 2015, 2016). With this type of sampling, participants have a known, non-zero probability of being included in the research sample (Fink, 2017; Verma et al., 2017).

The major advantage of probability sampling is its ability to determine a sampling error (Kolb, 2008). Limitations regarding money, workforce or time make it difficult for researchers following this technique to achieve an accurate random sample of the whole population (Etikan et al., 2015). Hence, there is a need for non-probability sampling (Etikan et al., 2015).

Non-probability sampling is a non-statistical sampling technique that allows the selection of sample units to be made subjectively, based on the researcher's judgment or for convenience (Creswell, 2014; Etikan et al., 2015; Verma et al., 2017). This technique involves no random selection; accessibility forms the basis for sample selection (Etikan et al., 2015). The technique involves a much reduced cost for research where representativeness of the population is not necessary, like in a case study (Verma et al., 2017).

In this study, the entire research population could not be examined due to time and resource limitations, and therefore, a sampling process was used to select a portion of the population of

interest. A non-probability sampling technique was used, and therefore, certain people of all those in the population stood a better chance of being selected than others. In this case, only medical and non-medical staff with access to Internet-based ICT in the hospital were selected, rather than all members of staff.

Also, as it was MMR, the aim of this research was not to test hypotheses or to generalise its results. the aim was to develop a framework that would assist in understanding the meaning that social actors in the context of public E-Health institutions attach to the complex phenomena of cybersecurity culture. Therefore, probability sampling was not an appropriate technique.

Qualitative investigations tend to have small research samples, the research is often flexible and iterative, and there is no evidence that the values, beliefs and attitudes that form the core of qualitative investigation are normally distributed (Marshall, 1996). A clear understanding of the aim of this study was developed before the research commenced. Based on this, a MMR that contained elements of both qualitative and quantitative approaches was selected. Hence, probability sampling techniques were not considered appropriate; instead, non-probability sampling techniques were used.

Due to the possibility of bias occurring when non-probability sampling is applied in selecting the research sample, the findings from this study will not be regarded as representative of the overall population (generalised). Instead, it will be applied cautiously to situations similar to the one in the sample.

Combining two sampling methods, namely purposive and convenience sampling, improved the chance of selecting relevant, targeted, and accessible participants. Firstly, the purposive method was employed to ensure that the study included knowledgeable participants. Hence, the research purposefully selected medical practitioners with direct experience of E-Health ICT use and cybersecurity. This guaranteed that the participants were well-informed and could provide valuable insights into the development of a cybersecurity culture within healthcare. By selecting individuals based on their roles and involvement in health information systems, the researcher aimed to maximise the depth, reliability, and contextual relevance of the data collected.

Secondly, convenience sampling offered the advantage of practical accessibility by acknowledging real-world difficulties in research into healthcare, including staffing shortages, time constraints and institutional hurdles. Since cybersecurity in healthcare is a niche area,

finding volunteers with the relevant knowledge can be difficult. Therefore, convenience sampling enabled efficient recruitment of participants while still ensuring a sample size large enough for in-depth qualitative data and topic saturation.

Sampling was purposive and was supported where necessary by both the convenience and snowball sampling approaches, given the specialised nature of cybersecurity roles and organisational access constraints. Purposive sampling ensured that participants possessed relevant knowledge, while snowball sampling helped with the identification of additional stakeholders involved in cybersecurity processes. Although these strategies limited statistical generalisation, they were appropriate for explanatory context-specific enquiry. Steps were taken to mitigate bias, firstly by establishing inclusion criteria, secondly by ensuring institutional diversity and thirdly by reporting sample characteristics transparently.

Table 5.9 provides a summary of different methods applicable to non-probability sampling.

Table 5.9: Non-probability Sampling Methods (Fink, 2003; Henry, 1990)

Sampling methods	Description
Convenience	Convenience is a sampling method that focuses attention on selecting units of the targeted population based on their accessibility, readiness, availability, willingness, and convenience. Convenience sampling is also referred to as Haphazard or Accidental Sampling.
Purposive	The Purposive method is also known as Judgement sampling. It is a non-statistical sampling technique where an individual (researcher) consciously selects elements of the population based on their personal judgment of the appropriate features of the sample.
Snowball	Snowball is also called Chain-referral-sampling. With Snowball, the researcher identifies a person or members of a group, and those people assist by giving directions on where or how to find other suitable members of the population.
Quota	Quota is a sampling method that divides the target population into mutually exclusive sub-groups based on gender (male and female) or age (younger and older) or some other characteristic and selects a sample non-randomly to reach an established quota.

Marshall (1996) discusses convenience, judgment and theoretical as three sampling technique categories that can be employed in qualitative research. A combination of convenience, snowball, and judgment sampling were employed in this study. **Sections 5.9.1 to 5.9.3** discussed these techniques, why and how they were applied in this study.

5.9.1 CONVENIENCE SAMPLING

With convenience sampling, selections are made based on convenience and availability (Creswell, 2014). Convenience sampling is the least costly technique in terms of time, effort and money, making it an appropriate technique for this study, given that academic research is normally subjected to time and resource constraints. This technique also allows the selection of the most accessible subjects (Marshall, 1996). The accessibility can be due to the researcher's contacts and networks (Verma et al., 2017). Non-probability sampling is normally used in qualitative research (Saunders et al., 2016).

One of the most compelling arguments in favour of the convenience sampling approach is that it is suitable in challenging situations that may require the researchers' intervention, particularly in using their personal or professional contacts or connections (Verma et al., 2017). Therefore, since it is not easy to obtain permission to conduct research in South African healthcare institutions, convenience sampling was appropriate for selecting the case province in this study. The researcher had to use contacts to get a letter of approval to conduct the research. It was much more convenient and faster for the researcher to choose the case province because of the existence of contacts in the hospitals in the province.

Convenience sampling was applied in the following ways in the study:

- In selecting the province from which the study sample was selected
- Partly in the snowball process of selecting ICT respondents for the interview

According to the government regulations, South African public hospitals are categorised into district, regional, tertiary, central and specialised hospitals (Department of Health, 2012b). Besides specialised and central hospitals, these categories of hospitals can be found across all provinces.

South Africa has nine provinces, and the researcher had access, through the research gatekeeper, to subjects from Mpumalanga located in the North-East of South Africa as its research convenience sample. **Figure 5.13** indicates the South Africa map.



Figure 5.13: Provinces in South Africa (places.co.za)

Another factor that contributed to the choice of the province was the findings of various safety and security audit reports conducted on the health facilities in public hospitals (Department of Health, 2012c, 2012d). According to an audit report on the national healthcare facilities baseline, Mpumalanga was the second worst province in terms of patient safety and security (Department of Health, 2012d). Furthermore, based on the Department of Health report conducted by the ministerial task team on safety and security, Mpumalanga was among the provinces whose hospitals scored less than 30% on the security of their technologies or system security (Department of Health, 2012c). (The worst performing provinces are the hospitals in the Northern and Eastern Cape hospitals.) However, since the researcher did not have any support or gatekeepers to help gain access to the hospitals in these two worst-performing provinces, data collection did not take place in the provinces.

The researcher collected data from one district hospital (located in a rural area) and a tertiary hospital (located in an urban area); both were in Mpumalanga province. Data was not collected from specialised hospitals because the researcher assumed that it might be difficult for an outsider to gain access to such hospitals. The researcher also did not collect data from central hospitals since not all provinces have central hospitals. However, it was considered necessary to include hospitals in both rural and urban areas, as this would provide variety in the data and enable the researcher to boost the reliability of cybersecurity culture factors that would emerge during data collection.

Convenience sampling was first applied in selecting the participants for the interviews. The ICT manager in charge of one of the district hospitals was the first accessible person contacted by the researcher, with the assistance of a nurse in charge of communicating with the ICT section that supports their hospital. With the help of the ICT manager, the two ICT support staff members were also interviewed before the snowball process started.

Convenience sampling has recognised limitations. It may result in poor data quality and a lack of credibility (Marshall, 1996). To address these challenges, the researcher also employed judgment and snowball sampling in selecting the participant sample.

5.9.2 PURPOSIVE SAMPLING

Purposive sampling, also known as judgment sampling, is a non-statistical sampling technique where researchers select participants based on the specific information or knowledge they possess that can benefit the research (Verma et al., 2017).

Judgment sampling was applied by the researcher to select subjects with specific experience and subjects with special expertise (the key informant sample) who would be most able to provide detailed and credible answers to questions. As recommended by Saunders et al. (2016), participants were chosen because the researcher felt that a great deal could be learned from those individuals. Another reason judgment sampling was selected as a sampling method was that the study is a case study, and judgment is appropriate for case study research with a very small sample size (Saunders et al., 2016; Verma et al., 2017).

In this study, judgment sampling was used when collecting both the quantitative and qualitative data used to develop the proposed framework. Judgment sampling was also applied during the expert review to collect data to evaluate the framework after it was developed. Purposive sampling is a suitable method for situations that require participant populations that are particularly well-informed (Saunders et al., 2016; Verma et al., 2017). This was the case in this study, because the researcher selected the participants for the quantitative, qualitative and expert review on the basis that a great deal of information could be learned from the individuals due to their experience and expertise in:

- Using E-Health ICT systems (system users)
- Managing, maintaining or supporting E-Health and other ICT systems (ICT staff)
- Cybersecurity and cybersecurity culture in the industry or academic sector

Firstly, the researcher distributed the questionnaire to those research participants who were system users. These were participants who used E-Health ICT systems to carry out their daily duties. Participants who did not use the E-Health system were not given the questionnaire.

Secondly, data was collected from ICT staff in interviews. This was because the researcher viewed ICT staff as a group of participants with a genuine understanding of the ICT-related concerns. These participants could help the researcher understand the phenomenon in the given context and hence contribute to the development of the CCSCF of the study.

Thirdly, the link for the framework review questionnaire was shared with expert participants working in the area of cybersecurity and cybersecurity culture in industry or academia. This sub-sample was selected because they were believed to have comprehensive knowledge and experience in cybersecurity culture.

5.9.3 SNOWBALL SAMPLING

Snowball sampling finds interesting cases from people who know other people who would be suitable research participants (Verma et al., 2017). Hence, as recommended by Fink (2003), the initial participant or group member identified was asked to assist by identifying other potential participants. Snowball sampling was used solely for qualitative data collection (interviews) in this study. Etikan et al. (2015) explain that snowball sampling often starts with convenience sampling.

Snowball sampling is appropriate in situations where a list of potential research participants is not easily available, or where it is difficult to contact such people (Etikan et al., 2015; Fink, 2003). In the Mpumalanga province, the essential functions of the ICT department are managed and provided at the provincial level. Only limited ICT technical support is located at the district level, meaning that the province does not have a full ICT section physically located at any of its hospitals. Hence, in this study, snowball sampling was used as the basis for the qualitative data collection because it was not easy for the researcher to get a list of ICT staff, including their contact details.

In this study, the researcher started by contacting an ICT manager who was immediately accessible. The ICT manager had been introduced to the researcher via a nurse in the district-level hospital where the data was collected. As part of her duties, this nurse interacted with the ICT section at the district level because she reported or communicated ICT issues to them. The ICT manager, in turn introduced the researcher to two support staff members, and they were

contacted and interviewed. After that, these recruited participants assisted in getting other participants (including those at the provincial level) and the sample snowball gathered participants until the series of interviews was completed.

5.9.4 SAMPLING STRATEGIES VERSUS DATA COLLECTION METHODS

This section provides a short summary of the sampling strategies used in terms of data collection methods.

The convenience, purposive and snowball sampling strategies that were applied for quantitative and qualitative data collection used questionnaires, semi-structured interviews and expert reviews.

For quantitative data collection:

- Convenience sampling was applied when selecting the province.
- Purposive sampling was applied when selecting medical and administrative staff (system users) to complete the questionnaires.

For qualitative data collection:

- Convenience sampling was used when selecting the province.
- Purposive sampling was used when selecting cybersecurity and cybersecurity culture experts, and ICT staff for the expert review and semi-structured interviews.
- Snowball sampling was used when ICT staff were selected to be interviewed (semi-structured interviews).

5.9.5 SAMPLING SIZE

There have been numerous discussions concerning an acceptable sample size. However, many scholars believe that saturation is the most crucial factor to consider when deciding whether the sample is large enough (Charmaz, 2006, 2014; Dworkin, 2012; Marshall, 1996; Mason, 2010).

The factors that influenced the sampling size in this research were as follows.

- (1) The research was a case study and had a small number of possible participants. The research was not defined universally, but as a case of the Mpumalanga province. A case study requires a small sample size (Creswell, 2014).

- (2) A limited number of medical and non-medical staff used Internet-based ICT in the hospitals where data was collected. This requirement (use Internet-based ICT in the hospital) was stipulated for selecting participants for quantitative data collection and affected the number of respondents.
- (3) There were a limited number of ICT staff who provided ICT support for the whole hospital. Therefore, qualitative data collection was limited to the available ICT staff.

In the qualitative data collection, the researcher interviewed one ICT manager of the two or three managers in the selected district and tertiary hospitals. The general ICT staff were also interviewed until the researcher was satisfied that sufficient data had been collected to answer the research questions, that is, until the data collection was at its saturation stage (Dworkin, 2012; Marshall, 1996; Mason, 2010).

- (4) The expert review focused on qualitative data collection and also only required a small sample. Additionally, the nature of the work that the cybersecurity experts were involved in affected their availability. The principle of data saturation also applied to the sample of experts who participated in the review as a qualitative inquiry.

Table 5.10 depicts a summary of the sampling frame and the responses achieved.

Table 5.10: Sampling Frame and Responses

Method	Category	Description	Distributed (n)	Achieved Responses (n)	Response rate (%)
Quantitative research	Public hospital healthcare workers	Medical like Doctors, Nurses, and Admin staff word clerks, HR staff	120	99	83%
Qualitative research	Public hospital healthcare workers	ICT staff and ICT managers	11	9	82%

5.10 ETHICAL CONSIDERATIONS

The primary objective of ethics is to ensure that everyone involved in a research project is protected and treated fairly and honestly by the researcher throughout the research process.

This is regardless of whether the person is involved directly or indirectly in the research (Oates, 2006). Ethics speaks to the moral principles that guide a research project.

Ethics is an essential aspect of every type of research and institutions require researchers to obtain ethical clearance before the commencement of any study. According to Creswell (2014), it is the responsibility of researchers to make sure the ethical requirements and standards of their institution are adhered to. Therefore, it is the responsibility of researchers to protect the research participants and respondents, protect their own organisation and the organisations to which the other participants belong from misconduct and improper behaviours. The researchers must also address any problem ethically that might emerge during the research.

The ways in which ethical issues were addressed in this study are presented below.

- Ethical clearance to conduct this study was approved by the University of South Africa College of Agriculture and Environmental Sciences (CAES) health research ethics committee (see APPENDIX_2A).
- The hospitals granted the researcher consent to conduct the research at their facilities. See APPENDIX_2B for the combined hospital's support letter. The consent from the hospitals was used to apply for permission at the provincial level. The Mpumalanga Provincial Department of Health Research Committee granted the researcher permission to conduct the research in the province (see APPENDIX_2C).
- Informed consent forms were signed by participants who completed the questionnaire and consented to by the interviewees, confirming their participation in the study was voluntary. Participants were provided with a description and explanation of the purpose of the study. They were also informed that completion of the questionnaire and participation in the interview were voluntary and that they had the right to withdraw at any point in time.
- The research participants' confidentiality and anonymity were maintained as per the university research policy. The researcher ensured that answers were not connected to participants. Responses from participants were numbered for identification (e.g., participant no 1, 2, 3, etc.), and that is how the participants were referred to during data analysis and presentation. The same is the case for publications arising from this research. The only people who had access to the raw data were the researcher and her supervisors.

When the ethical considerations were addressed, further critical reflection was provided regarding data protection and confidentiality in the E-Health context, given that cybersecurity practices and organisational vulnerabilities formed part of the data. The study ensured that secured digital storage, protected file strategies, and secure transmission of electronic responses were used. Identifying details were removed during transmission to prevent traceability. These measures strengthened participant protection and upheld confidentiality within the sensitive health information environment.

5.11 CONCLUSION

Chapter 5 has presented the research design followed in conducting the research. The researcher viewed the world pragmatically, allowing her to choose methods, techniques and procedures that best answered the research questions. The study followed a mixed-method approach. This approach allowed the researcher to use both quantitative and qualitative data collection techniques. The collection and analysis of qualitative and quantitative data were done concurrently in this research. Quantitative data was collected and analysed quantitatively, while qualitative data was collected and analysed qualitatively.

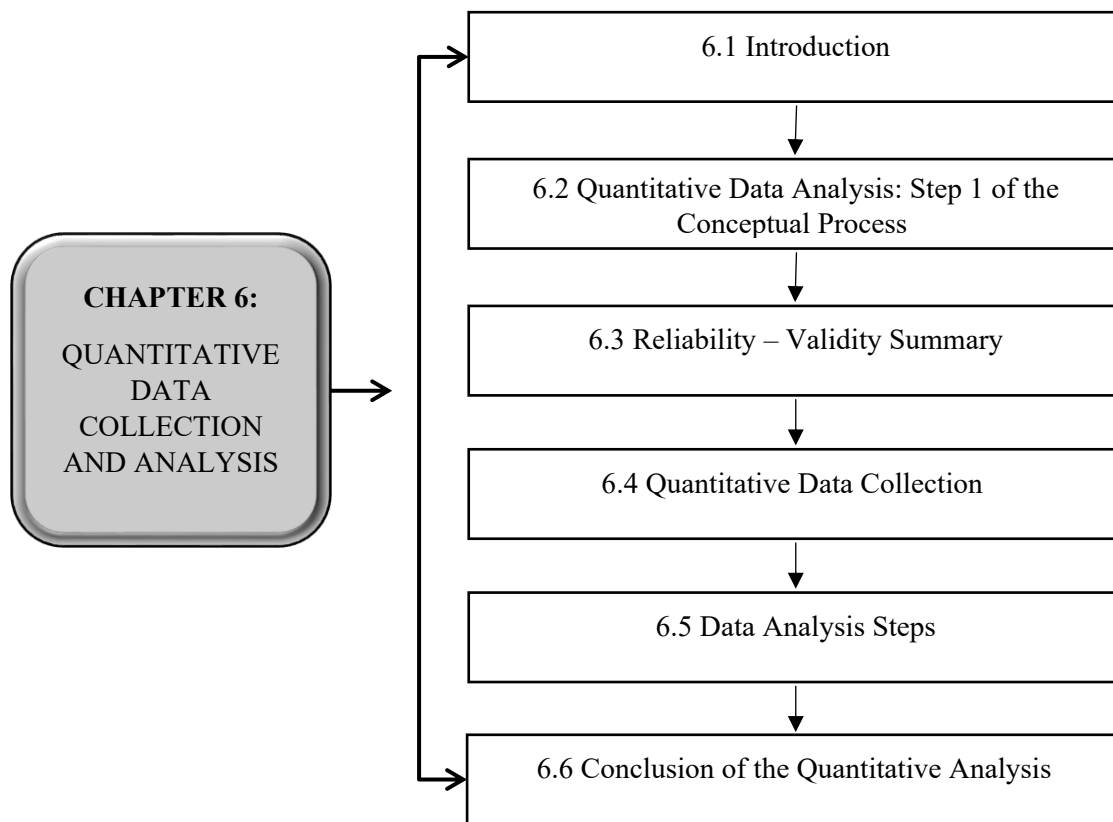
Interviews were conducted with ICT personnel, and the data collected was analysed using thematic analysis to identify essential cybersecurity culture contextual factors.

The questionnaire was designed from scratch, based on the different categories of research constructs found from the systematic review. The use of a questionnaire provided quantitative data that was analysed statistically. The findings from the questionnaire were triangulated with the qualitative findings to ensure the reliability and validity of the cybersecurity culture factors identified for the contextual framework. Understanding the meaning behind the data collected via interviews was essential.

The chapter demonstrates the conceptual framework analysis as the research strategy followed to achieve the main research question: *How can a contextual framework for establishing cybersecurity culture in the public E-Health institution in South Africa be developed and evaluated?*

The next two Chapters 6 and 7 present the qualitative and quantitative data collection and analysis.

CHAPTER 6: QUANTITATIVE DATA COLLECTION AND ANALYSIS



6.1 INTRODUCTION

A comprehensive list of factors and constructs associated with cybersecurity culture was identified in Chapter 4 through a review of the literature. Using the data collection and analysis methods discussed in Chapter 5, this chapter presents the empirical findings of the research data originating from the completed questionnaires.

The data analysis is presented in two parts. Part 1, which is in this chapter, presents the quantitative analysis. The results presented will be integrated through triangulation with the outcome of Part 2 (see Chapter 7) to answer the Research Sub-Question 3 (RSQ 3):

Research Sub-Question 3 (RSQ 3) *“What factors are associated with cybersecurity culture in the public E-Health institutions in South Africa?”*

The quantitative statistical analysis was carried out using version 28.0 of the Statistical Package for Social Sciences (SPSS) and Analysis of Moment Structures (AMOS) version 28.0.

This quantitative analysis chapter is summarised as follows: **Section 6.2** presents the role of quantitative analysis in achieving Step 1 of the conceptual framework analysis. **Sections 6.4** and **6.5.1** revisit data collection and analysis, and provide a framework for the quantitative analysis. **Section 6.5.2** presents the participant demographic statistics. In **Section 6.5.3**, the research constructs that shaped the measurement of the phenomenon of cybersecurity culture were revisited. Construct and instrument reliability and validity assessment of the measurement instrument were conducted in the study, and the results are presented in **Sections 6.5.4** and **6.5.5**. This is followed by descriptive analysis, Pearson correlation coefficient analysis and the conclusion of the quantitative analysis (see **Sections 6.5.6, 6.5.7** and **6.6**).

6.2 QUANTITATIVE DATA ANALYSIS: STEP 1 OF THE CONCEPTUAL PROCESS

Chapter 4 discussed the eight phases of the conceptual framework analysis process that were followed during the design and development of the cybersecurity culture contextual framework. The conceptual framework was made up of three steps. Step 1 consisted of phases 1 to 5, but this chapter only deals with activities that are related to the first three of those phases.

An extract from **Figure 5.8** which depicted the phases from Step 1 of the conceptual framework, is presented in **Figure 6.1**.

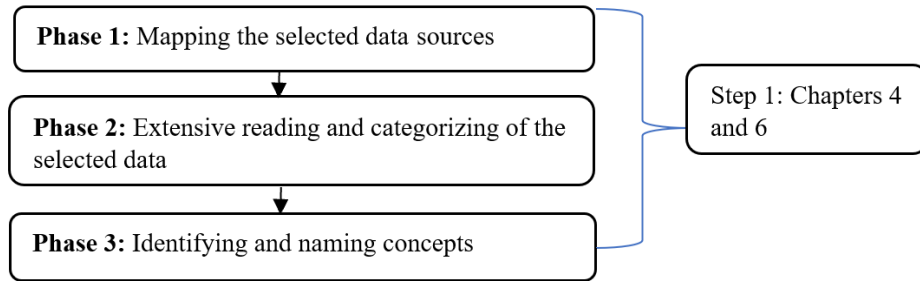


Figure 6.1: Step 1 of the Conceptual Framework Analysis (Adapted from Jabareen, 2009)

This chapter, which deals with collecting and analysing quantitative data to identify cybersecurity culture factors from system users' perspectives, is the second strategy followed to assist with accomplishing Step 1 of the conceptual framework analysis process. The three phases of Step 1 covered in this chapter are described in the sections that follow.

6.3 RELIABILITY-VALIDITY SUMMARY

Table 6.1 provides a brief statistical summary as proof of the validity and reliability of the research measurement instrument.

Table 6.1: Compact Reliability and Reliability

Factors	Questions	Cronbach's (α)	Factor retention	Variance Explained	Decision
Preparedness (P)	Q8_1 - Q8_15	(α) = .900	1 factor retained; eigenvalue > 1); factor loadings > 0.3; acceptable communalities (.652–.846)	45.174%	Reliable & Valid
Responsibility (R)	Q13_1 - Q13_19	(α) = .627	1 factor retained; eigenvalue > 1); factor loadings > 0.3; acceptable communalities (.651–.802)	17.047%	Reliable & Valid
Management (M)	Q14_1 - Q14_16	(α) = .816	1 factor retained; eigenvalue > 1); factor loadings > 0.3; acceptable communalities (.667–.834)	7.350%	Reliable & Valid

Factors	Questions	Cronbach's (α)	Factor retention	Variance Explained	Decision
External Environment (EE)	Q15_1 - Q8_6	(α) = .731	1 factor retained; eigenvalue > 1); factor loadings > 0.3; acceptable communalities (.664-.759)	2.116%	Reliable & Valid
Technology (Tech)	Q16_1 Q16_2	(α) = .607	1 factor retained; eigenvalue > 1); factor loadings > 0.3; acceptable communalities (.664-.759)	1.955%	Reliable & Valid
Extraction Method: Principal Component Analysis.					
Retention logic: Eigenvalue > 1; factor loading threshold > 0.3					

Reliability was established through Cronbach's alpha (α). This helped the researcher to measure the internal consistency of the research instrument. Cronbach's alpha (α) values of 0.6 and above ensure the reliability of the research instrument. The validity of the study was achieved using five step Exploratory Factor Analysis (EFA): (1) Kaiser-Meyer-Olkin (KMO) achieved an acceptable value of 0.761 across the research constructs and a p-value of 0.001 which indicated a significant result; (2) The Bartlett's test indicated above 95% degree of confidence with a p-value of 0.001; (3) Communality depicted values in the range between 0.651 and 0.846 for all constructs indicating a good relationship between constructs; (4) Total Variances Explained (TVE) identified 15 relevant components with eigenvalues greater than 1. The total variance showed a result of 73.642%, which indicated a statistically significant value. The research factors were valid as they obtained a loading value of more than 0.3, meaning that all the items of the questionnaire loaded on values greater than 0.3.

6.4 QUANTITATIVE DATA COLLECTION

The main objective of this research was to develop a contextual framework that could assist with establishing a cybersecurity culture in public E-Health institutions. As staff in public healthcare institutions were the main subject of this study, approaching them during the first phase, as a source of quantitative data, was necessary to prepare for gathering pertinent information.

The participants selected were system users, that is, they were people (the medical and administrative staff) who made use of Internet-based ICT devices routinely as part of their

work in the hospital. Collecting data from these participants helped the researcher to take an in-depth look into the factors, from system users' perspectives, which would form the basis of the contextual framework for establishing cybersecurity culture.

The quantitative part of data collection focused on system users who were considered not to be experts and were not experienced enough in ICT-related issues to engage them in an interview discussion. Therefore, a questionnaire was used to collect data from them. The nature of the selected participants' daily work was also considered when the decision was made for them to be engaged through a questionnaire.

As detailed in the methodology chapter (see Chapter 5), data was collected from one district hospital (Carolina Hospital) and one tertiary hospital (Witbank Hospital) in Mpumalanga as the research case for achieving the first phase of the conceptual framework. These two hospitals were selected because there was a gateway person who was prepared to introduce the researcher to the hospital management to seek approval to conduct the research in those facilities.

During quantitative data collection, 120 questionnaires were distributed to participants at the two hospitals, and 99 ($n = 99$) were completed. The completed questionnaires were the data source for the first phase. One of the major obstacles to collecting the data from medical and administrative staff in these hospitals was their everyday tasks, which restricted them from using ICT devices. The participants in Phase 1 data collection included medical staff (doctors, nurses, pharmacists, theatre assistants, clinical associates) and administrative staff (ward clerks, information officers, and human resource staff).

- Data collection instrument

Chapter 5 indicated that the design of the questionnaire as the collection instrument for quantitative data consisted of six sections (A to F). Section A had questions related to demographic information, and the remaining sections collected data regarding the different constructs of cybersecurity culture using a rating scale. The rating scale had five options and participants had to select one of these as an answer to each of the questions. The options were based on five levels of agreement, with 1 meaning strongly disagree, 2 meaning agree, 3 meaning neutral, 4 meaning agree and 5 meaning strongly agree.

6.5 DATA ANALYSIS STEPS

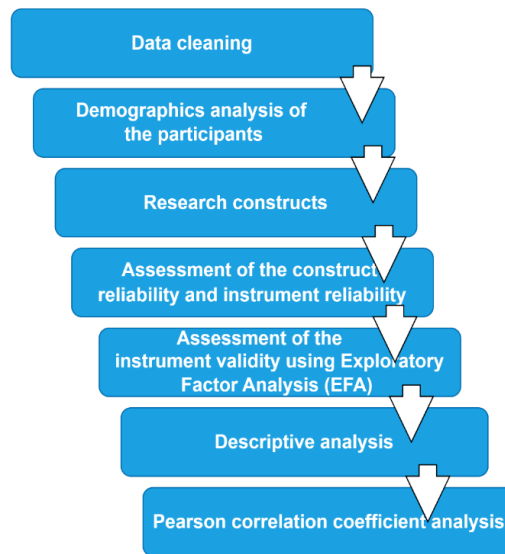


Figure 6.2: Quantitative Data Analysis Process (own source)

Figure 6.2 gives an overview of the steps used to analyse the quantitative data of the study. **Figure 6.2** shows how the data was collected in the first phase, was analysed and that the data was categorised using reliability tests and exploratory factor analysis. The second and third phases were achieved using descriptive and Pearson correlation analysis.

The remaining sections of this chapter, starting with data cleaning in **Section 6.5.1**, focus on the various steps undertaken during analysis and the results of those steps.

6.5.1 DATA CLEANING

Data cleaning prepared the data collected in the first phase for use in the second and third phases. The researcher assessed the data to ensure that only acceptable data (for example, completed data) would be used in the statistical analysis and to ensure that the research estimates were well-founded.

The collected data was captured and saved using Microsoft (MS) Excel. Attention was given to ensuring the appropriateness of data during the capturing process. The captured data was imported into SPSS software to prepare for analysis. The process of data cleaning during of these activities included:

- Check the questionnaires for duplicates and inconsistencies before they were captured.
- Check each question for obvious problems in data before it was captured,

- Check the correctness of data imported into SPSS. This was done in two ways: by cross-checking the data in SPSS against data on the original questionnaire and by using Excel to ensure data was captured correctly.
- Check for missing values in the data imported to SPSS for analysis.

Using SPSS, the missing values in the demographic analysis (Section A of the questionnaire) were highlighted and replaced with the mode, and the missing data in the descriptive statistics (Sections B - F of the questionnaire) were highlighted and automatically taken as appropriate for the study.

The mean per individual question used to map the data source for the quantitative data was above 0.5 to remove the bias of the participants in answering the research questions.

In this study, some of the questions were asked in the positive form or in the negative form to reduce participants' bias. The researcher treated all the questions in this study by converting negative questions to positive ones. The main reason to treat negative questions as positive was to measure a construct in one direction, which in this study was in a positive direction. There were no issues with skewness and kurtosis in the study - the data was normally distributed (Garren & Osborne, 2021).

6.5.2 DEMOGRAPHIC ANALYSIS OF THE PARTICIPANTS

The second phase of the conceptual framework, namely extensive reading and categorisation of concepts, was achieved through the analysis and interpretation of the quantitative data. Demographic analysis was used to study the characteristics of the participants in terms of gender, age, education level, job title, work experience in the hospital, and the use of a computer together with the Internet.

Table 6.2 to Table 6.5 show the demographic information of the 99 participants who responded to the questionnaire. The demographic analysis included the age, gender, education level, job title, participants' department or section at work, time worked in the hospital, use of ICT at work, and access to confidential data of patients.

Table 6.2: Age of the Participants

		Frequency	Percent
Age (in years)	21- 30	32	32.3
	31- 40	29	29.3
	41- 50	20	20.2
	51- 60	15	15.2
	60+	3	3.0
	Total	99	100.0

The analysis shows that the research participants were spread across different age ranges (see Table 6.2). A third of the participants (32.3%) were between 21 and 30 years old; almost as many (29.3%) were between 31 and 40 years, 20.2% were between 41 and 50 years. The older participants between 51 and 60 years contributed 15.2%, and those above 60 contributed 3%, respectively. Hence, there was a fairly even distribution across three age groups: 21 to 30, 31 to 40 and older than 40. This finding was considered favourable in the research as it would mean that the constructs that measure cybersecurity culture were evaluated by people from diverse age groups and not only by one specific group.

Table 6.3: Gender of the Participants

		Frequency	Percent
Gender	Male	43	43.4
	Female	56	56.6
	Total	99	100.0

Regarding gender, 43.4% of the participants were male, and 56.6% were female. Slightly more participants were female because in the hospitals, almost all the nurses were female. This also reflects the South African Nursing Council manpower distribution, which shows that the nursing profession is dominated by females (South African Nursing Council, 2022).

Education levels in this study are categorised into Secondary Education, Vocational Professional nursing training, Bachelor's degree, Master's (MSc) degree, and Doctoral (PhD) degree. Bachelor's degree had the highest number of participants with 57.6%, followed by PhD degree with 19.2, MSc degree with 9.1%, Secondary Education 8.1% (8), and Vocational professional nursing training with 6.1% (6).

The biggest group of participants was those with degrees (see Table 6.4) and these participants might have had knowledge of computer and Internet use, which positioned them as appropriate participants to answer the questionnaires. This is in line with reported research findings which show that higher education increases people's use of computers (Riddell & Song, 2017).

Table 6.4: Education Level of Participants

		Frequency	Percent
Education Level	Secondary Education	8	8.1
	Vocational professional nursing training	6	6.1
	Bachelor's degree	57	57.6
	Master's (MSc) degree	9	9.1
	Doctoral (PhD) degree	19	19.2
	Total	99	100.0

Other demographic characteristics covered included the participants' job titles and the period they had worked in the hospital, as depicted in Table 6.5.

Table 6.5 shows that the largest group of participants (36.4%) were medical doctors - every doctor used at least one ICT device to offer services to patients. Followed by administrative personnel (20.2%) and 'others' (18.2%), which was a collection of social workers, dieticians and physiotherapists. The two smallest groups were nurses (17.2%) and pharmacists (8.1%).

Table 6.5 also shows the participants' experience working in hospitals. Of the participants, 43.4% had between 1 and 3 years of experience, and 39.4% and 7.1% had worked in the hospital for more than 10 years or between 6 and 10 years. The rest of the participants had worked for between 4 and 5 years in the hospital. This confirmed that the participants were fairly experienced, and hence could be expected to be knowledgeable about the operation of the hospital as they had worked in the institution for at least 12 months. Therefore, they would have been able to answer questions that measured the cybersecurity culture constructs in relation to their hospitals.

The participants who completed the questionnaire did not include ICT personnel (ICT personnel only participated in the interviews, collecting qualitative data). The participants considered in this section were the appropriate group for the questionnaires, and the results collected were a true representation of their hospital cybersecurity issues.

Table 6.5: Other Demographics of the Participants

		Frequency	Percent
Job Title	Doctor	36	36.4
	Nurse	17	17.2
	Pharmacist	8	8.1
	Administrative personnel	20	20.2
	Other	18	18.2
	Total	99	100.0
Period Worked in Hospital	10+ years	39	39.4
	6-10 years	7	7.1
	4-5 years	10	10.1
	1-3 years	43	43.4
	Total	99	100.0

The remaining demographic data tables are in APPENDIX_3B. Based on that data, 91.9% of the participants said that they use ICT with the Internet for work purposes in the hospital, and only 8.1% indicated that their work did not involve the use of ICT. The vast majority (96%) had access to confidential and sensitive patient data; only 4% did not have access to such data. This result is important as it confirms the appropriateness of the research participants. It showed that, because the participants make regular use of Internet-based ICT to function in the institution, they could themselves be targets of cyber threats and attacks and that through them, the healthcare institution could experience cyber-attacks.

The demographic information showed that the people who answered the questionnaire were distributed across various departments or sections of the hospitals. These included maternity, admissions, casualty, family medicine, nursing management, paediatrics, ward clerk, information management, clinical associate, theatre and pharmacy. See APPENDIX_3B for the data analysis of time worked in the hospital, use of Internet-based ICT for work, access to confidential information, and the departments the participants worked at.

The result of the demographic analysis shows that the research participants had experience working in a medical setting, while making use of Internet-based ICT in their work to access patients' data. Therefore, they were an appropriate source of the quantitative data used to identify the factors associated with cybersecurity culture in this study.

6.5.3 RESEARCH CONSTRUCTS

To assist readers in understanding the upcoming sections, this section introduces the research constructs. The five constructs identified in Chapter 5 that formed the basis for measuring the cybersecurity culture phenomenon were:

- Preparedness (P),
- Responsibility (R)
- Internal organisational management (IOM) also referred to as Management cybersecurity practices (MCP) or Management (M)
- External environment and non-organisational management (EENOM), which can be referred to as External environment (EE)
- Technology (TECH)

For the rest of the quantitative and qualitative analysis, IOM is often referred to as Management (M), and EENOM will frequently be referred to as External Environment (EE) or environment.

These constructs were identified and adapted in Chapter 5 based on a combination of constructs from the following frameworks:

- Cybersecurity culture frameworks (Da Veiga, 2019; ENISA, 2017; Georgiadou et al., 2020b; Huang & Pearlson, 2019),
- Human Factor Domain (HFD) framework (Alhogail et al., 2015),
- STOPE framework, which is widely used to tackle digital technology problems in ERP, e-government, and e-readiness assessment (Bakry & Bakry, 2003; Bakry, 2005).

Elements that emerged from cybersecurity culture definitions in literature also supported the selection of these constructs.

The constructs of preparedness and responsibility were used to measure individual or human factors at the internal organisation level. In this study, preparedness and responsibility are used to represent organisational culture as the constructs contain components of human attitudes, perceptions and beliefs.

- Preparedness (P) relates to employees' awareness and competency, and their education on cybersecurity issues. Preparedness was measured in Section B of the questionnaire using question Q8. Q8 consisted of 15 individual items (Q8.1 to Q8.15).

- Responsibility (R) relates to human attitude and behavioural factors, for example, the practices and personalities of employees of the organisation in terms of cybersecurity. The construct is measured in Section C of the questionnaire using question Q13, which contains nineteen individual items Q13.1 to Q13.19.
- The Management (M) construct also relates to factors at the internal organisation level, but focuses on actions that are performed at the managerial level. This construct is measured in Section D of the questionnaire using question Q14, which comprises items Q14.1 to Q14.16.
- The External Environment (EE) construct deals with factors that are external to the healthcare organisation environment. The environment construct relates to non-organisational factors, such as law, regulations, competition between peer institutions, and external contracts and outsourcing. The External Environmental construct was measured using question Q15 in Section E of the questionnaire, which is made up of individual items Q15.1 to Q15.6.
- The Technology (TECH) construct in this proposed framework deals with relevant Internet and information technology issues related particularly to the use of technology. Examples include the increasing number of cyber-related threats, new and fast-emerging technologies, and the increasing need to use these new technologies. The construct was covered in Q16.1 and Q16.2.

6.5.4 ASSESSMENT OF THE CONSTRUCTS' RELIABILITY AND INSTRUMENT RELIABILITY

This section analysis in this evaluates the reliability of the research instrument used for the data source in the first phase. Questions found not reliable were removed, and thus, this process focused on identifying and naming the concepts that would be used in the third phase of the framework.

Reliability is used to assess the measurement instrument (i.e., the survey questionnaire) for consistency and accuracy (DeVillis, 2017; Streiner, 2003). In this study, Cronbach's alpha was used to ensure that the measurement instrument used in the study was reliable and could accurately assess the research constructs of preparedness, responsibility, management and environment. Consequently, it was used to ensure the validity of the research result as it was produced through consistent and accurate findings.

Constructs' Reliability Assessment: Cronbach's alpha (α) was used in this research to measure the internal consistency of a scale or questionnaire, and its value ranges from 0 to 1, with higher values indicating greater internal consistency. It is generally accepted that the threshold value for Cronbach's alpha is 0.6 or higher (Cossío-Silva et al., 2016; Hair et al., 2019; Hotchkiss et al., 2010). The assessment of internal consistency reliability in this study was conducted based on this value. The aim was to check the internal consistency of the individual construct measurement variables (Pallant, 2020). Research constructs or decision factors such as preparedness (P), responsibility (R), management (M), external environment (EE), and technology (TECH) were analysed for their internal consistency and stability.

The Cronbach's alpha values of all the research constructs were above or equal to the threshold value of 0.6 (Cossío-Silva et al., 2016), as depicted in Table 6.6.

Table 6.6: Cronbach's Alpha Reliability of the Construct Items

Constructs (factors)	Cronbach's Alpha
Preparedness (P)	0.900
Responsibility (R)	0.627
Management (M)	0.816
External Environment (EE)	0.731
Technology (TECH)	0.607
cybersecurity culture	0.896

The construct preparedness (P) measured by Q8 had a Cronbach's alpha value of 0.900. The construct Management (M) measured by Q14 had a value of 0.816. The construct representing responsibility (R) (Q13 but excluding 3 items, namely Q13.9, Q13.11, and Q13.18) had a Cronbach's alpha value of 0.627. External environment (EE) was measured using of Q15, but two questions (Q15.6 and Q15.8) were excluded. EE had a Cronbach's alpha value of 0.731. Finally, technology (TECH) had a value of 0.607. For detailed individual items, specific Cronbach's alpha, see APPENDIX_3C

The research instrument must be reliable if it is to develop and evaluate the research objectives. Since all the Cronbach's alpha values were above or equal to the threshold of 0.6, it meant that the research instrument used for the study data source was reliable. Therefore, this was an indication that the instrument was fit for further analysis.

As previously indicated, Table 6.6 summarises the results of the reliability test. The result showed that all the constructs or decision variables met the Cronbach's benchmark of 0.6. The result was an indication that all the questions of the questionnaire were reliable and, therefore, could be used in answering **Research Sub-Question 3 (RSQ 3):** *“What factors are associated with cybersecurity culture in the public E-Health institutions in South Africa?”*

6.5.5 ASSESSMENT OF THE INSTRUMENT'S VALIDITY USING EXPLORATORY FACTOR ANALYSIS (EFA)

Exploratory Factor Analysis (EFA) was used to identify latent variables that explain the correlations among a set of observed factors (preparedness (P), responsibility (R), management (M), external environment (EE)) through the reduction technique, and technology (TECH), following the steps of (Pallant, 2020).

To ensure that the research questionnaire was able to produce accurate and reliable factors that are associated with cybersecurity culture in E-Health institutions, a validity assessment was conducted. According to the conceptual framework phases followed in this study, this process was required to identify and name the concepts, which is the third phase of the framework. Validity of a construct is the degree to which a question (made up of a group of items in a questionnaire) measures what it was intended to measure (Pallant, 2020).

In this study, the construct's validity was measured by exploring the relationship between the research instrument related to the constructs investigated by means of the questions in the questionnaire. These constructs were preparedness (P), responsibility (R), management (M), technology (TECH) and external environment (EE).

The assessment of validity using Exploratory Factor Analysis (EFA) was performed following five steps: Kaiser-Meyer-Olkin (KMO), Barlett's, Communalities, Total Variance Explained (TVE), Scree plot and Component Matrix.

6.5.5.1 KAISER-MEYER-OLKIN (KMO) AND BARLETT'S TEST

Kaiser-Meyer-Olkin (KMO) is a measure of sampling adequacy used in exploratory factor analysis (Pallant, 2020). The KMO statistic measures the proportion of variance in the observed variables that can be explained by a common set of underlying factors. Hence, KMO is used as an indicator to determine the suitability of correlation metrics for factor analysis.

The KMO value ranges from 0 to 1, with higher values indicating better sampling adequacy. A KMO value of 0.6 (60%) or above is generally considered acceptable for factor analysis (Kaiser & Rice, 1974; Pallant, 2020).

Barlett's test and KMO are both statistical measures that are used by SPSS to evaluate how factorable the research data is (Pallant, 2020). The acceptable Barlett's test has a p-value of 0.05 or less (Pallant, 2020). The Barlett's value of 0.05 or smaller indicates the existence of a significant correlation between the indicators for factor analysis. The general expectation is that there should be a moderate to strong relationship between the indicators (variables or items) for them to be suitable for factor analysis.

The results of the sphericity measurement, known as the Kaiser-Meyer-Olkin value (KMO) and Bartlett's Test, are shown in Table 6.7. The KMO value of 0.761 indicated the percentage of variation that was shared across the four constructs, preparedness (P), responsibility (R), Management (M), technology (Tech) and external environment (EE). This KMO value was significant for assessing the components as recommended by Pallant (2020).

A p-value (Sig) of less than 0.05 indicates a significant result (it is not due simply to chance), and in this study, Bartlett's test has a p-value of 0.001, indicating a more than 95% degree of confidence in the results. This demonstrates how the KMO and Bartlett's test was used as the first stage to test validity.

Table 6.7: KMO and Bartlett's Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.761
Bartlett's Test of Sphericity	Approx. Chi-Square	3301.716
	df	1378
	Sig.	.000

The data depicted in Table 6.7 shows a favourable KMO measure of 0.761. This indicates a large correlation between the decision variables analysed. Similarly, the in Table 6.7 shows a significant Bartlett's test value ($p < 0.05$). Therefore, the result indicates a significant relationship between the items and that it is appropriate to perform factor analysis on them.

6.5.5.2 COMMUNALITIES

Communalities show the extent to which each variable's variance had been accommodated. It is an indication of how a construct correlates with other constructs (Pallant, 2020). Items with communality values of less than .3 are an indication of non-correlation (Pallant, 2020). A low-value communality means that the item does not relate well with the other items in its component and should be removed (Mohd Rohani et al., 2009; Pallant, 2020).

Communalities were calculated as the sum of the squared factor loadings for each variable, and range from 0 to 1 (Pallant, 2020). A high communality value (0.3 and above) indicates that the variable is well-represented by the factor solution, while a value below 0.3 indicates that the variable should be removed.

The variables in this study had communality extraction values ranging from 0.651 to 0.846 (see Table 6.8). Hence, the communality extraction values for all 53 items of the questionnaire, measuring the different constructs, were between 0.651 and 0.846. This was an indication that a good association existed between the constructs represented by the items of the questionnaire. This, therefore, means that the items of the questionnaire were appropriate for answering **Research Sub-Question 3 (RSQ 3)**, which aimed to identify factors associated with cybersecurity culture in public E-Health institutions in South Africa.

Table 6.8: Summarised Extraction of the Instrument Communalities

Communalities		
Questions	Initial	Extraction (Range)
Q8_1 - Q8_15 Preparedness (P)	1.000	.652 -.846
Q13_1 to Q13_19 Responsibility (R)	1.000	.651 -.802
Q14_1 to Q14_16 Management (M)	1.000	.667 -.834
Q15_1 to Q15_6 External Environment (EE)	1.000	.664 -.759
Q16_1 to Q16_2 Technology (TECH)	1.000	.664 -.759
Extraction Method: Principal Component Analysis.		

Table 6.8: Summarised Extraction of the Instrument Communalities

Table 6.8 shows the summarised communalities (ranges showing results for the items in the question) extracted for the research construct questions. These values are sorted from the

smallest to the largest lower range value and do not give the extraction value per item. For detailed individual items specific communality, see APPENDIX_3D.

A communality with a value close to 1 shows items with a high correlation with other items. As depicted in Table 6.8, the lowest communality value extracted was 0.664, found for items in both the external environment (EE) and technology (TECH) constructs (for example, Q16.1 and Q16.2).

Table 6.8 shows that the highest communality (0.846) was found in item Q8.9 of the preparedness (P) construct.

The results of the extracted communalities showed that the values were all above 0.5. This, therefore, indicated that the major components extracted explained many variances of the research items (Q8.1 to Q16.2, but excluding questions Q13.9, Q13.11, Q13.18, Q15.6, and Q15.8). None of the items' values were below 0.3, meaning that all items related well, and as a result, no further items were removed. In this study, communalities were used as stage two of testing validity.

6.5.5.3 TOTAL VARIANCE EXPLAINED (TVE) AND ROTATED COMPONENT MATRIX

Table 6.9 to Table 6.12 depict an excerpt from the component matrix, along with the cumulative results of the total variance's findings for the research constructs. These tables also show loadings for each factor on each rotating component and the eigenvalues of the factor construct.

According to Pallant (2020), the eigenvalue is used to indicate the total number of variances the factor explains, and this is among the most popular techniques used for the extraction of factors. The eigenvalue rule recommends the selection of factors with an eigenvalue greater than 0.1 for further investigation (Pallant, 2020). The study employed the eigenvalue rule to determine which of the factors should be extracted.

Total Variance Explained (TVE) shows what percentage of a dataset's overall variability can be accounted for by a given collection of variables, and hence is used to decide how many components or factors to retain (Hair et al., 2019; Jolliffe, 2002; Pallant, 2020). TVE is often used in conjunction with other extraction methods and multivariate statistical analysis, such as eigenvalues and scree plots, as well as factor analysis and Principal Component Analysis (PCA). With these methods, TVE is employed to assess how well the analysis captured the variability in the initial dataset (Hair et al., 2019; Jolliffe, 2002).

In this study, TVE identified that 15 components were relevant as they had eigenvalues greater than 1. PCA was used as a reduction tool to find the most important components using the varimax rotation technique. Additionally, as shown in Table 6.9 to Table 6.12 constructs that had Eigenvalues larger than 1 were loaded in categories.

The criteria for the total variance should be greater than 60% (Chiyangwa & Mnkandla, 2017; Pallant, 2020). The results of this investigation can be regarded as statistically significant because the total variance (73.642%) explained all the factors in the study (through the 14 components) and was above the 60% threshold. Forty extraction iterations were performed in as required by the 14 categories, and the 53 components together contributed to the variance of 73.481%.

The factors that are loaded in each component are determined by the rotation process. According to Pallant (2020), a valid factor is one with a loading value greater than 0.3. As can be seen from Table 6.9 to Table 6.12, all items of the questionnaire loaded above 0.3 on a component and the 53 research items were loaded on 14 components.

Table 6.9: Factor Loading and TVE of Preparedness Construct

Factors	Questions	Rotated Component Matrix	Component Matrix	Total Variance Explained	Eigenvalue
Preparedness (P)	Q8_1	.538	1	45.174%	23.942%
	Q8_2	.646			
	Q8_3	.679			
	Q8_4	.431			
	Q8_5	.745	2		
	Q8_6	.593			
	Q8_7	.717			
	Q8_8	.519			
	Q8_9	.447	3		
	Q8_10	.479			
	Q8_11	.610			
	Q8_12	.702			
	Q8_13	.485	4		
	Q8_14	.672			
	Q8_15	.701			

Factors	Questions	Rotated Component Matrix	Component Matrix	Total Variance Explained	Eigenvalue
Extraction Method: Principal Component Analysis					
a. 4 components extracted					

For preparedness (P) (see Table 6.9) four items were loaded onto components 1, 2 and 3, and three items were loaded onto the 4th component. Hence, preparedness (P) was the component with the highest values (45.174%) on the TVE compared with responsibility (R), management (M), technology (TECH) and external environment (EE). This indicated that preparedness (P) accounted for much of the variance of the constructs investigated and had a strong correlation with many of the observed constructs. This finding suggested that preparedness played a more significant role in establishing a cybersecurity culture in E-Health institutions than the other constructs. The eigenvalue of 23.942%, which was much greater than one, shows that the factor of preparedness should be selected for further investigation.

Table 6.10: Factor Loading and TVE of Responsibility Construct

Factors	Questions	Rotated Component Matrix	Component Matrix	Total Variance Explained	Eigenvalue
Responsibility (R)	Q13_1	.556	5	17.047%	9.035%
	Q13_2	.402			
	Q13_3	.519			
	Q13_4	.646	6		
	Q13_5	.517			
	Q13_6	.486			
	Q13_7	.614	7		
	Q13_8	.604			
	Q13_10	.660			
	Q13_12	.602	8		
	Q13_13	.542			
	Q13_14	.720			
	Q13_15	.669	9		
	Q13_16	.424			
	Q13_17	.397			

Factors	Questions	Rotated Component Matrix	Component Matrix	Total Variance Explained	Eigenvalue
	Q13_19	.406			
Extraction Method: Principal Component Analysis a. 5 components extracted					

The items that measure responsibility (R) (see Table 6.10) were loaded on 5 components. Four items loaded on component 8, and three sets of items loaded on components 5, 6, 7 and 9. Values for TVE (17.047%) and eigenvalue (9.035%) were achieved for this construct. This eigenvalue indicated that the responsibility (R) factor should be included for further investigation.

Table 6.10 also shows that responsibility was the factor with the second-highest value of TVE. This is an indication that responsibility also has a strong influence on the establishment of cybersecurity culture in E-Health institutions.

Questions Q13_9, Q13_11, and Q13.18 were excluded because they were not supported when EFA was carried out, and hence they did not pass the validity and reliability test.

Table 6. 11: Factor Loading and TVE of Management Construct

Factors	Questions	Rotated Component Matrix	Component Matrix	Total Variance Explained	Eigenvalue
Management (M)	Q14_1	.616	10	7.350%	3.895%
	Q14_2	.701			
	Q14_3	.571			
	Q14_4	.410			
	Q14_5	.591			
	Q14_6	.368	11		
	Q14_7	.738			
	Q14_8	.667			
	Q14_9	.563			
	Q14_10	.487			
	Q14_11	.629			
	Q14_12	.731			
	Q14_13	.473			

Factors	Questions	Rotated Component Matrix	Component Matrix	Total Variance Explained	Eigenvalue
	Q14_14	.660	12		
	Q14_15	.651			
	Q14_16	.441			
Extraction Method: Principal Component Analysis					
a. 3 components extracted					

As shown in Table 6. 11Management (M) items were loaded on 3 components. Five sets of items (Q14_1 to Q14_5) loaded on components 10 and 11, and six items were loaded onto component 12.

The factor TVE values (7.350%) positioned Management (M) as the third most significant construct in terms of its correlation with the other constructs that were observed and with the development of cybersecurity culture. This eigenvalue was, however, significantly lower than the eigenvalue obtained for preparedness and responsibility.

However, the factor of Management (M) was still approved for further investigation because the eigenvalue was above the recommended threshold (≥ 1).

Table 6.12: Factor Loading and TVE of Technology and External Environment Constructs

Factors	Questions	Rotated Component Matrix	Component Matrix	Total Variance Explained	Eigenvalue
External Environment (EE)	Q15_1	.614	13	2.116%	1.122%
	Q15_2	.444			
	Q15_3	.443			
	Q15_4	.488			
Technology (Tech)	Q16_1	.633	14	1.955%	1.036%
	Q16_2	.475			
Extraction Method: Principal Component Analysis.					
a. 2 components extracted.					

Finally, Table 6.12 shows that items for technology (TECH) and external environment (EE) only loaded on 13 and 14 components. Four items were loaded on Component 13, and two items were loaded on Component 14, respectively.

The TVE results of 2.116 % and 1.955% in Table 6.12 confirm that technology and environment were the least important construct factors associated with cybersecurity culture. Cybersecurity culture is considered as the whole question, which comprises many items on a Likert scale. Although technology (TECH) and external environment (EE) are the factors that had the lowest Total Variance Explained, the eigenvalues, which were only marginally greater than the threshold value of 1, allowed the factors to be considered for further investigation.

Based on all the results depicted in Table 6.9 to Table 6.12, it is evidence that:

- All 53 items (representing the individual questions in the questionnaire) were grouped into 14 components using the component matrix because they all obtained a loading value greater than 0.3, which is the acceptable threshold (Pallant, 2020). This is an indication that all items of the questionnaire are being considered for further analysis and that no item was omitted.
- The eigenvalues, shown for all the factors (see Table 6.9 to Table 6.12) were greater than 1. This means that all the research constructs (preparedness (P), responsibility (R), Management (M), technology (TECH), and external environment (EE)) were selected and used for further investigations.
- Finally, the accumulated TVE value of 73.642% from the constructs preparedness (P), responsibility (R), Management (M), technology (TECH), and external environment (EE) indicates that it is possible to retain 73. 642% of the TVE information after the 53 components (that make up the 5 constructs) were grouped to create 14 components.

TVE and rotated component Matrix were steps 3 and 4 used to test the validity of the research instrument. For detailed TVE, see APPENDIX_3E

6.5.5.4 SCREE PLOT

A scree plot is a line plot of the eigenvalues of factors in an analysis (Pallant, 2020). The scree plot was used to determine the number of factors to retain in an exploratory factor analysis, to keep in a principal component analysis (Pallant, 2020).

A scree plot **Figure 6.3** shows the component numbers that are used in this research study as the x-axis and eigenvalues as the y-axis. Fourteen components were retained in this study, with an eigenvalue above 1 on the y-axis. These 14 components were associated with 5 constructs, namely management (M), responsibility (R), preparedness (P), technology (TECH), and external environment (EE), as shown in **Figure 6.3**.

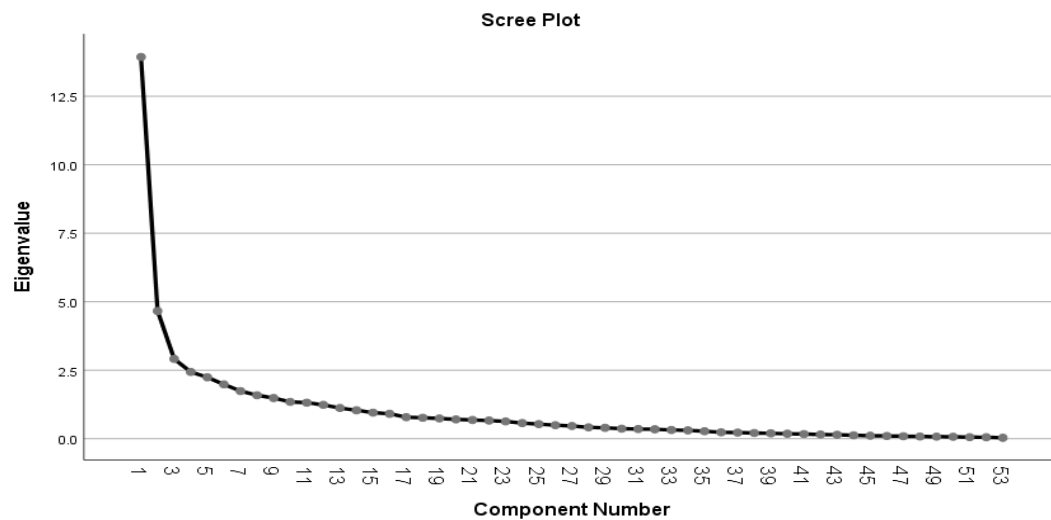


Figure 6.3: Scree Plot (own source generated from SPSS)

In summary, the study used a five-step EFA in to test the validity of the factors associated with cybersecurity culture in E-Health institutions. Based on the result of the analysis, factors related to cybersecurity culture in public E-Health institutions were identified, which contributed to answering Research Sub-Question 3.

Research Sub-Question 3 (RSQ 3):

“What factors are associated with cybersecurity culture in the public E-Health institutions in South Africa?”

Section 6.5.6 provides the results of the descriptive statistics.

6.5.6 DESCRIPTIVE ANALYSIS

The researcher used descriptive statistics to summarise and describe the main constructs identified for this study (see Table 6.13). The mean, minimum number of participants, maximum number of participants, and standard deviation were calculated per construct.

Pearson correlation was used to check for the strength and direction of the association between constructs, such as preparedness (P) and responsibility (R).

Table 6.13 presents the summarised descriptive statistics, including the mean and standard deviation for the research constructs studied. For detailed descriptive statistics of the individual items that measure the constructs, see APPENDIX_3F.

Table 6.13: Summarised Descriptive Statistics

Constructs	N	Minimum	Maximum	Mean	Std. Deviation
Preparedness (P)	99	1.00	4.13	2.4963	.78282
Responsibility (R)	99	1.56	4.06	2.7898	.44351
Management (M)	99	1.50	3.81	2.5739	.56845
External Environment (EE)	99	1.00	5.00	2.7374	.75628
Technology (TECH)	99	1.00	5.00	2.6667	.93405
cybersecurity culture	99	1.50	3.56	2.6221	.45953

Table 6.13 shows a consolidated mean and standard deviation for cybersecurity culture as well as for each of the constructs that measured it: preparedness represented by employee awareness and competency, including training and education; responsibility characterised by employee attitude and behaviour; management cybersecurity practices of the institution; the healthcare environment; and technology.

The constructs shown were interrogated using questions that were reliable and valid. This process, therefore, involved identifying and naming the concepts, and achieved the third phase of Step 1 according to the conceptual process.

In this study, the interpretation of the mean related to each of the Likert scale values is shown in Table 6.14. This helped avoid a biased interpretation of the descriptive statistics data.

Table 6.14: Likert Scale Mean Interpretation (Adapted from Pimental, 2010; 2019)

Likert Scale	Interval	Difference	Description
1	1.00 -1.79	0.79	Strongly disagree
2	1.80 to 2.59	0.79	Disagree
3	2.60 to 3.39	0.79	Neutral
4	3.40 to 4.19	0.79	Agree

Likert Scale	Interval	Difference	Description
5	4.20 to 5.00	0.80	Strongly agree

Based on Table 6.14, the mean point range of 1.00 to 1.79 shows strongly disagree, 1.80 to 2.59 represents disagree, 2.60 to 3.39 indicates neutral, 3.40 to 4.19 is agree, and 4.20 to 5.00 shows strongly agree (Pimentel, 2010, 2019). The approach was applied in this study because it has been in existence for many years (since 2010) (Pimentel, 2010) and continues to be relevant in research (Pimental, 2019). It has been used in recent studies (Abdelrady & Akram, 2022; Al-Maqbali & Al-Shamsi, 2023; Al-Maqbali & Hussain, 2022). The approach assisted the researcher in ensuring the data interpretation was unbiased (Pimentel, 2010, 2019).-

Sections 6.5.6.1 to 6.5.6.6 present the descriptive statistics of the research constructs.

6.5.6.1 DESCRIPTIVE STATISTICS FOR PREPAREDNESS (P)

The descriptive statistics for the cybersecurity preparedness (P) show that participants do not all agree that (either through the provision of information or training) they are competent and aware of all the cybersecurity items that were tested in this construct. ‘Disagree’ is depicted by a mean of 2.4963 (see Table 6.15). This shows that as a whole, participants disagreed with most of the items, but there was no general agreement amongst the participants as the Standard Deviation was high.

Table 6.15: Descriptive Statistics for Preparedness Construct

Construct	N	Minimum	Maximum	Mean	Std. Deviation
Preparedness (P)	99	1.00	4.13	2.4963	.78282

Looking at the individual items, participants disagreed that they were aware of the emerging cybersecurity threats that affect healthcare institutions, cybersecurity practices of their hospitals, actions to take with regard to cybersecurity incidents, or were trained on the importance of cybersecurity, cybersecurity skills, and abilities, as well as actions that are needed to protect the hospital computer systems from cyber-attacks.

For the remaining items, Q8_1, Q8_4, Q8_6, Q8_8, Q8_9, Q8_10, Q8_11, and Q8_13, the participants also did not agree that they were aware or competent about preparedness items that

these questions measured. However, there were some neutral or mixed answers regarding whether they:

- had been informed or trained on issues like the Protection of Personal Information Act (POPIA), and were aware of the financial and non-financial implications of their security practices (Q8_1, Q8_4);
- could confidently recognise cybersecurity incidents and/or security activities that could sustain or endanger the security of the hospital's critical resources (Q8_6);
- knew whether a computer device had experienced a virus or other security attacks (Q8_9); and
- knew what to do or who to contact when they received suspicious emails, or their computer was hacked (Q8_10, Q8_11).

6.5.6.2 DESCRIPTIVE STATISTICS FOR RESPONSIBILITY(R)

Responsibility in this study had a value of 2.7898, which is between the values of 2.60 and 3.39 as per the interval scale shown in Table 6.16. According to Pimental's (2010) interpretation, a mean of 2.7898 is an indication of 'neutral'. As a result, in this study, the researcher could conclude that the decision variable of responsibility as a whole was neutral.

The mean score of 2.7898 depicted for responsibility (R) in Table 6.16 shows that the participants were unsure or neutral regarding many of the statements concerning cybersecurity attitudes and behavioural items that were related to the responsibility construct. Therefore, overall, they neither agreed with nor disagreed with statements regarding attitude and behaviour and how these affect cybersecurity culture.

Table 6.16: Descriptive Statistics for Responsibility Construct

Construct	N	Minimum	Maximum	Mean	Std. Deviation
Responsibility (R)	99	1.56	4.06	2.7898	.44351

The participants were, for example, neutral on the following items:

- Adhering to security practices, policies, and measures of the hospital presented a challenge to their main business function (Q9_1).
- They were happy to conform to their hospital security practices and guidelines (Q9_2).

- Employee behaviours like carelessness, negligence, and personal intentions were the main challenges of cybersecurity in their hospital (Q9_6).
- Their colleague's behaviour towards security influenced the way they perceived security (Q9_13).
- The source of the email attachment was checked before opening it (Q9_16).
- They needed to lock their computer device when not in use (Q9_19).
- And lastly, that they used personal devices like USBs and phones to store and transfer information (Q9_17).

The participants indicated that they did not totally agree with statements about several other items related to the responsibility construct. For instance, the participants did not agree that:

- their hospital was well prepared to handle cyber threats because of the kind of attention they gave to security-related issues (Q9_4);
- there was a collaboration between departments and colleagues in creating awareness or solving cybersecurity issues (Q9_12);
- sharing of tips was a common practice among colleagues in attending to cybersecurity (Q9_8);
- some colleagues were outspoken with regard to cybersecurity, and that helped create awareness among others (Q9_14);
- a cybersecurity knowledgeable employee assisted other colleagues (Q9_15); and
- they reported colleagues or third parties that fail to follow security policies (Q9_10).

Participants indicated agreement with one security behaviour of the responsibility construct. No participants strongly disagreed or strongly agreed with any of the items of the construct.

6.5.6.3 DESCRIPTIVE STATISTICS FOR MANAGEMENT (M)

Management (referred to elsewhere as Internal Organisational Management (IOM)) obtained a mean value of 2.5739 (see Table 6.17) and since this is between the values 1.80 to 2.59 (see the interval scale of Table 6.14) the researcher can argue that the value for the decision variable for the Management (M) construct is negative. Hence, for Management (M), a mean score of 2.5739 indicated that participants mostly disagreed with the statements given in the items that tested the Management construct. This implies that participants did not agree that there was good Management (M) with respect to cybersecurity culture in the E-Health organisation where they worked.

Table 6.17: Descriptive Statistics for Management Construct

Construct	n	Minimum	Maximum	Mean	Std. Deviation
Management (M) was referred to as Internal Organisational Management (IOM) elsewhere	99	1.50	3.81	2.5739	.56845

However, participants disagreed with the statements made in several individual items of the constructs.

For example, they did not support the claims that:

- their hospital had a cybersecurity policy and a well-known cybersecurity department or team (Q14_1, Q14_2);
- the employees were punished for non-compliance with cybersecurity practices (Q14_5);
- campaigns were used to keep employees up to date with cybersecurity issues (Q14_7);
- employees' cybersecurity knowledge was tested through cyber-threat exercises (Q14_8);
- the hospital's top management participated in cybersecurity activities like attending cybersecurity-related discussions and meetings (Q14_9, Q14_10);
- security guidelines were made available to employees (Q14_12); and
- and the hospital's internal communication mediums were used to encourage cybersecurity activities among employees (Q14_11).

Participants neither agreed nor disagreed (they were neutral which could mean that they were unsure) that the computer devices or E-Health systems they used in the hospital were outdated. Similarly, they were neutral regarding whether employees were rewarded for their efforts in cybersecurity practices, their healthcare institutions used access control to restrict access to the working environments, employees were encouraged to act to protect the hospital assets by following the right channel to report weaknesses in computer devices, and their computer systems only accepted strong passwords.

6.5.6.4 DESCRIPTIVE STATISTICS FOR HEALTH ENVIRONMENT (HE)

The environment (also referred to as External Environment and Non-Organisational Management (EENOM) in this study) scored a mean value of 2.7374 (see Table 6.18). This is

between 2.60 and 3.39, as per the interval scale in Table 6.14. Hence, based on Pimental's (2010) interpretation of the mean, the researcher concludes that the decision characteristics of the environment (HE) are neutral with respect to this construct.

A mean score was a general indication that participants were neutral on the items related to the environment (HE) construct.

Table 6.18: Descriptive Statistics for Environment Construct

Construct	N	Minimum	Maximum	Mean	Std. Deviation
External Environment (HE) also referred to elsewhere as External Environment and Non-Organisational Management (EENOM)	99	1.00	5.00	2.7374	.75628

A neutral mean was obtained for the following items: that the way that the institution and its society see cybersecurity has an impact on employee behaviour, that their hospital does not pay sufficient attention to cybersecurity issues because it is are small and not located in a busy cities, and finally that the frequency with which government policies on the use of technology in healthcare change is a challenge.

Some disagreements were also indicated. For example, participants disagreed that healthcare practitioners have many professional and government regulations to adhere to.

6.5.6.5 DESCRIPTIVE STATISTICS FOR TECHNOLOGY (TECH)

Technology in this study had a mean value of 2.6667 (see Table 6.19). Pimental's (2010) interpretation sees a mean of 2.6 as neutral (see Table 6.14). Hence, overall, participants were neutral regarding the items related to the Technology (Tech) construct.

Table 6.19: Descriptive Statistics for Technology Construct

Construct	N	Minimum	Maximum	Mean	Std. Deviation
Technology (TECH)	99	1.00	5.00	2.6667	.93405

For example, participants neither agreed nor disagreed with the claim that the emergence of new cyber threats made it difficult for them to keep up with cybersecurity threats.

6.5.6.6 DESCRIPTIVE STATISTICS FOR CYBERSECURITY CULTURE

As the mean value of cybersecurity culture was 2.6221 (see Table 6.20), and hence was in the range between 2.60 and 3.39, according to Pimental (2010) it was neutral (see Table 6.14). Hence, the researcher concluded that the combined responses to the research items of cybersecurity culture were neutral (recall that cybersecurity culture is considered the entire set of items with options on the Likert Scale).

Table 6.20: Descriptive Statistics for Cybersecurity Culture Construct

Construct	N	Minimum	Maximum	Mean	Std. Deviation
Cybersecurity Culture	99	1.50	3.56	2.6221	.45953

In summary, the descriptive statistics provided an overview of the responses from the participants regarding the factors influencing cybersecurity culture in public E-Health institutions. Across the constructs, preparedness (P) recorded the highest mean scores, suggesting that staff readiness, awareness, and proactive security measures were considered to be critical in shaping cybersecurity culture, directly addressing RSQ 3 and SRO 3. Responsibility (R) also showed relatively high scores, indicating that accountability, adherence to policies, and individual roles were considered to play a significant role in establishing a secure environment.

Management (M) received moderate scores, reflecting that leadership commitment, strategic planning, and resource allocation were considered to influence the effectiveness of cybersecurity culture, while technology (TECH) and external environment (EE) obtained lower mean scores, implying that although essential, these factors were considered to be less impactful on cultural adoption compared to human and organisational dimensions. Overall, these patterns highlight the importance of focusing on preparedness and responsibility when developing a contextual framework for cybersecurity culture, linking directly to RSQ 5 and SRO 5, while also informing the identification of constructs that can be adapted from existing frameworks (RSQ 4 and SRO 4) for enhancing public E-Health institutions' cybersecurity practices.

6.5.7 PEARSON CORRELATION COEFFICIENT ANALYSIS

Pearson correlation was used to measure the relationship between research variables to determine the strength, nature, and, most importantly, the significance of the association between the research variables (Chalil, 2020).

The strength of a relation is depicted as large if it has a Pearson Correlation value (r) above 0.5, moderate if it is between 0.3 and 0.49, small if between 0.1 to 0.29, and weak if below 0.1. A relationship can be positive or negative. Lastly, a relationship is a significant correlation only if it has a p-value less than 0.05 (sig).

This chapter aimed to identify the factors associated with cybersecurity culture in E-Health institutions through quantitative analysis. Therefore, identifying and naming the significant concepts (constructs) after the Pearson correlation was carried out, also identified the factors associated with cybersecurity culture. Achieving this answered **Research Sub-Question 3 (RSQ 3):** “*What factors are associated with cybersecurity culture in public E-Health institutions in South Africa?*”

Therefore, a Pearson correlation coefficient test was conducted to assess the magnitude, nature, and significant relationship that existed between the variables preparedness (P), responsibility (R), management (M), technology (TECH), and external environment (EE). And between each of those variables and cybersecurity.

Table 6.21 shows the result of the Pearson correlation analysis.

Table 6.21: Pearson Correlation Analysis

		P	R	M	EE	TECH	Cybersecurity Culture
Preparedness (P)	Pearson Correlation	1					
	Sig. (2-tailed)						
	N	99					
Responsibility (R)	Pearson Correlation	.563**	1				
	Sig. (2-tailed)	.000					
	N	99	99				
Management (M)	Pearson Correlation	.570**	.574**	1			

		P	R	M	EE	TECH	Cybersecurity Culture
	Sig. (2-tailed)	.000	.000				
	N	99	99	99			
external environment (EE)	Pearson Correlation	.009	.150	.012	1		
	Sig. (2-tailed)	.332	.019	.339			
	N	99	99	99	99		
Technology (TECH)	Pearson Correlation	.039	.208*	.034	.742**	1	
	Sig. (2-tailed)	.698	.016	.505	.000		
	N	99	99	99	99	99	
cybersecurity culture	Pearson Correlation	.850**	.815**	.817**	.242**	.253*	1
	Sig. (2-tailed)	.000	.000	.000	.004	.046	
	N	99	99	99	99	99	99
** . Correlation is significant at the 0.01 level Sig (2-tailed). * . Correlation is significant at the 0.05 level Sig (2-tailed). ** . N = the number of participants							

The correlation observations on the relationships between pairs of variables (see Table 6.21) are discussed below.

Preparedness (P) and responsibility (R): The Pearson correlation of preparedness (P) and responsibility (R) was found to be large and positive ($r = 0.563$), and the relationship was statistically significant ($p\text{-value} < 0.000$). This shows that the more preparations the hospitals made to attend to cybersecurity issues (by providing staff members with cybersecurity awareness, education and training, and equipping them with the necessary skills), the more positive the employees' attitudes and behaviour toward cybersecurity would be.

Preparedness (P) and Management (M): The Pearson correlation for these two constructs was also found to be large and positive ($r = 0.570$) and statistically significant ($p\text{-value} < 0.000$). Hence, the finding shows that the more prepared healthcare institutions are (they provide awareness, education and training, and necessary cybersecurity skills to employees), the more the actions of the institutions' management would reflect their support of established cybersecurity practices. The management actions include having a cybersecurity policy, a visible (well-known) cybersecurity department or team, cybersecurity reward and punishment strategies, and other forms of management support and engagement for cybersecurity-related activities. Stating it differently, the relationship shows that a healthcare institution with well-established cybersecurity practices and management is likely to be more prepared in terms of providing cybersecurity training, education, and awareness.

Preparedness (P) and External Environment (EE): No Pearson correlation was found to exist between preparedness and external environment ($r = 0.009$). The relationship was also statistically insignificant with a $p\text{-value}$ greater than 0.05. This, therefore, indicates that in these healthcare institutions, external environment issues did not have a noticeable effect on how the institutions prepared their employees with cybersecurity-related training and education.

Preparedness (P) and Technology (TECH): There was no significant Pearson correlation between preparedness and technology ($r = 0.039$), and the association was statistically insignificant ($p\text{-value} > 0.05$). This indicated that technology was not considered an issue with regard to preparing employees for cybersecurity.

Responsibility (R) and Management (M): Table 6.21 shows a large positive relationship between these two variables with a Pearson correlation value of $r = 0.574$, and this was statistically significant ($p\text{-value} < 0.05$). Hence, an increase in management action in terms of cybersecurity practices would lead to a change in employees' attitudes and behaviour as these relate to cybersecurity activities. Management actions that are seen as being positive would cause employees to become more responsible. For example, increased management engagement and support and the introduction of a cybersecurity team could be expected to make the attitudes and behaviour of employees more positive regarding cybersecurity activities.

Responsibility (R) and External Environment (EE): The Pearson correlation between these variables was found to be positive but small ($r = 0.150$). Nevertheless, the correlation was found to be significant ($p\text{-value} < 0.05$). This relationship shows that, with an increase in the

healthcare external environment factors, there could be a corresponding change in attitudes and behaviours of the employees toward cybersecurity. Since r has a positive value, environmental factors considered to be positive would cause positive changes in attitudes and behaviours, and similarly, environmental factors judged as negative would cause negative attitudes and behaviours.

Responsibility (R) and Technology (TECH): The Pearson correlation between these variables indicates that there is a positive but weak relationship ($r = 0.208$). Nevertheless, the association was significant ($p\text{-value} < 0.05$). This demonstrates that an increase (positive) in technological factors could lead to an increase in the positive attitudes and behaviours of the employee toward cybersecurity.

Management (M) and External Environment (EE): The result in Table 6.21 show that no correlation existed between these two variables ($r = 0.012$), and the relationship was insignificant ($p\text{-value} > 0.05$). Hence, an increase in the healthcare external environment issues would not be the cause of an increase in M within the hospital.

External Environment (EE) and Technology (TECH): The result in Table 6.21 revealed a large positive Pearson correlation ($r = 0.742$), and the association was statistically significant ($p\text{-value} < 0.05$). This indicates that an increase in technological issues would lead to an increase in matters related to the external environment within the hospital.

Cybersecurity culture and all the constructs (preparedness, responsibility, management, external environment, and technology): The Pearson correlations of all these pairs of constructs were found to be positive, but the size of the correlation varied, either being large, moderate or weak. Their relationships were all statistically significant.

Preparedness (P) and Cybersecurity Culture had a large positive Pearson correlation ($r = 0.850$), which shows that the more prepared the hospitals are to increase cybersecurity awareness, education, training, and equipping staff with the necessary skills, the better the culture of cybersecurity in the institution would be.

Management (M) and Cybersecurity Culture also had a large positive Pearson correlation ($r = 0.817$). The implication is that the more positive actions of management of the institutions undertaken in terms of cybersecurity practices, like having a cybersecurity policy or a well-known cybersecurity department or team, the greater the likelihood would be that there would be improvements to the cybersecurity culture.

Responsibility (R) and Cybersecurity Culture showed a large positive Pearson correlation. This suggests that the cybersecurity culture of the institution would be increased if the cybersecurity behaviour and attitudes of employees improved.

External Environment (EE) and Cybersecurity Culture, and Technology and Cybersecurity Culture show small positive Pearson correlation values ($r = 0.242$ and $r = 0.253$, respectively). The results suggest that an increase in environmental or technological factors could lead to a positive security culture.

Based on the observations discussed above, there were only positive correlations between the variables, and they were mostly significant. These showed that meaningful correlations existed between the variables discussed, except in the cases of P and EE, P and TECH, M and EE, and M and TECH, which show no correlation, and the relationships were found to be insignificant.

All constructs that measured relationships between cybersecurity culture and another construct had positive correlation, and were found to be statistically significant, indicating that good correlations existed between the constructs and cybersecurity culture. One can, therefore, conclude that these relationships were important when it came to cybersecurity culture. As such, factors related to the research constructs like awareness, competency, attitude, behaviours, cybersecurity practices, environment, and technology were also examples of the factors associated with cybersecurity culture in public E-Health institutions.

The summary of the Pearson correlation results is shown in Table 6.22 and **Figure 6.4**. The relationship between constructs depicted in Table 6.22 is described as either ‘supported’ or ‘not supported’. Cybersecurity culture has a relationship with P, R, M, EE, and TECH.

Table 6.22: Constructs Correlation Decisions

Correlation	Decision
P and R	Supported
P and M	Supported
P and EE	Not Supported
P and TECH	Not Supported
P and Cybersecurity Culture	Supported
R and M	Supported
R and EE	Supported
R and TECH	Supported

R and Cybersecurity Culture	Supported
M and EE	Not Supported
M and TECH	Not Supported
M and Cybersecurity Culture	Supported
EE and TECH	Supported
EE and Cybersecurity Culture	Supported
TECH and Cybersecurity Culture	Supported

Based on the information presented under **Section 6.10** and Table 6.22, **Figure 6.4** depicts the quantitative analysis model.

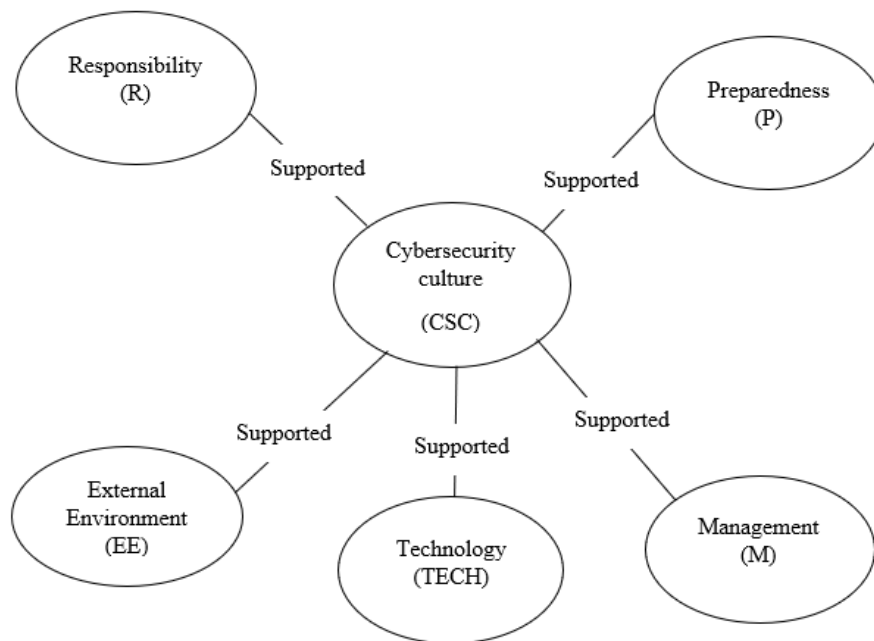


Figure 6.4: Quantitative Analysis Model (own source)

Figure 6.4 shows that the constructs, namely preparedness (P), responsibility (R), management (M), technology (TECH), and external environment (EE), all had associations with cybersecurity culture according to the input from system users at the surveyed hospitals in Mpumalanga, South Africa.

6.6 CONCLUSION OF THE QUANTITATIVE ANALYSIS

This chapter reported on findings from the quantitative data collected from the research surveys. The demographics of the respondents, including age and gender, were reported in this

chapter. The study used Cronbach's alpha and EFA to assess the reliability of the data and hence to validate the study instrument.

Descriptive statistics used to summarise the research constructs showed that responses from the research respondents to the statements regarding preparedness and management decision variables were largely negative, while in the case of the remaining constructs, the data indicated that responses were neutral. To provide answers to the research issues posed by this study, construct correlation was performed using Pearson correlation coefficients analysis. The findings revealed a positive association and high significance between the research variables. However, correlations between A&C and EE, A&C and EE, A&C and TECH, M and EE, and M and TECH were not significant.

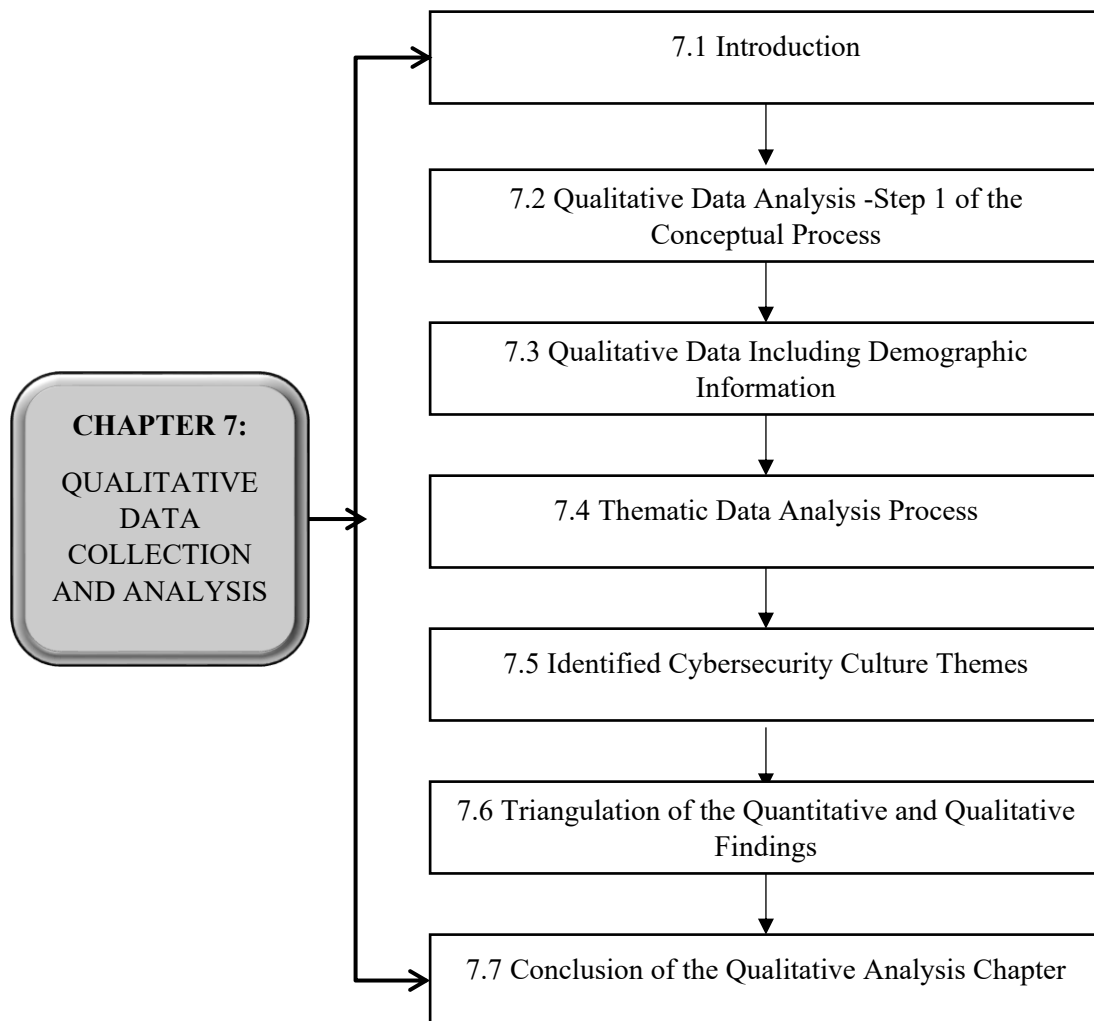
From the analysis of the quantitative data collected using questionnaires, it is evident that issues related to awareness and competency (within the preparedness construct) played a major role in cybersecurity culture in public E-Health institutions.

Important points that came out strongly regarding the management cybersecurity practices were that no cybersecurity department, team, or section exists in the health institutions to handle cyber-related issues, and little to no support and participation exists on the part of top management regarding cyber issues. What was also concerning from the responses was the participants' lack of knowledge of their hospital's cybersecurity policies and guidelines.

Participants indicated that their hospitals were not prepared to handle cybersecurity because they perceived that little attention was given to cybersecurity issues; therefore, the number of actions should be increased or be brought more strongly to the attention of end users for these hospitals to be considered to be organisations that take cybersecurity seriously.

The analysis revealed issues regarding a lack of collaboration, assistance and interaction between healthcare workers and between different departments, resulting in barriers to sharing knowledge and tips on cyber threats and cybersecurity issues. The next chapter will present the qualitative part of data analysis.

CHAPTER 7: QUALITATIVE DATA COLLECTION AND ANALYSIS



7.1 INTRODUCTION

Chapter 7 describes the processes undertaken for qualitative data collection and analysis, and the findings. These findings were subsequently used to triangulate the qualitative data with the quantitative data (discussed in Chapter 6) and the results from the systematic review (presented in Chapter 5). Chapter 7 aims to identify, from the perspective of ICT staff, the factors associated with cybersecurity culture in public E-Health institutions.

The findings of this chapter are combined with the outcome of the findings presented in Chapter 6 to answer the **Research Sub-Question 3 (RSQ 3)**: “*What factors are associated with cybersecurity culture in public E-Health institutions in South Africa?*”

This qualitative data analysis starts in **Section 7.2** by presenting the conceptual framework analysis phases that were followed. **Section 7.3** explains the qualitative data collection process and the associated demographic information. **Section 7.4** presents the thematic data analysis used for the qualitative analysis. **Section 7.5** highlights the cybersecurity culture themes that were identified. **Section 7.6** discussed the triangulation of the qualitative and quantitative findings, and a model is formulated as a thematic diagram. The chapter ends with a conclusion in **Section 7.7**.

7.2 QUALITATIVE DATA ANALYSIS: STEP 1 OF CONCEPTUAL PROCESS

Chapter 5 described the eight phases of the conceptual framework analysis process adopted in this study to develop a contextual framework of cybersecurity culture. The phases of the framework were grouped into three steps. Step 1 consists of the first five phases; some elements of Phases 1 to 3 were discussed in Chapters 4 and 6. Chapter 7 continued the discussion of elements from Phases 1 to 3 as well as some aspects of Phase 4. **Figure 7.1** shows Step 1 of the framework extracted from **Figure 5.8** in Chapter 5. The quantitative and qualitative data collection and analysis in Chapters 6 and 7, together with Chapter 4, contribute towards achieving the main research objective in Chapter 8. Chapters 6 and 7, together with Chapter 4, achieve Step 1 in designing and developing the contextual framework as the main contribution of this research study.

The main research objective was *to develop a Contextual Cybersecurity Culture Framework (CCSCF) for public E-Health institutions in South Africa*.

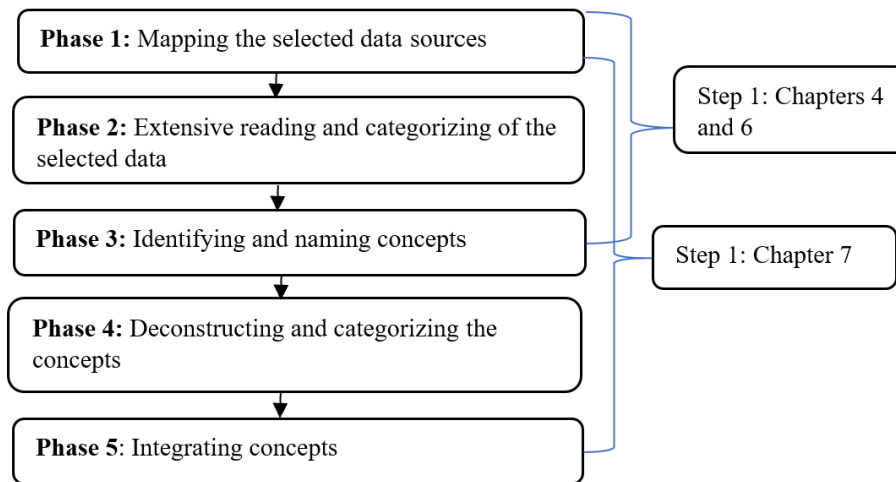


Figure 7.1: Phases 1-5 of the Conceptual Framework Analysis Process (Adapted from Jabareen, 2009)

The analysis in this chapter of qualitative data for the identification of cybersecurity culture factors from the perspective of ICT staff is the third strategy followed to accomplish Step 1 (Phases 1 to 5) of the conceptual framework analysis process (see Table 7.1). Phases 1 to 5 of Step 1 were discussed in **Sections 7.3 to 7.6** but, depending on the section, some phases received more attention than others. For example, Phase 1 is mainly covered in Section 7.3, while Phases 2, 3 and 4 are mainly covered in **Sections 7.4, 7.5 and 7.6**. Phase 5 is only covered in **Section 7.6**.

7.3 QUALITATIVE DATA INCLUDING DEMOGRAPHIC INFORMATION

This study collected quantitative data from system users in public E-Health institutions and focused on qualitative aspects based on data obtained by interviewing ICT staff, including ICT management. Hence, a mixed-method approach was used (see Chapter 5). As noted in Chapter 6, the data analysis is presented in two parts. Part 1, the presentation of the quantitative analysis was presented in Chapter 6. This section (**Section 7.3**) presents Part 2, namely qualitative data collection and analysis. These two data collection methods were followed to allow the researcher to build a diverse and comprehensive view of factors associated with cybersecurity culture in E-Health institutions. The mixed method approach also helped to ensure the validity and reliability of the findings, and in particular of the factors identified.

The qualitative data collection used the same location, Mpumalanga province, as the source of data as for the case study described in Part 1. However, the researcher realised during the qualitative data collection that the major ICT function was centralised at the provincial level in

Mpumalanga. This means that no ICT department was located at any of the provincial hospitals (other than limited technical support, which was located at the district level). The ICT department was made up of the following sections: support, system, server, governance (this section was dormant), and client service.

Figure 7.2 depicts the steps of the qualitative part applied in this study, and these are discussed in the subsequent sub-sections.

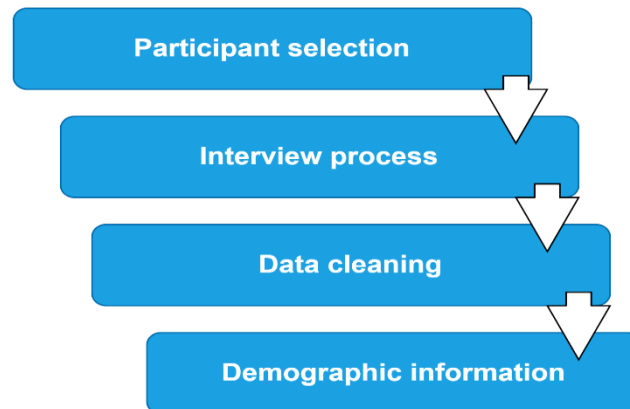


Figure 7.2: Qualitative Analysis Process (own source)

Figure 7.2 illustrates the process followed for the data collection in the first phase of developing the framework and how the collected data was categorised in the second phase during the analysis and reading.

7.3.1 PARTICIPANT SELECTION

Only eleven potential interviewees were approached because the study case was small. Firstly, the case focused on a single province (Mpumalanga), and secondly, the ICT department that maintained all the hospitals and clinics in the province was small and had a limited number of personnel. Further participants were not approached after the initial nine interviews because the researcher decided that the saturation point had been reached. Stopping interviews once the saturation point is reached is the norm for a qualitative study (Morse, 1995; Saunders et al., 2018). Additionally, nine is within the recommended number of interviews (Krueger, 2015; Langford et al., 2002).

The participants were all experienced and had a good understanding of ICT-related issues; hence they were able to provide rich data that would assist in achieving the research objective.

Table 7.1 gives an overview of the participants selected to be interviewed. The nine available participants were from different ICT sections and operated at various levels of the healthcare department. The ICT managers operated both at the provincial and district levels.

Table 7.1: Interview Participant's Details

Number of interviewees	ICT Role	Operation Level
2	Managers	Both provincial and district levels
4	Support	District level
3	Systems and server administrator	Provincial level

7.3.2 INTERVIEW PROCESS

This section describes the process followed in selecting the participants and collecting the qualitative data. The interview processes are explained in the following steps:

7.3.2.1 Step 1 Initial Communication with the Participants

The researcher visited the Mpumalanga province to become familiar with the environment. Before interviews commenced, the chief executive officers (CEOs) of the two hospitals being studied were contacted telephonically, and the CEOs referred the researcher to the ICT managers responsible for those hospitals. The ICT managers, in turn, helped to establish telephonic communication with eleven potential interviewees, as indicated in the previous sub-section.

Only nine participants were available, and all of those who volunteered to participate were selected. Interviewing these participants helped the researcher obtain enough rich information from the viewpoint of ICT staff regarding the culture of cybersecurity in the public E-Health institutions being studied. Data saturation was reached by interviewing the nine participants.

7.3.2.2 Step 2 Scheduling Interviews

The participants' volunteering served as their initial consent to participate in the interview. Once this was confirmed, interview dates were established, and online meetings were scheduled and accepted. The interview was conducted electronically via the Microsoft Teams

platform because the ICT staff (particularly the support staff) worked in more than one location, serving hospitals and clinics in their district to support and maintain their ICT systems.

7.3.2.3 Step 3 Obtain Each Participant's Full Consent in the Meeting

Before the interview started, the interviewee was provided with a description of the purpose of the study, including how the interview would be managed. Participants were also informed that participation was voluntary and that they had the right to withdraw at any time. These arrangements were communicated to help them make properly informed consent decisions.

7.3.2.4 Step 4 Data Recording and Transcription

Permission was obtained to record the interviews for analysis purposes, and the documents giving official permission and ethical approval to conduct the interview were shown to the participants. To enable satisfactory transcription of the recording for the second and third phases of the framework, the Microsoft Teams transcription feature was activated during the interview meeting.

Each interview took approximately 60 minutes. It consisted of three sections. Section A covered research ethics as described above, and Section B was used to gather the participants' biographical information as well as their ICT background. Section C contained questions regarding the current state of cybersecurity culture, practices and the institution's cybersecurity from the perspectives of ICT staff. APPENDIX_4A of this chapter shows the qualitative interview questions.

7.3.3 DATA CLEANING

After the interview, transcriptions of the recordings, together with the recordings, were downloaded. The recordings were listened to repeatedly by the researcher to check on the correctness of the transcribed data for effective data reading (second phase) and identification of cybersecurity culture factors (third phase). To ensure confidentiality, the participants' names were replaced with codes.

The transcriptions were cleaned by removing unnecessary words and repetitions manually using Microsoft (MS) Word. Unnecessary words in this context refer to filler words like 'Umm,' 'Uh,' and 'Hmm.'

7.3.4 DEMOGRAPHIC INFORMATION

Table 7.2 summarises the demographic information of ICT staff who participated in the interviews. Most of the respondents had extensive experience working as ICT staff in hospitals. They all had relevant ICT-related qualifications (related to ICT support, systems, server administrator or ICT manager), which confirmed that they were appropriate interviewees who could provide rich data about the cybersecurity culture of the institutions.

The majority of the respondents were between 20 and 40 years. Three were in the 41 to 60 age group, and only one participant was above 60 years. The interviewees were ICT staff who support and maintain ICT in the same hospitals (Witbank and Carolina) used for the quantitative data collection. Maintaining a similar context was appropriate as it had the advantage of a consistent setting being used for the two data sets.

Table 7.2: Demographic Information

Experience in the Hospital	Frequency	Percentage (%)
0-10 years	4	44,44
11-20 years	4	44,44
Above 20 years	1	11,11
Total	9	100
Age	Frequency	Percentage (%)
20 - 40 years	5	55,56
41 - 60 years	3	33,33
Above 60 years	1	11,11
Total	9	100
Education Qualification	Frequency	Percentage (%)
National Diploma	8	88,89
Undergraduate degree	1	11,11
Total	9	100
ICT Job Title	Frequency	Percentage (%)
Support	4	44,44
Systems and server administrator	3	33,33
Manager	2	22,22
Total	9	100

District of the Hospital	Frequency	Percentage (%)
Nkangala	2	22,22
Gert Sibande	7	77,78
Total	9	100

7.4 THEMATIC DATA ANALYSIS PROCESS

As discussed in Chapter 4, thematic data analysis is a commonly used qualitative analysis technique that examines data to identify recurring patterns and analyse meaning (Attride-Stirling, 2001; Braun & Clarke, 2006; Cruzes & Dybå, 2011; Thomas & Harden, 2008). The major benefits of this form of analysis are theoretical freedom and flexibility; hence, it is a valuable tool used for interpreting rich and detailed data (Braun & Clarke, 2006).

The main objective of using thematic analysis was to gain substantial insights from the cybersecurity culture data. Thematic analysis also helped the researcher to develop a genuine and comprehensive understanding of the factors associated with the research topic. Analysing the qualitative data using the thematic method achieved the second phase of the conceptual framework process, which can only be done by carefully studying the transcribed data.

Various thematic analysis approaches exist (Attride-Stirling, 2001; Braun & Clarke, 2006; Cruzes & Dybå, 2011; Thomas & Harden, 2008). However, the thematic approach to qualitative analysis of Braun and Clark (2006) was adopted as the primary method in this study. Its flexibility supports the pragmatic research philosophy embraced as the foundation of this study. Also, where necessary, influences were drawn from other thematic approaches.

Figure 5.12 is shown again here as **Figure 7.3** and depicts the thematic analysis stages followed for the qualitative analysis.

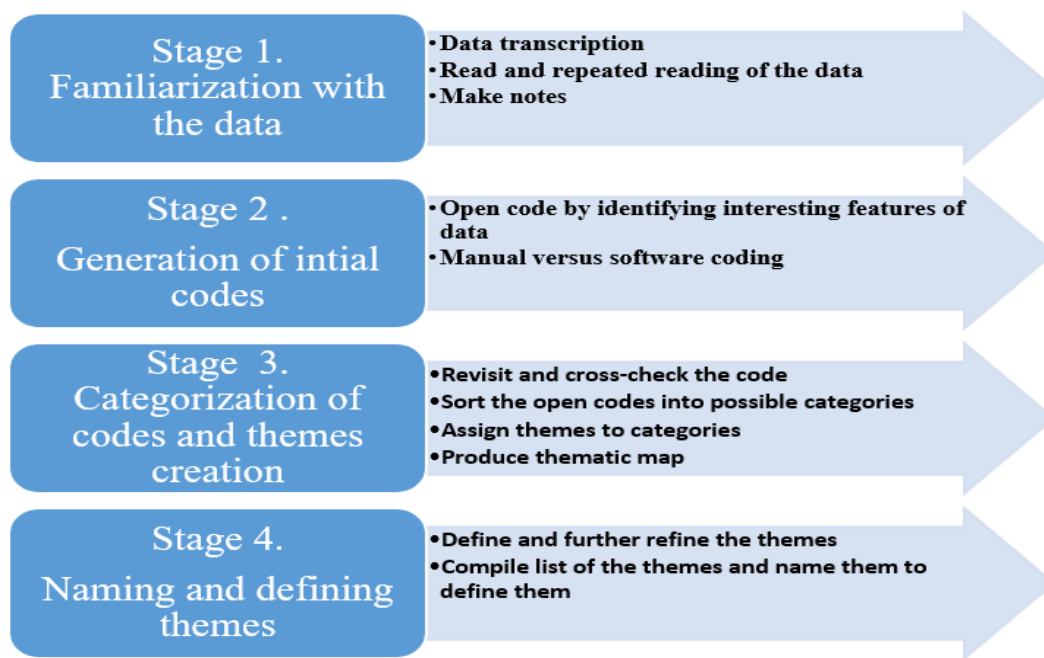


Figure 7.3: Stages of Qualitative Analysis (Adapted from Braun & Clarke, 2006)

Subsections 7.4.1 to 7.4.4 show the processes followed in reading through the data and analysing, explain the stages more fully, and show how they were applied in this study. This was achieved during the second phase of the conceptual framework. Thematically analysing the data also initiated the third phase, which identified and named themes (see Table 7.3 and Table 7.4).

7.4.1 STAGE 1: FAMILIARISATION WITH THE DATA

If the researcher is working with a verbal file obtained in an interview, the first essential task is transcribing the spoken words into written text (Bird, 2005; Braun & Clarke, 2006).

As indicated in Step 2 of the interview process, Microsoft Teams was used to conduct the interview, and the software can produce a transcription of the audio data. The researcher downloaded the transcribed data into MS Word and went through the data repeatedly, together with the audio recording. This was to ensure that the transcribed data accurately represented what was said in the interview, and that it faithfully reproduced the original information.

Stage 1 of qualitative analysis entailed the researcher immersing herself in the data to be thoroughly familiar with the aspects and nuances of the data.

Conducting the interview as an interactive exchange or conversation with the interviewee, and performing the transcription process personally, provided the researcher with knowledge of the

data early, at the initial stage of analysis and before the actual reading started. The researcher read through the data repeatedly to thoroughly understand all aspects and to deliberately uncover meanings and patterns in the data.

While actively reading through the data, important ideas, meanings, and patterns that appeared in the data were highlighted using MS Word, and comments were included to facilitate informed coding during Stage 2.

7.4.2 STAGE 2: GENERATION OF INITIAL CODES

Stage 2 of thematic data analysis begins once the researcher has actively (by adding comments and highlights) read and understood the data. In stage 2, initial codes or labels were created that drew attention to the meaning of the data and patterns observed in Stage 1 (Braun & Clarke, 2006). Codes were the most basic data element that could be evaluated meaningfully to create a better understanding of the phenomenon (Boyatzis, 1998). They were used to identify a set of data characteristics, data chunks, segments, or groups that were found to be interesting and meaningful (Boyatzis, 1998). Codes point out interesting concepts that have been identified systematically across the data set (Cruzes & Dybå, 2011).

ATLAS.ti version 9 was used for the qualitative data analysis in this study. After the researcher had familiarised herself with the raw data, the files were imported into ATLAS.ti version 9 for coding and categorisation of codes into themes.

There are various coding methods; however, in this research, open coding was used because it allowed the researcher the flexibility to code freely, as a deep and comprehensive understanding of the data was developed related to the topic, cybersecurity culture. The advantage of flexibility in open coding was compatible with the flexibility of both the inductive research approach and pragmatism.

Open coding is the least prescribed approach for qualitative research and was particularly suitable in this case, as it follows an inductive approach when examining data (Glaser, 2016; Holton, 2010; Khandkar, 2009). With open coding, at the initial stage, the researcher approaches the qualitative data with an open mind, and with few or no predetermined assumptions, so as to reveal the intended meaning, thoughts and concepts in the data (Glaser, 2016; Holton, 2010; Khandkar, 2009; Roehl, n.d.). Hence, open coding offers an unbiased way of coding freely to identify themes and other essential concepts from the data.

In Stage 2, the researcher read through the transcribed data using ATLAS.ti and created open codes semantically in a data-driven way. Thus, the researcher coded the data by merely observing the surface meanings communicated by the ICT staff. The code names assigned represented a superficial (initial) understanding of respondents' statements of the data chunk. The data was not approached with a predefined set of codes.

One hundred and two open codes were generated during the initial coding (see APPENDIX_4B). These were initial codes and were therefore prone to change; they could be deleted or merged with other codes in the following two stages as part of code categorisation and theme creation, as well as naming and defining codes.

7.4.3 STAGE 3: CATEGORISATION OF CODES AND THEME CREATION

After patterns and chunks of data had been identified and coded, Stage 3 categorised the codes and created themes (see Table 7.3). Stage 3 is described as a translation step where codes are converted into themes and sub-themes (Cruzes & Dybå, 2011).

The researcher revisited and analysed the 102 codes identified in Stage 2, and the following changes were made:

1. Codes with similar names but the same meaning were combined.
2. Some code names were changed to reflect the data they represented more clearly.
3. Codes whose data extracts were not meaningful or did not contribute greatly to finding themes associated with cybersecurity culture in E-Health institutions, were discarded.

Although this stage revisited and analysed the code list developed in the previous stages, the focus was on theme creation and refinement.

The final set of codes was sorted into categories to be considered as potential themes. The categorisation of themes in this stage happened predominantly using pre-existing terms in literature. For example, terms commonly used to represent the factors of cybersecurity culture are cybersecurity awareness, training, and education. This confirms the saying that the researcher and their theoretical commitments cannot operate in a vacuum (Braun & Clarke, 2006). Where pre-existing themes did not exist, and groups of codes could not be categorised for code generation, the original code names were maintained.

A total of 24 candidate themes emerged based on the categorisation of codes in this stage. The summary of the initial candidate themes with their original codes was depicted using the

models in APPENDIX_4C. The identified candidate themes were reviewed for accuracy as per the transcribed data and to refine the themes. The candidate themes were cross-checked, and it became clear that some candidate themes should be discarded either because there was insufficient coded data to back the themes or because two themes could be merged.

The themes were first compared with the identified codes and the data extracts to ensure a coherent pattern. Then they were checked against the data as a whole. Where necessary, new codes were generated, codes were moved between themes and unnecessary codes were deleted. Based on the review and refinement of themes, the initial 24 candidate themes were reduced to 22. Table 7.3 depicts the 22 themes identified by the end of Stage 3.

Table 7.3: The 22 Themes Identified from Stage 3

The Final 22 Themes of Stage 3	
training and education	risk assessment
communication and information sharing	centralisation
change of old practice	organisational learning
knowledge	business continuity
cybersecurity awareness	security governance
attitude	communication channels
compliance and monitoring	discipline
security behaviour	interest in cybersecurity
defence and protective mechanism	cybersecurity policy
priority on medical tasks	physical security
leadership	rules and regulation

7.4.4 STAGE 4: NAMING AND DEFINING THEMES

In Stage 4, the thematic tables or diagrams from the preceding phase were reviewed and refined further to finalise the themes that would be used for the last analysis. The essence of this stage was to identify the core themes and decide what the theme captures (Braun & Clarke, 2006). This was similar to Cruzes and Dybå's (2011) fourth thematic step, which recommended generating a model of high-order themes by exploring the relationships between the themes.

After final refinement, the themes were compiled into a list, and appropriate names were assigned to them. For consistency across the study, the qualitative part of the research used the five main constructs that the quantitative analysis was based on as the high-order theme names.

Hence, these were used to define and categorise the 22 themes. The constructs were preparedness (P), responsibility (R), internal organisation management (IOM), referred to as Management (M) in Chapters 6 and 7, technology (TECH), and external environment and non-organisational management (EENOM), referred to as external environment (EE) in this chapter. The constructs that influenced the naming of the themes emerged from the literature (Alhogail et al., 2015; Bakry, 2003; Da Veiga, 2019; Georgiadou et al., 2020b; Huang & Pearson, 2019).

At this stage, the 22 themes identified in Stage 3 were grouped, and theme names (that is, the high-order themes) were assigned to them. Assigning high-order theme names meant the 22 themes would thereafter be considered sub-themes under the high-order themes.

The five essential high-order themes used to group the 22 sub-themes were preparedness (P), responsibility (R), internal organisation management (IOM), referred to as Management (M) in Chapter 6, and external environmental and non-organisation management (EENOM). EENOM is referred to as the external environment (EE) in Chapter 6. The fifth theme, technology (TECH), had no sub-theme categorised under it, but three codes were grouped under it. Essentially, this stage could be called theme categorisation.

7.4.4.1 Theme Category 1: Preparedness (P)

Figure 7.4 shows the summary of ATLAS.ti model of the preparedness (P) construct with its sub-themes.

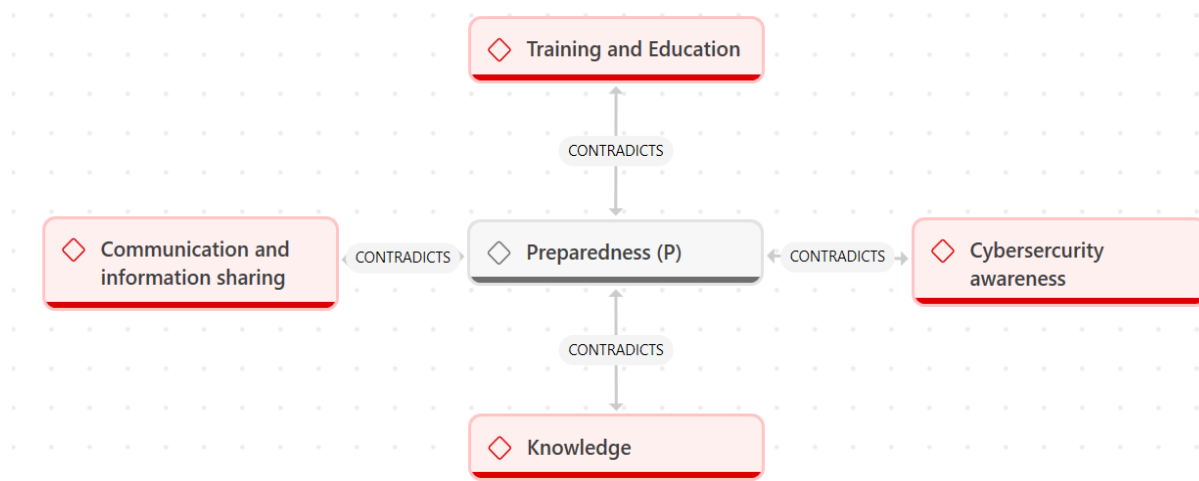


Figure 7.4: Summary of Preparedness Meta-theme (own source generated from ATLAS.ti)

The preparedness (P) theme illustrates how public E-Health institutions get ready for cybersecurity and prepare their employees (both management and non-management staff) to

avoid cyber incidents. The preparedness (P) construct is related to the staff's awareness and competency with regard to cybersecurity-related issues.

Density is the number of links to a theme from a given data set (Passonneau & Coffey, 2011). Grounding denotes the number of connections of the codes to the theme (Rambaree, 2018).

Fourteen codes were connected to the theme preparedness (P) (see Table 7.4). The Grounding (G) of most codes showed their relevance to the theme, but their association with preparedness was mostly negative. The codes were categorised into 4 sub-themes (see Table 7.4 and **Figure 7.4**). The themes associated with the preparedness construct were categorised and named accordingly. Table 7.4 provides a full summary of findings related to preparedness, including the sub-theme codes and their associations.

Table 7.4: Preparedness (P) Theme Category

Theme category	Sub-Themes	Preparedness theme codes	Association	G	D
Preparedness (P) theme	Knowledge	No knowledge of NCPF*	Negative (-)	5	3
		Disposal of ICT equipment	Negative (-)	1	1
		Knowledge of POPIA*	Positive (+)	7	3
		Unknowledgeable and a need for CS	Negative (-)	20	1
	Training and Education	Informal education	Positive (+)	5	1
		Lack of CS training for ICT staff	Negative (-)	7	2
		Limited informal education	Negative (-)	1	1
		Collaborated CS training and education	Negative (-)	1	1
		Lack of CS education and training	Negative (-)	29	2
Preparedness (P) theme	Communication and information sharing	Intranet and website	Positive (+)	2	2
		Lack of and need for information	Negative (-)	3	1
		Limited or lack of CS incidents	Negative (-)	4	2
		Lack of communication, information sharing, and interaction between departments	Negative (-)	3	2
	Cybersecurity awareness	Lack, ineffective, and need for CS awareness	Negative (-)	34	2
*National Cybersecurity Policy Framework (NCPF)					
*Protection of Personal Information Act (POPIA)					

The preparedness (P) high-order theme (see Table 7.4) showed that, overall, this theme had contradicting associations with each of the sub-themes (the current situation was considered to be unsatisfactory). This indicated that there was little or no evidence that the public E-Health institutions tried to prepare their staff for a culture of cybersecurity. For example, the institutions lacked the necessary competency, awareness and training to develop an appropriate cybersecurity culture.

The data analysis (see Table 7.4) showed that most of the individual codes also had contradictory associations with the preparedness theme (the current situation was considered to be unsatisfactory). For example, all knowledge codes had a contradicting relationship with the theme, except for the ‘knowledge of the Protection of Personal Information Act (POPIA)’ code; this was an indication of a lack of understanding and knowledge of cybersecurity.

Based on the findings from the interviews, staff in the public E-Health institutions, including the managers, lacked preparedness characteristics. For example, participants indicated that:

Participant 6: *“Number one is the understanding of cybersecurity itself from senior managers, from managers. OK, let me just explain that in most cases, senior managers, they don't understand IT...”*

Participant 7: *“lack of knowledge and understanding of cybersecurity, cyber threats that are out there. Yeah, lack of knowledge and understanding of what is really going on in the cyberspace. Because everyone is now using technology, but the use of technology without understanding of the possible threats that comes with the technology, says, it's one, is a major...”*

Training and education are considered to be functions at the individual level (Alhogail et al., 2015; Georgiadou et al., 2020a; 2020b). But they are also seen as functions at the management level of the organisation (Huang & Pearlson, 2019). In this research, ‘training and education’ was identified as a cybersecurity culture sub-theme that applied at both the management and the individual level of the organisation. Under the preparedness (P) high-order theme, the training and education sub-theme was viewed from the perspective of the individual.

The association of the codes with the training and education sub-theme (see Table 7.4) were mostly negative, indicating limited or even a complete lack of cybersecurity training and education among ICT staff and other system users in public E-Health institutions. The following comments reported the lack of cybersecurity training and education:

Participant 6: *“Hey. Let me say ‘none’. Yes, the reason for that is that the department is currently or is always operating under a cost curtailment regulation which prohibits any training or for you going out for training”*

Participant 3: *“No, we have not even attended any. I haven’t attended any. No training.”*

The data analysis showed that codes associated with the communication and information sharing sub-theme indicated contradictions (the situation was considered to be unsatisfactory) except for the ‘Internet and website’ code (see Table 7.4). The contradictions were evidence that there was ineffective communication and information sharing in the public E-Health institutions. The institutions had communication structures (intranets and websites) that could have been used for cybersecurity communication, but they were not being used effectively.

For example, ICT staff, including support technicians, server administrators and managers indicated:

Participant 4: *“It’ll will go back to that information or sharing. I think we need to share more information to our clients...”*

Participant 9: *“To achieve cybersecurity, the main barrier it’s lack of information...”*

Almost all the participants attested in one way or another through their responses to the significance of cybersecurity awareness and the lack of it among people in their institutions. Although this sub-theme was closely related to the knowledge sub-theme, it was treated as a separate theme in this research because of its significance in cybersecurity literature, and this was confirmed in this analysis with the degree of Groundedness ($G = 34$) of the sub-theme in the data. Some supported data extracts are:

Participant 9: *“Awareness, awareness and awareness. It says a very first step, even if they will take what you say, they will take seriously or not take seriously, but it all starts with awareness. And this awareness should be driven by the institution...”*

In general, the finding of the preparedness (P) construct revealed:

- no formal training in cybersecurity
- ineffective communication and sharing of cybersecurity information
- Lack of awareness and knowledge of cybersecurity threats, policy, and practices of the institution

Hence, the current situations and prevalent practices worked against (contradicted) the establishment of a culture of cybersecurity being developed. These findings reflected a weak to non-existent cybersecurity culture in E-Health institutions. In the literature, these sub-themes have been indicated as among the most crucial factors in creating a strong culture of any security (Alhogail, 2015; Alhogail et al., 2015; Chen et al., 2015; ENISA, 2017).

7.4.4.2 Theme Category 2: Responsibility (R)

The ATLAS.ti model that summarises the responsibility (R) construct is depicted in **Figure 7.5**. The responsibility theme describes the behaviour of ICT staff in terms of their attitude and perceptions towards cybersecurity and potential cyber-attack incidents.

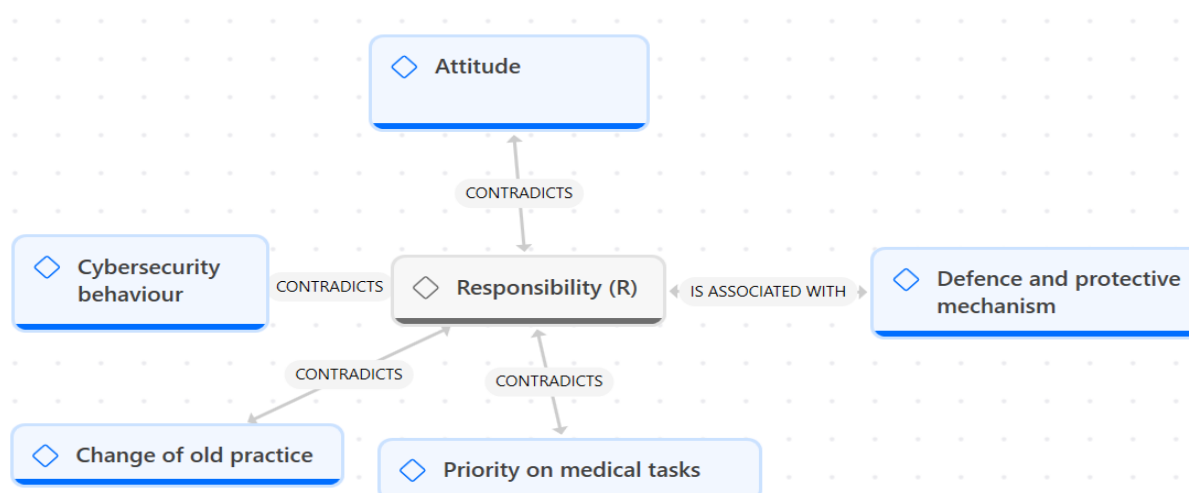


Figure 7.5: Summary of Responsibility Theme (own source generated from ATLAS.ti)

The 5 sub-themes related to responsibility (R) as a theme were categorised and presented in Table 7.5, together with the codes linked to them. From this figure, it can be seen that only one of the sub-themes, ‘Defence and protective practices’, had a positive association with responsibility (R). This sub-theme had the highest Grounding (G = 24) (see Table 7.5), The remaining four sub-themes had contradictory relationships (negative associations) with responsibility (R).

Table 7.5: Responsibility (R) Theme Category

Theme category	Sub - Theme	Responsibility theme codes	Association	G	D
	Attitude	Lack of willingness	Negative (-)	7	2

Theme category	Sub - Theme	Responsibility theme codes	Association	G	D
Responsibility (R) theme		Negative attitude and lack of interest towards CS	Negative (-)	8	1
	Change of old practice	Resistance to change	Negative (-)	4	1
	Cybersecurity behaviour	Inappropriate CS behaviour	Negative (-)	6	1
		Age has an impact on security behaviour	Negative (-)	3	1
		Personal money gain	Negative (-)	2	1
		Lack of security consciousness	Negative (-)	1	1
	Defence and protective practices	Protective measures of CS	Positive (+)	24	2
	Priority on medical tasks	Focus on medical work	Negative (-)	6	2

The data analysis found nine responsibility (R) codes, grouped into five sub-themes (see Table 7.5). The codes' Grounding (G) values showed their significance to the study and to the sub-themes they were linked to. Overall, the associations between the sub-themes emerging from the codes and the responsibility (R) high-order theme showed that the attitude and behaviour of public E-Health institutions in South Africa with respect to cybersecurity were not what they were supposed to be.

Based on the information in Table 7.5, the data extract suggests that most codes had a negative association with responsibility (R) as a theme. For example, both codes of the Attitude sub-theme showed a contradictory association with this theme, showing that individual employees of the institutions did not have a positive attitude towards cybersecurity and its practices. This could be due to a lack of interest in cybersecurity; when a lack of interest exists with regard to cybersecurity, it is likely to be followed by negative attitudes. Some evidence in the data relating to employees' negative attitudes supports this argument.

Participant 3: “like, you know, with my users, I don't think they show some interest...”

Participant 5: “I think, number one, we can deal with attitudes. The thing of saying we in government and nothing much. Some people are not taking their job maybe seriously or taking security seriously. Thinking everything is someone else's fault or someone has to deal with it...”

Participant 1: “...Others is the unwillingness of the users...”

The associations between the cybersecurity behaviour theme and its codes was mostly negative (see Table 7.5), indicating a problem with the cybersecurity behaviour of people in public E-Health institutions. If not addressed timeously, this could pose a serious threat to the institutions' essential assets (forms of patients' data, information, ICT systems, and ICT infrastructures). Examples of more general participants' comments related to this follow:

Participant 2: *"...They get frustrated cause it's old people". They say... "when I have to log into something, why must I put my password now and this and that and that, you know, it's asking me a million questions..."*

Participant 1: *"Is the users themselves, they are easily being trapped by these things. Yes, they are not vigilant enough. Some, they can click even untrustworthy mails. They can just open some links that are not.... or that they see off, but they will open them anyway."*

In contrast with the rest of the codes, 'Protective measures of cybersecurity', had a positive association and a high Grounding score (G=24), which showed that the public E-Health institutions do perform some activities that support the creation and strengthening of a culture of cybersecurity.

Examples of respondents' comments that showed protective measures in place in the institutions were:

Participant 7: *"...We do have firewalls because our network is managed by SITA. And SITA is making sure that firewalls and all those things are properly in place. And fireworks are one of our measures..."*

Participant 9: *"System, we control our access to that information in the form of a login username and password. So, there's no one who can access the system without a username and a password. And we discourage all types of system that comes, and they are without a username access control. So yeah, that one we do, yeah. It's the measure that we have..."*

The code 'Resistance to change' showed a negative association with this sub-theme, which suggested that people in the institutions preferred their old ways of doing things. This could be a challenge to implementing new cybersecurity practices for a better cybersecurity culture. ICT at the systems section, including their manager, made the following statements:

Participant 9: *“So I think managers have got a problem in my view of getting used to things done in a particular way.”*

Participant 8: *“Yeah. You know, the older people, actually they, like to stick to a routine. Yeah. So, if maybe there are some changes they are not handling them well because they are used to things being done this way”*

The code ‘focus on medical work’, that is, prioritising treatment of patients, had a negative association with the sub-theme of priority on medical tasks. In the literature, the fact that medical institutions tend to focus attention primarily on medical tasks has been given as one of the reasons the institutions are highly targeted by cyber-attacks (Martin et al., 2017). This finding concurs with information in the literature and emphasises the seriousness of the factor towards creating a cybersecurity culture.

- Some evidence from the code statement included:

Participant 3: *“You know another thing that I released with Department of Health, because it's a Department of Health, yes, they do have ICT, but then they focus mostly on the Primary Things, the services that they are providing mostly...”*

Participant 8: *“... But if you tell them about the security guide, that is less of a priority, you know...”*

The respondents made it clear that the E-Health institutions in the context of this case study did not show much interest in cybersecurity. The reason given was that their primary focus and priority was on medical work and treating patients, and not on providing security. This might be as a result of the organisation's culture, which focuses on patients rather than cybersecurity.

As a result, the institutions compromised activities that support and promote cybersecurity. The institution also needs to understand the importance of cybersecurity because patients' information can be stolen, and patients can die if a system becomes unavailable as a result of a cyber-attack, and the organisation could be sued.

Participant 3: *“No, most of the clinicians, maybe let me say 90% of the clinicians, they do their work, and then that's it. They don't want, they don't do other things or...”*
“they are not interested as well. They just want to do their work. Yeah, they just want to do their work and then go.”

“Department of Health, they do have ICT, but then they focus mostly on the Primary Things, the services that they are providing mostly, that's why the ICT is not that big here”

The finding of the responsibility (R) theme showed that public E-Health institutions had certain defence mechanisms and practices in place to ensure security of their critical assets, including protecting the hospital servers and systems. However, the security behaviours and attitudes of the institution members, and the fact that the E-Health institutions paid much more attention to the medical task of patient treatments, work against (contradict) the institution's efforts to strengthen cybersecurity. Also, people stick to their established security practices while using computer-based technological devices. This resistance to changing old security practices is a serious challenge.

Due to the contradictions found with some of the sub-themes, the current attitudes and behaviours related to responsibility (R) worked against (contradicted) the establishment of a culture of cybersecurity being developed, particularly from a human security behaviour perspective. However, this finding did not indicate as large a problem as was the case with the preparedness (P) as a theme.

7.4.4.3 Theme Category 3: Management (M)

Figure 7.6 depicts the ATLAS.ti model for the management (M) theme and sub-themes, indicating their associations and frequency.

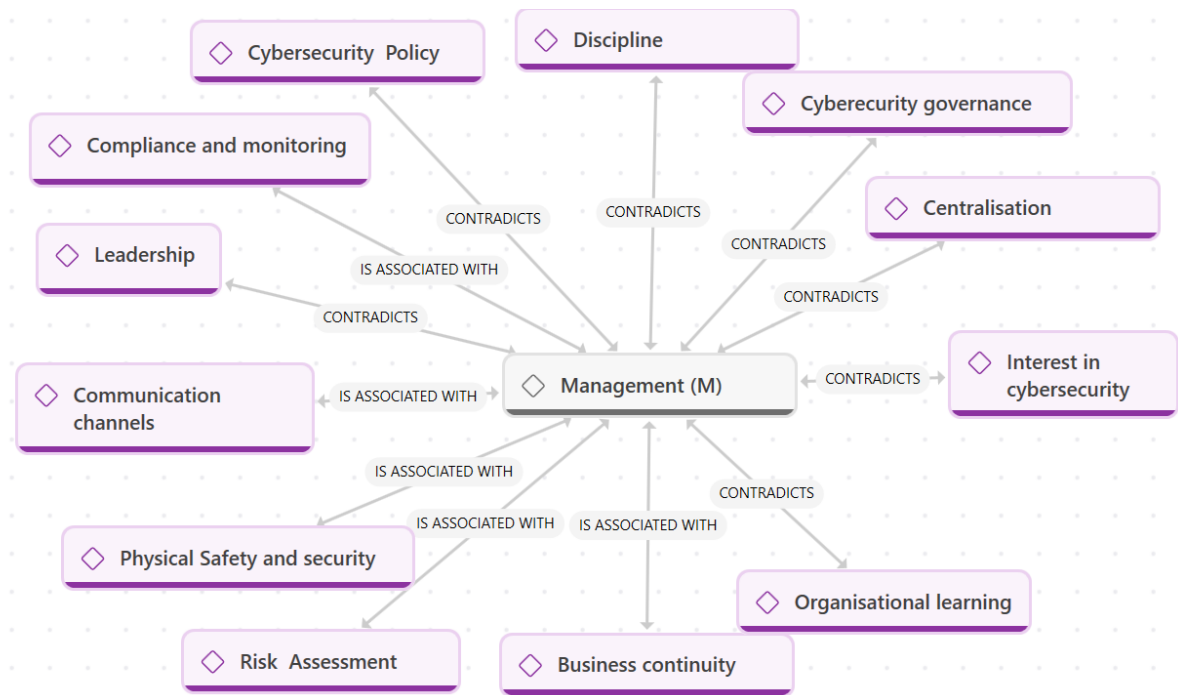


Figure 7.6: Summary of Management Theme (own source generated from ATLAS.ti)

The management (M) theme revealed the actions of the public E-Health institutions' top management in relation to cybersecurity culture and its potential threats and incidents. The analysis revealed 36 codes linked to the sub-themes of management (M), and these were categorised into 12 sub-themes (see Table 7.6). Some of these codes were particularly important as they were not unique to management but also had associations with other themes. Examples include codes linked to the organisational learning and communication channel sub-themes.

The grounding of the codes was evidence of their importance to the related sub-themes. The associations the sub-themes had with the management (M) theme, as modelled in Table 7.6, were mostly negative (see Table 7.6). This indicated that, according to the interviewees, there were insufficient actions from the internal organisation management that would assist in creating a culture of cybersecurity in the public E-Health institutions in South Africa.

Table 7.6: Management Theme Category

Theme category	Sub-themes	Management theme codes	Association	G	D
Management (M) theme	Organisational learning	No way to build and retain CS	Negative (-)	4	1
		Lack of CS training	Negative (-)	7	2
	Leadership	Lack of resource	Negative (-)	14	1
		Financial constraints or support	Negative (-)	16	1
		Management response time	Negative (-)	1	1
		Lack of ICT personnel capacity	Negative (-)	10	1
		Lack of CS champion or team	Negative (-)	18	1
		Inappropriate decision making	Negative (-)	3	1
		Top management support and involvement	Negative (-)	16	1
	Communication channels	Intranet and/ website	Positive (+)	2	2
		Lack of communication and information sharing	Negative (-)	4	2
		Email communication awareness	Positive (+)	9	1
	Cybersecurity policy	No/unaware of CS policy existence	Negative (-)	7	1
		Existence of outdated or no strategic security policy	Positive (+)	4	1
		Engagement in policy development and management	Positive (+)	3	1
	Discipline	Lack of discipline	Negative (-)	2	1
	Interest in cybersecurity	Limited attention to CS	Negative (-)	18	1
		Limited or lack of CS incidents	Negative (-)	4	2
		Lack of willingness and interest	Negative (-)	7	2
	Cybersecurity governance	Lack of governance structures	Negative (-)	6	1
		Lack of plan to ensure, manage, and improve CS	Negative (-)	5	1
		No penetration test exists	Negative (-)	6	2
		Limited measures for CS plan, management, and improvement	Negative (-)	1	1
	Compliance and Monitoring	User Restrictions	Negative (-)	2	1
		Sharing of password	Negative (-)	4	1
		Authentication	Positive (+)	7	1
		Restrictions	Positive (+)	8	1
		Monitoring and evaluation	Negative (-)	2	1

Theme category	Sub-themes	Management theme codes	Association	G	D
Management (M) theme	Business continuity	Security planning activities	Positive (+)	5	2
		Lack of continuous vulnerability management activities	Negative (-)	9	2
		No contingency plan	Negative (-)	6	3
		Existence of a disaster recovery plan	Positive (+)	4	1
	Risk assessment	Lack of risk assessment	Negative (-)	4	2
		Conduct risk assessment	Positive (+)	3	2
	Physical security	Physical security activities	Positive (+)	5	2
	Centralisation	Centralisation of CS/ICT	Negative (-)	3	1

The analysis based on the 12 sub-themes shown in Table 7.6 revealed that the two codes associated with the organisational learning sub-theme exhibited a negative association, which reflected a lack of organisational learning in the public E-Health institutions. This means that, according to the interviewees, there was no formal way for the institutions to develop their staff's cybersecurity knowledge. No cybersecurity training was provided either to the ICT staff or the medical and administrative staff. The following extract from an interview supports this.

Participant 9: *“Nothing is done along this line, I must say. Nothing is done. Nothing, nothing. Nothing is done. At least to see if people were just aware, there were just awareness. Even if, after an awareness, nothing was done. But that people, at least know that in itself is a measure. Because if you are aware that you don't have to just open any e-mail that you just don't know. You see, even if you're not aware of a specific virus or what? But that becomes a major in itself that you know the strange emails. You know, things that has got the potential to harm your computer. Then you will know how to deal with it...”*

All seven codes identified showed a contradictory relationship with the leadership sub-theme. Hence, the actions of public E-Health institutions' top management did not actively support or favour the development of a cybersecurity culture. The institutions had limitations with respect to cybersecurity; they did not have dedicated cybersecurity champions, there were not enough qualified ICT personnel, and there was insufficient financial support. These limitations

negatively impacted cybersecurity to such an extent that the institutions did not even have anti-virus protection at that time. Supporting qualitative data included:

Participant 8: *“I know in department, there's no team. No dedicated cybersecurity team/section/person. Yeah, I hadn't. Maybe that's why you find that it's something that is not happening as often as we would like it to be. Yes, because there's nobody that Champions it...”*

Participant 5: *“we need to have a dedicated team which will deal with security because currently, we don't have those people...”*

Participants 5 and 1: *“....we're understaffed. We're not sufficient.”*, *“The Hospital is very big for one IT to support the users. It affects the turnaround time of resolving ICT queries...”*

Participant 6: *“And then the problem also emanates from the fact that if management does not take a key role in as far as securing the information of the department is concerned, then it becomes a problem because you need to have policies...”*

Most codes associated with the communication channel's sub-theme, including 'email communication awareness' and 'intranet and/or website', revealed the existence of appropriate communication channels in the E-Health institutions. However, some respondents still indicated a lack of communication and interdepartmental collaboration.

Extracts from the qualitative data supporting the existence of communication channels include:

Participant 3: *“...Yeah, the department. OK, most of the policies we have, I think they are on our website. Or we used to have the Internet local intranet where everybody can access any policy for the department, so that one I don't think, I don't know if it's still active...”*

Participant 5: *“They normally will distribute like the different policies via maybe emails, and then we have the Internet.”*

Codes for the cybersecurity policy sub-theme revealed equal Groundedness for the combined positive associate relationships and the contradictory ones, which suggested the existence of security policies in institutions. However, the security policy was outdated or not strategic, and staff members were not fully aware of its existence in the institution, as attested by the respondent's comments.

Participant 6: *“Yes, we do. we have a cybersecurity policy. But you see the problem is with security or with anything else that it is effective if it is understood and also implemented from a strategic point of view. ...”*

Participant 5: *“There is a security policy, but in my view, it's outdated. But somehow there is a policy for that? It was developed. I'm not sure when it was developed...”*

Table 7.6 shows that two codes were associated with risk assessment (they indicated opposite views). One had a positive association, but the second code had a negative association with the sub-theme (the negative relationship was only slightly greater).

The positive association comment suggested the existence of a risk assessment structure in the institutions. However, the practice of assessing to identify possible cybersecurity risks for the institution was not being done in the way it should, or it had not happened for a long period (since the appointment of some ICT staff), hence the negative association of the ‘lack of risk assessment’ relationship. Extracts from respondents reflecting both types of relationships are depicted below:

Participant 8: *“Yes, the risk is performed because there is a section that is dedicated to dealing with that which is placed under internal audit...”*

Participant 2: *“Since I've been here, it hasn't been done...”*

Participant 6: *“No, no risk, it's at the provincial level, but normally we do not do this assessment ourselves...”*

The extracts from the transcriptions related to codes for the ‘discipline’ sub-theme showed the absence of actions by the top management, which would act as a deterrent in the studied public E-Health institutions with regard to unacceptable behaviour regarding cybersecurity policy. In this study, the codes associated with the interest in the cybersecurity sub-theme all showed a negative relationship with the sub-theme. Limited attention on cybersecurity emerged as the code with the dominating negative relationships with the sub-theme.

The following statement bears this out:

Participant 4: *“I was saying there's nothing that they can do to make you feel scared. Maybe they block you from using the Internet for a week. There's no such thing. Yeah, they'll just say you did it. Don't do it again. Yes. Nothing... Nothing will happen to you. Nothing will happen.”*

The remaining codes were ‘lack of interest’ and ‘limited or lack of cybersecurity incidents’.

Limited attention to cybersecurity implied that senior management was not taking their role and responsibility as seriously as they could have. They did not enforce the application of good CS practice, which resulted in ICT risks. Management's apparent disregard for cybersecurity issues could be evident in the bottom-up approach the institution followed with regard to cybersecurity, which had proven inefficient.

Instead, employees suggested that a better strategy would be a top-down approach. Limited attention to cybersecurity also implied that some employees lacked interest in or paid little attention to the CS practices of the institutions. The neglect of cybersecurity by the management and employees in the institutions could be attributed to their having had no serious cybersecurity incident; the only known kind of attack they had experienced in the past was pop-up virus attacks. On the other hand, this impression could be because they were not aware of attacks that had occurred since these were not monitored, and no records of past incidents were maintained.

Participant 6: *“And then the problem also emanates from the fact that if management does not take a key role in as far as securing the information of the department is concerned, then it becomes a problem...”*

Participant 8: *“... I think the best approach may not be this bottom down approach but Top button approach...”*

The code ‘lack of willingness’ related to an unwillingness to comply with cybersecurity practices on the part of employees who preferred to focus mainly on work that was obviously healthcare, and paid little attention to cybersecurity. Lack of willingness and interest was also interpreted as being due to a lack of awareness of cybersecurity practices and a lack of training. Clearly, this can be avoided by training system users or having a dedicated team that is responsible for a variety of cybersecurity practices in the hospital.

Participant 1: *“Others is the unwillingness of the users. The awareness is very important. Even training as well...”*

Participant 7: *“I think it's the will and the understanding of the importance of cybersecurity within the decision makers in the department...”*

No positive associations existed between any of the codes and the security governance sub-theme. The contradictions revealed a lack of security governance measures instituted by the top management of the public E-Health institutions studied. The institutions were, however, beginning to make plans in this direction. Extracts from the data attest to this.

Participant 7: “...we do not run tests. Yeah But, internally we do not run test.”

Participant 6: “...No, ma'am. Currently, they don't get involved. I'll say, I'll tell you why. Because our department does not have an ICT steering committee. Where senior managers are sitting and looking into you know all the things that are needed in by ICT to be effective, including security...”

Table 7.6 showed almost an equal strength of association (Groundedness) between codes indicating a positive and supportive situation, and codes reporting the opposite situation with regard to the compliance and monitoring sub-theme. The two codes that had a positive association with the sub-theme did not have a high Groundedness compared to codes with a negative association. Nonetheless, the associations suggested that the public E-Health institutions did have some evaluation and control measures in place that checked on their security practices. Nevertheless, institutions require more concerted action to counter the negative non-compliance issues. The following data extracts support this claim:

Participant 2: “... they have a 30-day policy which rotates, and It's constrained to that 30 days, but if you don't follow that, you are locked out. You understand what I'm saying? Yeah. So, if you don't follow those security constraints, you are locked out. We take you out of the system. So, I think that's the only way they can monitor.”

Participant 3: “And then the other thing that we do in each machine we don't give the users the administrator rights.”

On the negative side, employees do not comply with the basic roles as they share their passwords.

Participant 6: “...They are sharing passwords. In some instances, a person will leave his computer and go and ask a friend to finish up or to do his part or to assist him on something on his computer...”

Although the business continuity sub-theme categorised codes under the management theme, ensuring business continuity could also be seen as a responsibility construct, which is the domain most closely related to the practices and performance of staff. This applies, particularly when considering the ICT staff. Hence, ensuring business continuity should not be seen only as the responsibility of management, but instead as that of the management, employees (ICT and non-ICT staff), and business units. This is because its positive or negative impacts affect the entire healthcare ecosystem.

Respondents indicated that both the ‘security planning activities’ code and the ‘existence of disaster recovery plans’ had positive associations with the business continuity sub-theme. Although some participants indicated the existence of a disaster recovery plan (G=4), other participants contradicted that and said that there was no evidence of a contingency or recovery plan (G=6). The contradictory comments from different respondents could possibly be that some were less well informed than others (they lacked awareness and knowledge of the existence of a contingency or recovery plan), which would confirm the need for and importance of awareness in the institution.

Based on the interviewees’ comments, there was a ‘lack of continuous vulnerability management measures’ because the public E-Health institutions reacted to events instead of being proactive. The quality of their information security was not good as unauthorised people could gain access to important information. This confirmed what was stated previously, that participants’ claims that no security incidents occurred in the institutions might be due to a lack of awareness of cyber-attack incidents that had occurred previously. This in turn could be because the institutions failed to monitor or maintain records of cyber-attack incidents.

Participant 9: *“the level of security of the information is not to the correct level. Sometimes they even gain, lawyers can even gain access to such information...”*

Participants 3 and 4: *“I don't think we do have those plans in place, especially for this, the PEIS system because it is a local server....” “... currently they don't have anything in place.” “Example, if a computer crashes, all that data would be gone. There's nothing in place that would or recovery software that we might use to recover anything. They don't have backups...”*

Participant 6: *“It's very difficult, ma'am, to say they support it. Because like I said before, to you that we don't have an antivirus even now. Yes, so, yes, you see the problem is.”*

The code ‘physical security activities’ had a positive association with the physical safety and security sub-theme, which showed that the E-Health institutions implemented some forms of physical security to protect their ICT assets. The following extract from the interview supports this sub-theme.

Participant 2: *“...we also have lockable. This thing you tie to your table. Yeah. The tying of the laptops.... And then you also have your cameras in place...”*

The code associated with the centralisation sub-theme showed a contradiction (the situation was considered to be unsatisfactory). The analysis found that Mpumalanga province's public E-Health institutions' ICT department was centralised at the provincial level. From the provincial level, support was provided to the hospitals and clinics located at the district level, and some of them were very far apart, which required the ICT support team to travel some distance to the hospitals that required their services. This was considered a serious problem that could hamper efforts to cultivate a culture of cybersecurity because it sometimes took ICT staff more than 24 hours to respond to issues reported by the different hospitals of the district.

Quotes from the respondents which supported the problems related to centralisation follow:

Participant 1: *"The IT is central.... everything is centralised there...the budget is there in the head office, and they are doing everything in the head office..."*

Participant 3: *"...it is centralised actually through there provincial level."*

Participant 6: *"... You see, the people that are at the hospital level, they depend on the district and the province to educate them on security..."*

Based on the information given in Table 7.6, the finding revealed management (M) as a significant theme in the qualitative analysis presented in this chapter. The analysed data, as depicted in Table 7.6, revealed that most sub-themes (seven sub-themes) associated with the management construct had negative (contradictory) associations. Five sub-themes, 'communication channels', 'business continuity', 'risk assessment', 'compliance and monitoring', as well as 'physical safety and security', had positive associations with this theme.

The ICT staff interviewed, including the managers, indicated that in the public E-Health institutions, not much interest was shown in cybersecurity affairs. This was because the E-Health institutions that were studied did not consider cybersecurity to be their primary priority. This might be because they had not experienced a serious cyber-attack incident, or they were not aware of one as there were no records of past incidents. This confirmed what respondents said, that the management was not proactive regarding cybersecurity.

Participant 5: *"... it applies even to the management. I would say, yeah, yeah. Yeah, because you know the approach is normally reactional, like if something has happened.... Yeah, it's not like proactive...", "I'm saying to you, every time things like this is on a reactional basis..."*

7.4.4.4 Theme Category 4: Environment (EE)

The ATLAS.ti model that summarised the Environment (EE) construct theme and codes is given in **Figure 7.7**.

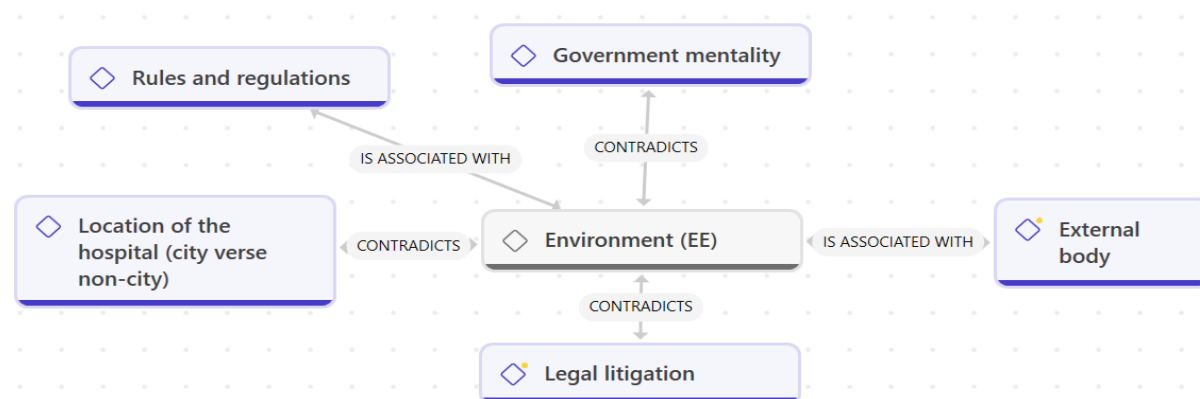


Figure 7.7: Summary of Environment Theme (own source generated from ATLAS.ti)

The external environment (EE) theme category concerns the environmental factors of public E-Health institutions in relation to cybersecurity and potential threats. The analysis of the transcript discovered seven codes that were linked to the theme (see Table 7.7).

Three codes, namely ‘no knowledge of the National Cybersecurity Policy Framework (NCPF)’, ‘knowledge of the Protection of Personal Information Act (POPIA)’, and ‘health ethical issues’, were categorised as ‘rules and regulations’, which showed a positive association with the environment (EE) theme. The codes ‘external body’, ‘government mentality’, ‘legal issues’ and ‘hospital location’ were also regarded as sub-themes. Most of the Groundedness (G) of the codes were above 1, which shows their importance to the environment as a theme.

Table 7.7: Environment Theme Category

Themes category	Sub-theme	Environmental theme codes	Association	G	D
Environmental theme	Rules and regulations	No knowledge of NCPF	Negative (-)	5	3
		Knowledge of POPIA	Positive (+)	7	3
		Health international ethical standard	Positive (+)	2	2
		External body	Positive (+)	4	1
		Government mentality and political matter	Negative (-)	4	1
		Legal issues /litigations	Negative (-)	2	1
		Hospital Location	Negative (-)	2	1

The codes classified under the rules and regulations' theme (see Table 7.7) confirmed the existence of legislation and guidelines like the Protection of Personal Information Act (POPIA) and the National Cybersecurity Policy Framework (NCPF). These legislations guide the use and protection of information in public E-Health institutions. However, it appears that some members of the ICT staff did not have much knowledge of the legislation and guidelines. This could be seen by the positive (is associated with) and negative (contradicts) relationships that existed between the codes and the rules and regulations sub-themes.

Figure 7.7 and Table 7.7 show the one sub-theme and the five uncategorised codes of the environment theme and their associations. According to **Figure 7.7**, one theme and one code had positive relationships (with a total Groundedness $G = 18$), and four other codes (with a total Groundedness $G = 7$) had negative relationships.

The finding on the positive side noted the existence of legislation and regulations that guide cybersecurity in institutions, which is a good practice if a culture of cybersecurity is to be achieved. The institutions had external bodies, the Auditor General of South Africa (AGSA) and the State Information Technology Agency (SITA), that offered services that supported cybersecurity culture; SITA provides network security using firewalls, and AGSA assists with security compliance of critical infrastructures.

Supporting extracts from the data to these findings follow:

Participant 6: “...AG makes sure that we have to be in compliant...”

Participant 6: “...Yeah, but you remember that if you are talking about health, health has their own special policies. Because we are dealing with information..... there are also international standards when it comes to health, like your HL 7 standard, which deals with health level 7, they are calling it health level 7 standard...”

Another environmental issue that threatened the security of information in the healthcare institutions studied was the possibility of legal claims brought by a lawyer against the institutions. This creates high-security threats as the lawyers try to gain access to information at all costs. If the people working in the institution had a lackadaisical mentality, the situation could worsen because they might not adhere to security practices or take security seriously. The location of the hospital was also considered to be an environmental issue because people were perceived to be exposed to more cybersecurity threats in big cities than in rural environments and had access to more cybersecurity institutions. Examples of codes indicating some environmental issues include:

Participant 6: “These days is this thing of, you know, litigations. Where a patient dies in the hospital due to suspicious medical conditions, and then the people from outside will request people from within the department to steal information for them? So that they can sue the department...”

Participant 9: “Lawyers, when they challenge the department, they have more information than the department because the level of security of the information is not to the correct level. Sometimes lawyers can even gain access to such information...”

7.4.4.5 Theme Category 5: Technology

Figure 7.8 demonstrates the ATLAS.ti model that identified codes associated with the Technology theme.

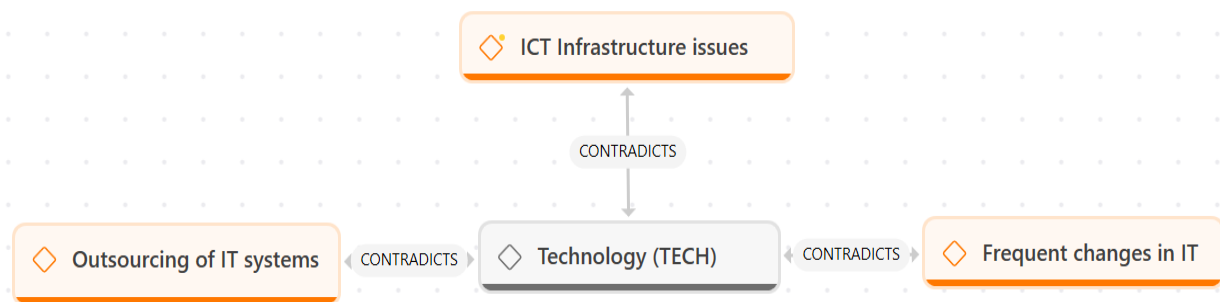


Figure 7.8: Summary of Technology Codes (own source generated from ATLAS.ti)

ICT was characterised by the interviewees as constantly changing and hence, requiring continuous investment in ICT infrastructure to keep up with emerging cyber threats. However, the findings revealed low levels of actual investment in ICT infrastructure in public E-Health institutions. This resulted in the institutions not having sufficient, good quality and updated infrastructures to support cybersecurity. Respondents identified issues like slow Internet speed, legacy systems and outdated software, and suggested that, to achieve or support a cybersecurity culture, the most recent security patches and proper ICT infrastructure that supports cybersecurity were needed.

Table 7.8 also showed the codes that fell under the technology (TECH) theme.

Table 7.8: Technology Codes

Themes category	Themes	Technology theme codes	Association	G	D
Technology theme	ICT infrastructure issues	Legacy system	Negative (-)	3	2
		Adequate ICT infrastructure	Negative (-)	2	1
		ICT budget	Negative (-)	2	1
	Frequent changes to IT	Software update and maintenance	Negative (-)	1	2
		Continuous investment	Negative (-)	1	1
	Outsourcing of IT systems	Standards and Outcomes	Negative (-)	1	2
		CS requirement assessment	Negative (-)	1	2

Outsourcing is the practice of using the services of third parties to maintain and operate ICT systems and services. The finding showed that the public E-Health institutions outsourced some of their ICT systems.

***Participant 2:** “The infrastructure is not in place. Maybe if there were more infrastructure certain things would be protected, very protected...”*

***Participant 3:** “there are systems that are outsourced from maybe some companies...”*

In general, the technology construct had unsatisfactory relationships with the associated codes, as the data indicated that the recommended practices were either met only partially or not at all (see Table 7.8 and **Figure 7.8**). The finding revealed that issues related to technology, including infrastructural issues, the impact of rapidly changing ICT things, and the possible implications of outsourcing for ICT systems, were not given proper attention in the public E-Health institutions.

7.5 IDENTIFIED CYBERSECURITY CULTURE THEMES

The objective of this chapter was to identify factors that were associated with cybersecurity culture in the public E-Health institutions in South Africa. This objective was partly achieved in this section by identifying cybersecurity culture factors qualitatively, as depicted in **Figure 7.9**.

The final result is achieved by performing triangulation in **Section 7.6**. Identifying factors associated with cybersecurity culture under the five higher-order themes depicted in **Figure 7.9**, achieved the third phase of the framework analysis, “*identifying and naming concepts*,” and the fourth phase, “*deconstructing and categorising the concepts*”.

Based on the findings summarised and compared in this chapter, the study revealed that the constructs of preparedness (P), responsibility (R), management (M), technology (TECH), and environment (EE) all had an association with a culture of cybersecurity. This also meant that sub-themes categorised under these themes had either positive (satisfactory) or negative (contradictory) associations with cybersecurity culture in the case study of public E-Health institutions.

A positive relationship implied that the E-Health institutions had some of the required activities in place to develop and strengthen a particular theme of cybersecurity culture, while the reverse was the case with a negative relationship with a theme.

The finding was substantial as it provided lists and strengthened the understanding of cybersecurity culture themes in the research context. These themes were used as the basis for developing a framework for establishing a cybersecurity culture for public E-Health institutions in South Africa.

Figure 7.9 portrays the cybersecurity culture themes with their associated sub-themes based on the findings of the qualitative data analysis. These are the factors associated with cybersecurity culture from the qualitative analysis.

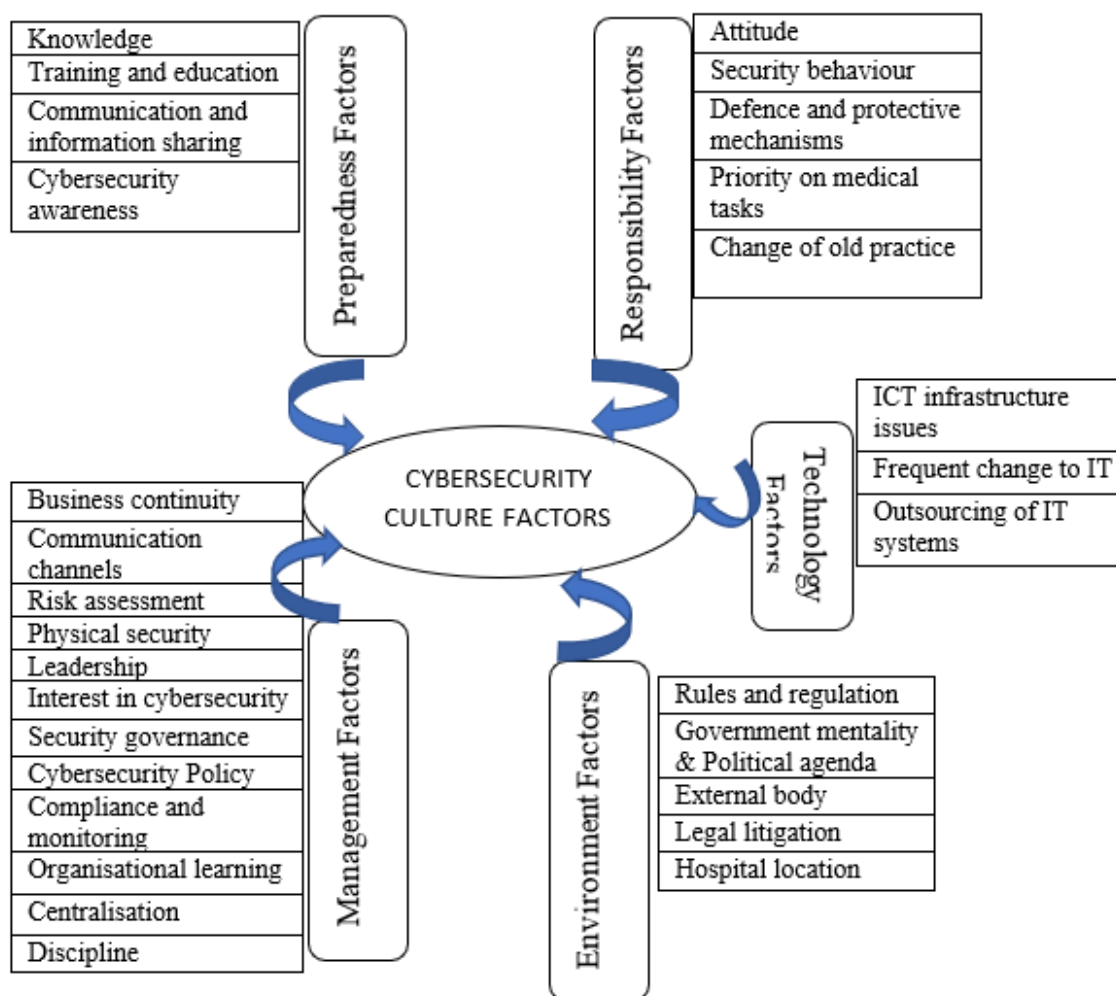


Figure 7.9: Cybersecurity Culture Themes of Public E-Health Institutions (own source)

7.6 TRIANGULATION OF FINDINGS

This section explains how triangulation was achieved in this study. First, the findings of the quantitative and qualitative models were compared, and the identified factors from the mixed method were triangulated. Secondly, further triangulation took place between the document analysis and the mixed method triangulation finding.

7.6.1 QUALITATIVE AND QUANTITATIVE COMPARISONS OF MODELS

Figure 7.10 and **Figure 7.11** depict the ATLAS.ti model of the final thematic diagram and the quantitative summary model, as well as their relationship with cybersecurity culture in public E-Health institutions in the case study context.

The thematic diagram shown in **Figure 7.10**, was used to summarise the main themes of qualitative analysis, and **Figure 7.11** was revisited (it originally was included in Chapter 6 as **Figure 6.4**) to help compare the two analysis methods regarded as the triangulation approach.

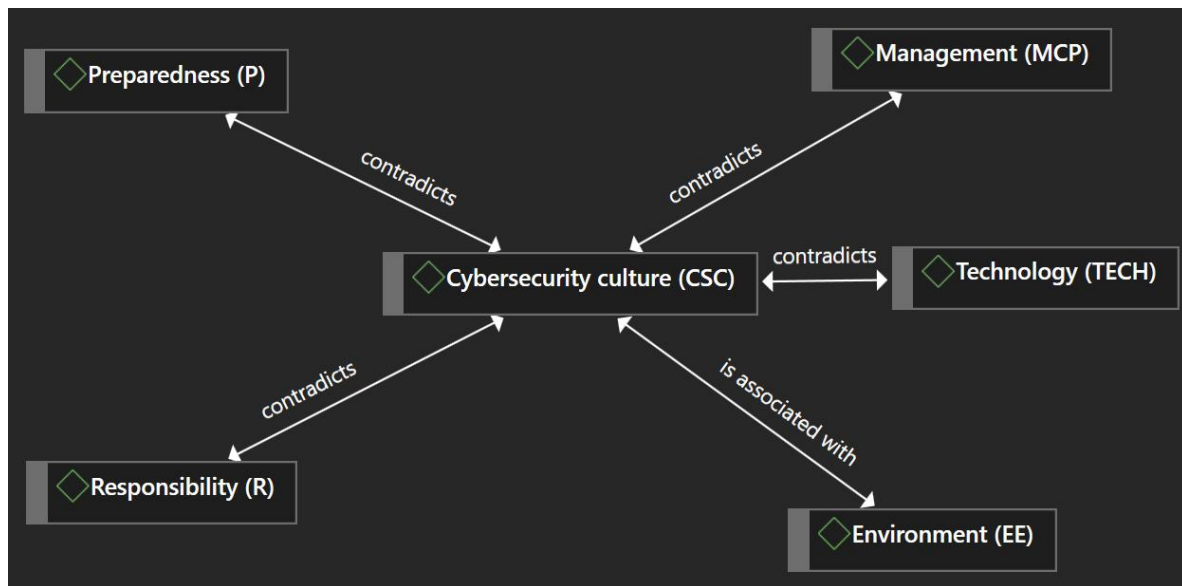


Figure 7.10: Model of the Final Thematic Diagram (own source generated from ATLAS.ti)

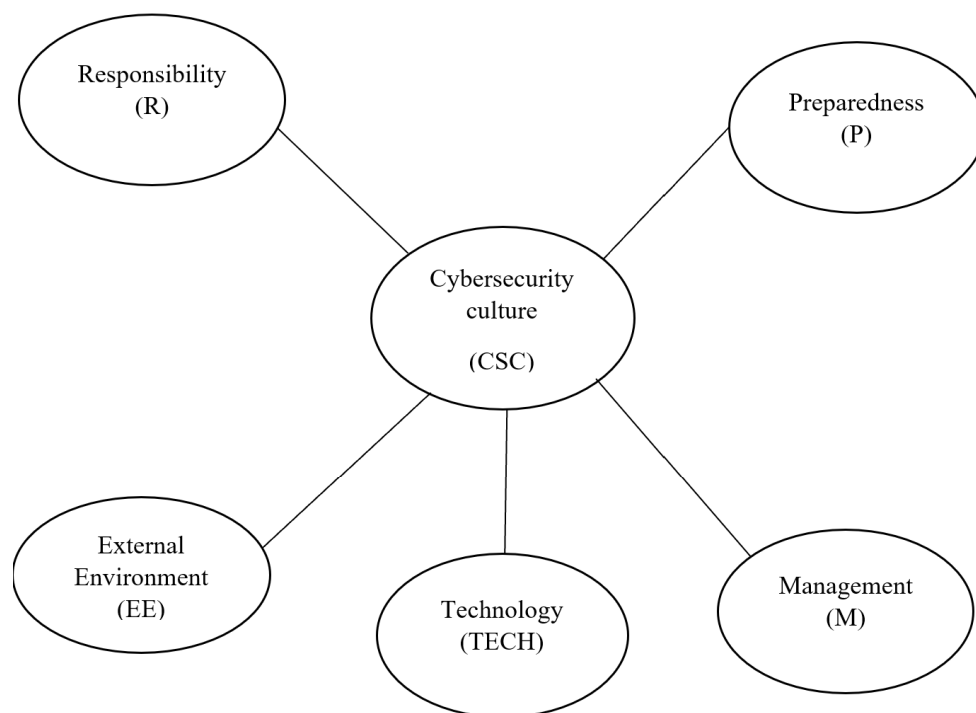


Figure 7.11: Revisited Quantitative Analysis Model (own source)

7.6.1.1 Preparedness (P) and Cybersecurity Culture

In summary, preparedness (P) can be said to be closely associated with cybersecurity culture in public E-Health institutions, as it clearly illustrates the relationship with cybersecurity culture. From the perspective of the ICT employees interviewed (see **Figure 7.10**) Preparedness (P) was considered to be Cybersecurity Culture's second most important theme. This can also be seen Table 7.4, which shows the number of sub-themes, their associated codes, and the Groundedness attached to the codes in relation to preparedness (P). The finding indicated that preparedness (P) was lacking in public E-Health institutions.

This finding was consistent with the quantitative analysis result obtained from non-ICT personnel (see **Figure 7.11**), which found that issues related to preparedness have a major impact on the development of cybersecurity culture in public E-Health institutions.

In the case study, sub-themes that were associated with preparedness that were not in place (negative association) (see **Figure 7.4**) included cybersecurity awareness, communication and information sharing, and training and education. These were found in Chapter 3 to be reasons why healthcare institutions were highly targeted, as well as a challenge that confronted E-Health institutions (Ghafur et al., 2019; Luna et al., 2016; Mello, 2017).

In Chapter 5, these themes were also identified as factors of cybersecurity culture (Corradini, 2020; Huang & Pearlson, 2019; Marotta & Pearlson, 2019; Ogden, 2021; Saigushev et al., 2020; Xiao & Watson, 2019).

7.6.1.2 Responsibility (R) and cybersecurity culture

Responsibility (R) was also negatively associated with cybersecurity culture, based on the thematic analysis shown in **Figure 7.10**. In addition, comparing the association between responsibility (R) and cybersecurity culture to the association between preparedness (P) and cybersecurity culture shows that these are similar in terms of Groundedness.

This finding was also supported by the quantitative analysis, which found responsibility (R) to correlate strongly with cybersecurity culture and other constructs (see Table 6.21). The results regarding the relationship between responsibility (R) and cybersecurity culture were also supported by the model produced in the quantitative study, which showed that there was a correlation between responsibility (R) and cybersecurity culture, as in **Figure 7.11**.

The themes associated with responsibility (R) (i.e., human cybersecurity behaviour, compliance, and priority on medical tasks) were also found as either a factor of cybersecurity culture or as reasons why healthcare institutions were high targets for cyber-criminals, as discussed in Chapters 3 and 5 (Ciuperca et al., 2019; Corradini, 2020; ENISA, 2017; Gundu et al., 2019; Leenen & Van Vuuren, 2019; Uchendu et al., 2021; Van 't Wout, 2019).

7.6.1.3 Management (M) and Cybersecurity Culture

As was the case with preparedness (P) and responsibility (R), the management (M) theme was found to have a relationship with cybersecurity culture in public E-Health institutions. In the qualitative analysis, Management (M) indicated a contradicting association with cybersecurity culture (see **Figure 7.10**). Management (M) appeared to be the dominating theme of cybersecurity culture from the viewpoint of the ICT employees interviewed. This was shown by the high number of sub-themes and grounded codes associated with the theme. The finding suggested that the public E-Health institutions investigated lacked the management qualities required to create a culture of cybersecurity.

The result of the qualitative analysis was in line with a quantitative study conducted with input from non-ICT staff (see **Figure 7.11**). The result demonstrated that management-related concerns influenced the cybersecurity culture in public E-Health institutions. Sub-themes associated negatively with management (M) (see **Figure 7.6**) (i.e., leadership, discipline, interest, organisational learning, and cybersecurity government) were found to be consistent with factors or elements identified by cybersecurity culture literature. For example, in her study, Da Veiga (2019) argued that the desired foundational elements of a security culture include leadership, governance, policies, and procedures (Da Veiga, 2019).

The themes that this study obtained from the data collected in the investigated public E-Health institutions corresponded with those identified in the literature review of this study and discussed under the management theme. In Chapter 4, some of the themes (i.e., for example, lack of resources, lack of cybersecurity champions, and financial (budget) constraints, which were negatively associated with the management theme in Chapter 7) were also identified as reasons why public healthcare institutions were highly targeted and as challenges that confronted E-Health institutions (Coventry & Branley, 2018; Jalali & Kaiser, 2018; Kruse et al., 2017; Martin et al., 2017; Morgan, 2020b).

The systematic review of Chapter 5 also listed management themes as being important in establishing a cybersecurity culture (Aiken, 2019; Clark et al., 2017; Gcaza & von Solms, 2017a; Gundu et al., 2019; Leenen et al., 2018; Rinchi, 2019; Uchendu et al., 2021; Van 't Wout, 2019; Wierzynski, 2019).

7.6.1.4 Technology (TECH) and Cybersecurity Culture

The qualitative analysis found that Technology (TECH) had a negative (contradictory) association with cybersecurity culture in public E-Health institutions based on the data collected from the interviews (see **Figure 7.10**). Technology (TECH) was the fourth theme selected based on its sub-themes and the Groundedness of the codes associated with it. The finding indicated that the public E-Health institutions investigated gave insufficient attention to problems related to ICT infrastructural issues, legal issues and outsourcing of ICT systems.

The results from the qualitative analysis were consistent with the quantitative findings, and showed that technology (TECH) was correlated with cybersecurity culture and other constructs (see the Pearson correlation given in Table 6.21 as well as **Figure 7.11**).

7.6.1.5 Environment (EE) and Cybersecurity Culture

The environment (EE) theme (see **Figure 7.10**) had an association with cybersecurity culture, but the relationship was not considered to be strong because of the difference between the “associate with” and “contradict” codes, extracts of the theme (see Table 7.7). The two sets of codes had an equal number of code quotations and equal Groundedness. Environment (EE) as a theme had a relationship with cybersecurity culture in public E-Health institutions, but the association was not a strong positive relationship, as was the case with the other three themes, all of which had strong negative relationships with cybersecurity culture.

In the qualitative analysis, the EE theme showed a positive “associate with” from the perspective of ICT employees, but the environment was the least important theme of cybersecurity culture (see **Figure 7.10**). With regards to cybersecurity culture, the findings indicated that the EE theme was not considered to need additional attention in the public E-Health institution. In other words, issues related to the environment were not seen by ICT staff as much of a problem with regard to creating or maintaining a culture of cybersecurity in their institutions.

This finding was also consistent with the findings of the quantitative analysis using data obtained from non-ICT personnel (see **Figure 7.11**). Based on the quantitative findings, issues related to the environment had no major impact on the culture of cybersecurity in public E-Health institutions. From the input from non-ICT staff, the issues were unpredictable with regard to cybersecurity.

7.6.2 TRIANGULATION OF FACTORS

The fourth phase (deconstructing and categorising) and fifth phase (integrating concepts) of the conceptual framework were carried out under triangulation. Table 7.9 depicts the triangulation results in column three as the list of factors associated with cybersecurity culture in public E-Health institutions.

This provided the final answer to the **Research Sub-Question 3 (RSQ 3)**: “*What are the factors associated with cybersecurity culture in the E-Health institutions in South Africa?*”

Table 7.9: Triangulation of Quantitative and Qualitative Findings

Factors (quantitative analysis)	Factors (qualitative analysis)	Results of Triangulation
Preparedness (P)	Preparedness	Preparedness
Training and Education	Training and Education	Training and Education
Cybersecurity Awareness	Cybersecurity Awareness	Cybersecurity Awareness
Knowledge	Knowledge	Knowledge
Communication and Information Sharing	Communication and Information Sharing	Communication and Information Sharing
Informal Learning	Informal Education	Informal Learning
Responsibility (R)	Responsibility	Responsibility
Attitude And Perception	Attitude	Attitude
Cybersecurity Behaviour	Cybersecurity Behaviour	Cybersecurity Behaviour
	Protective Practices	Protective Practices**
Priority On Medical Tasks	Priority On Medical Tasks	Priority On Medical Tasks
	Change Of Old Practices	Change Of Old Practices**
Management (M)	Management (M)	Management (M)
Cybersecurity Policy	Cybersecurity Policy	Cybersecurity Policy
Leadership	Leadership	Leadership
Punishment	Discipline	Discipline

Factors (quantitative analysis)	Factors (qualitative analysis)	Results of Triangulation
Reward		
Institutional Learning	Organisational Learning	Organisational Learning
Test Exercises	Security Governance	Security Governance
Guidelines		
Communication Channel	Communication Channel	Communication Channel
Compliance And Monitoring	Compliance And Monitoring	Compliance And Monitoring
	Business Continuity	Business Continuity**
Physical Security	Physical Security	Physical Security
	Centralisation	Centralisation**
	Interest In CS	Interest In CS**
	Risk Assessment	Risk Assessment**
Environment (EE)	Environment (EE)	Environment (EE)
Rules And Regulations	Rules And Regulations	Rules And Regulations
Location Of Hospital	Hospital Location	Hospital Location
Reputation damage		Reputation damage**
	External body	External body**
	Legal issues/litigation	Legal issue/litigation**
National culture	Government mentality and political matter	National culture
Technology (TECH)	Technology (TECH)	Technology (TECH)
Outdated technology	ICT Infrastructure	ICT Infrastructure
Frequent changes to IT	Frequent changes to IT	Frequent changes to IT
	Outsourcing of IT systems	Outsourcing of IT systems**
** Depicts factors identified from data collection but were not consistent across quantitative and qualitative		

In this study, factors that were validated using exploratory factor analysis and tested for reliability using Cronbach's alpha to formulate the significant factors of cybersecurity culture using correlation are shown in the first column of Table 7.9. In addition, ATLAS.ti was used to formulate factors regarded as sub-themes during qualitative analysis. These sub-themes are depicted in the second column of Table 7.9, and they were used to develop the different thematic network diagrams in the study. The third column shows the results of triangulating the two research methods.

In Table 7.9, the results from the triangulation show common factors in the quantitative and qualitative analyses, derived from factors highlighted by the system users and ICT staff as associated with cybersecurity culture in their institutions.

Column three highlights factors that were inconsistent when comparing the quantitative and qualitative methods. These factors are marked with an asterisk and depict factors that were only emphasised by one of the two groups (either by the system users or by the ICT staff). The results of the quantitative and qualitative analysis (columns 1 and 2), as well as the results of the triangulation (column 3), were presented according to the category (the high-order themes).

It is important to emphasise that although the third column of Table 7.9 contains factors that were not highlighted by both quantitative and qualitative data collection methods; they were still considered vital factors of cybersecurity culture in this study. This was because, according to the different employees of the hospitals (system users and ICT staff), these point out factors that need attention with regard to cybersecurity culture and, therefore, should not be ignored when cultivating cybersecurity culture in the public E-Health institution. These factors were identified from data as having an association with cybersecurity culture in the public E-Health institutions investigated and will be considered when the study framework is developed in Chapters 8 and 9.

Identifying these employee-specific factors increased the depth of understanding of the operations and business of E-Health institutions., This is an important step in cybersecurity culture development and implementation (ENISA, 2017). Therefore, the contextual framework developed in Chapter 8 was built on the triangulation results, including the employee-specific factors (factors with an asterisk).

7.6.3 COMPARING THE TRIANGULATION RESULT WITH THE SYSTEMATIC LITERATURE REVIEW DATA

This section extends the fourth and fifth phases of the conceptual framework analysis. The two phases deconstruct and integrate the cybersecurity culture factors from the triangulated result with the factors identified from the literature to produce the final list of critical cybersecurity culture factors. In these phases, cybersecurity culture, similar factors from the literature and triangulation lists are combined as a single factor. This process allows the identified cybersecurity culture factors to be reduced to a reasonable number to avoid duplication. The final list of cybersecurity culture factors is depicted in Table 7.10.

Table 7.10: Final Categorised and Integrated List of Cybersecurity Culture Factors

Cybersecurity Culture factors (literature)	Cybersecurity Culture (Triangulation Results)	Final list of Cybersecurity Culture factors
Preparedness	Preparedness	Preparedness
Training and Education	Training and Education	Training and Education
Engagement		
Collaboration		
Awareness	Cybersecurity awareness	Cybersecurity awareness
	Informal education**	Informal education**
Knowledge and understanding	Knowledge	Knowledge
Communication	Communication & information sharing	Communication & information sharing
Information Sharing		
Responsibility	Responsibility	Responsibility
Human behaviour and Organisational culture	Attitude Cybersecurity behaviour	Attitude Cybersecurity behaviour
	Priority on medical tasks**	Priority on medical tasks**
	Change of old practice**	Change of old practice**
	Defence and protective practices**	Defence and protective practices**
Management	Management	Management
Top management or leadership support	Leadership	Leadership
Role and responsibility		
Encouragement		
Budget and resources		
Commitment		
Cybersecurity champion or team		
Cybersecurity hub		
Cybersecurity strategy		
Interest	Interest in CS	Interest in CS
Compliance	Compliance and Monitoring	Compliance and Monitoring
Security audit		
Cybersecurity policy and procedures	Cybersecurity policy	Cybersecurity policy
Rewards and sanction	Discipline	Discipline
Risk and change management	Risk assessment	Risk assessment

Cybersecurity Culture factors (literature)	Cybersecurity Culture (Triangulation Results)	Final list of Cybersecurity Culture factors
Physical security	Physical security	Physical security
Business continuity plan	Business continuity	Business continuity
Accountability	CS governance	CS governance
Communication channel	Communication channel	Communication channel
	Centralisation**	Centralisation**
	Organisational learning	Organisational learning
Environment	Environment	Environment
legal and regulatory	Rules and regulations	Rules and regulations
Ethical conduct		Ethical conduct
	External body**	External body**
	Hospital Location**	Hospital Location**
	Legal issues/ litigation **	Legal Issues/ litigation **
National culture	National culture	National culture
Collectivism		
Ethical conduct	Reputational damage	Reputational damage
Trust		
Technology	Technology	Technology
	ICT infrastructure**	ICT infrastructure**
Outdated technology	Frequent changes to IT	Frequent changes to IT
	Outsourcing of IT systems**	Outsourcing of IT systems**
** Depicts factors identified from the data collection triangulation table but were not specifically indicated in the literature or relationally linked to factors indicated in the literature.		

By comparing, deconstructing and integrating the cybersecurity culture factors from the literature with factors obtained from the quantitative and qualitative data (triangulation results), the finding shows that the data from the data collection were generally in line with the literature. However, the survey also identified context-specific factors that were not in the literature. For example, centralisation, hospital location, legal issues, informal learning and technology-related factors. These context-specific factors were considered essential as they emphasised the importance of contextual differences that must be considered when cultivating cybersecurity culture.

The information in the final list of cybersecurity culture factors (see Table 7.10) was considered for the design and development of a contextual framework for establishing the cybersecurity culture in public E-Health institutions.

7.7 CONCLUSION OF THE QUALITATIVE ANALYSIS CHAPTER

A sub-objective that this study sought to achieve was **Research Sub-Objective 3 (RSQ 3)**. This aimed to identify factors associated with cybersecurity culture in public E-Health institutions. To achieve this objective, empirical work was conducted using a mixed-method approach. Chapter 7 presented the qualitative part of data collection, and the analysis performed to achieve this research sub-objective. The chapter used interviews as the qualitative data collection instrument, and thematic data analysis was used to analyse the data to reaffirm the cybersecurity culture themes that had already been provisionally identified.

To answer the **Research Sub-Question 3 (RSQ 3)**, “*What factors are associated with cybersecurity culture in public E-Health institutions in South Africa?*” The findings of the qualitative and quantitative approaches were triangulated. Based on the triangulation, it was evident that five constructs, preparedness (P), responsibility (R), management (M), environment (EE), and technology (TECH), were all associated with cybersecurity culture in the public E-Health institutions in the context of this study.

In the qualitative analysis, the four themes (preparedness (P), responsibility (R), management (M), and technology (TECH)) were found to have negative associations with cybersecurity culture as they were not being implemented to any extent. In contrast, environment (EE) as a theme had a slight positive relationship from the perspective of ICT staff.

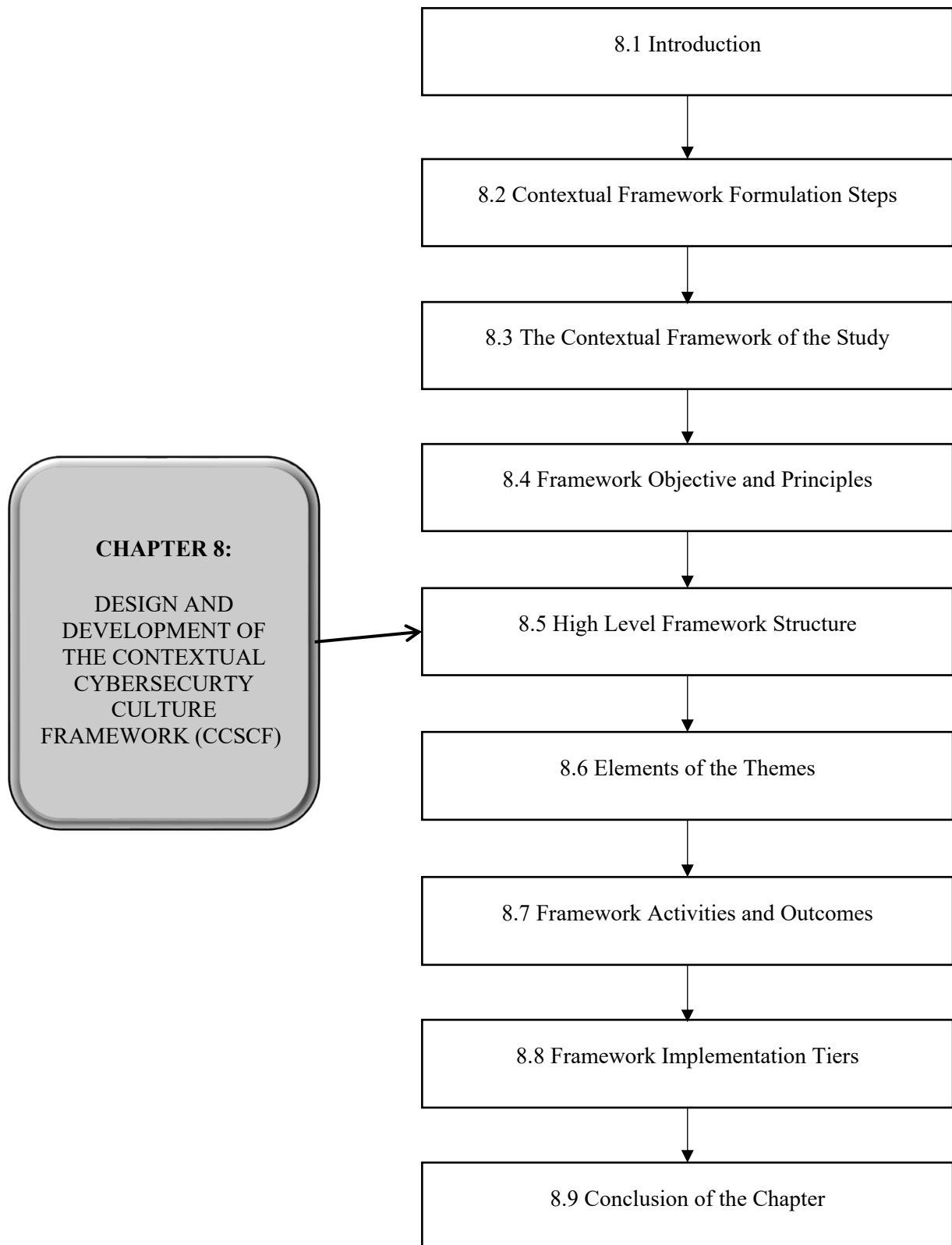
From the quantitative analysis, cybersecurity culture was found to be associated with all the constructs. Therefore, the five factors of cybersecurity culture were confirmed because the triangulation was made up of factors across various themes and constructs.

The study described in this chapter contributed to the body of knowledge by identifying cybersecurity culture factors related to five constructs and specific to the public E-Health institutions in the South African context. The findings implied that currently there was a weak cybersecurity culture in the investigated E-Health institutions and suggested a need for the establishment of a formal cybersecurity culture in the institutions. A formal cybersecurity culture could be achieved by focusing attention on certain management (M), preparedness (P),

responsibility (R), and technology (TECH) factors, including leadership, awareness, training and education, attitude, security behaviours, and the fast-changing nature of IT.

The next chapter will develop the contextual framework for cybersecurity culture in the public E-Health institutions in South Africa.

CHAPTER 8: DESIGN AND DEVELOPMENT OF THE CONTEXTUAL CYBERSECURITY CULTURE FRAMEWORK (CCSCF)



8.1 INTRODUCTION

This chapter focuses on the Research Sub-Question 5. The chapter discusses the design and development of the contextual framework for establishing a cybersecurity culture.

Research Sub-Question 5: *How can the identified factors be used to design and develop a contextual framework for establishing cybersecurity culture in public E-Health institutions in South Africa?*

In Chapter 4, a systematic review of the literature was conducted to investigate and provide a comprehensive list of factors associated with cybersecurity culture, as a way to address the human-related problems in cybersecurity. Chapter 4 also reviewed existing theoretical frameworks to reach a better understanding of the cybersecurity culture construct. Chapters 6 and 7 provided detailed information on the quantitative and qualitative results of the data collection. Therefore, based on outcomes from the three chapters preceding this one, the overall factors associated with cybersecurity culture have been identified and will assist with the CCSCF to be developed in this chapter.

This chapter is organised as follows: **Section 8.2** provides the contextual framework formulation steps. In **Section 8.3**, the contextual framework of the study is discussed. The framework objectives and principles are articulated in **Section 8.4**. This is followed by a presentation of the high-level framework structure (see **Section 8.5**). The elements of the framework themes, as well as the activities linked to each of the elements and outcomes, are discussed in **Sections 8.6** and **8.7**. Finally, **Section 8.8** explains the implementation tiers of the framework, and the chapter conclusion is in **Section 8.9**.

8.2 CONTEXTUAL FRAMEWORK FORMULATION STEPS

Chapter 5 outlined the conceptual framework analysis phases used to guide the design and development of the CCSCF for E-Health institutions. Conceptual framework analysis is a technique that describes processes and procedures for developing a conceptual framework based on grounded theory (Jabareen, 2009).

Reasons for adopting this technique in this study were its flexibility, modification capacity, and the fact that it focuses on understanding rather than just predicting (Jabareen, 2009). The flexibility advantage is also compatible with the pragmatic viewpoint of this study.

Figure 8.1 recaps the conceptual framework phases depicted in Chapter 4.

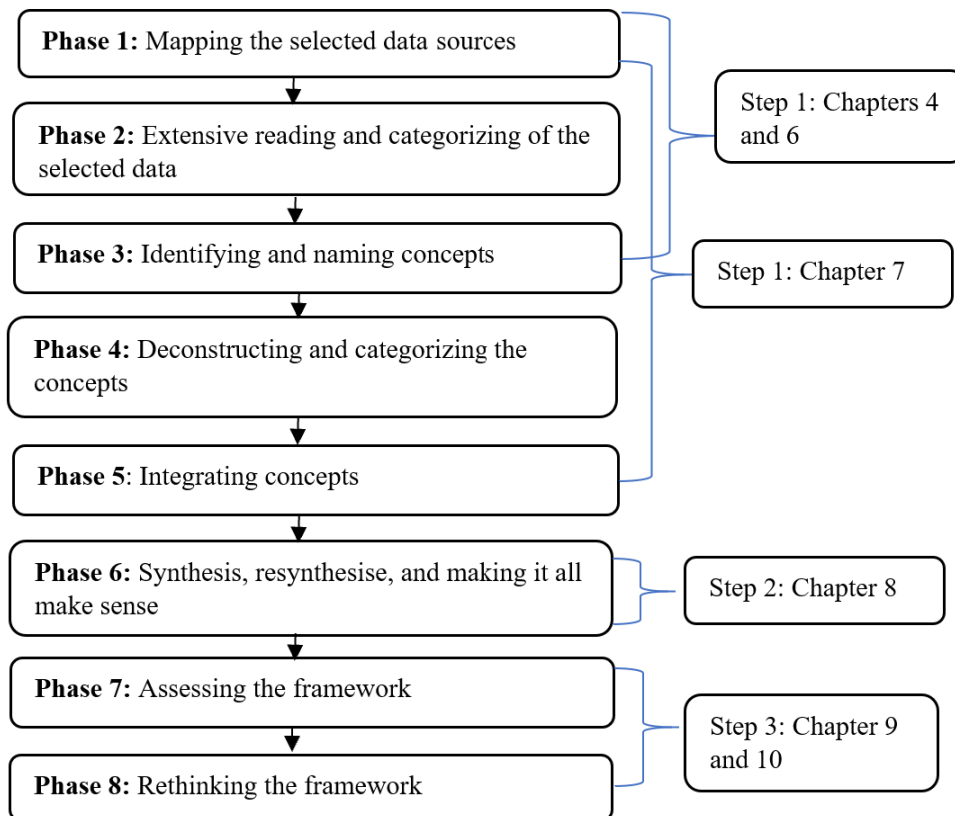


Figure 8.1: Phases of the Conceptual Framework Analysis (Adapted from Jabareen, 2009)

Figure 8.1 shows the different chapters that describe the processes carried out in the different phases of the conceptual framework analysis (grouped into 3 steps). The process and outcome of Step 2 (Phase 6) are covered in this chapter, which describes the design and development of the contextual framework. However, the last part of this **Section** provides an overview of the phases that have already been described in detail in the preceding chapters. These phases had to be completed before the design and development of the contextual framework could proceed.

PHASES 1 to 5 of the conceptual framework analyses re-visited:

- **Phase 1**

Mapping the data source for textual data was achieved in Chapter 4 with a database search and retrieval of 58 records. Additionally, the mapping of data sources for non-textual data was achieved in Chapters 6 and 7 with qualitative and quantitative data collection and analysis.

- **Phase 2**

Extensive reading and categorising of the data were accomplished by reading and re-reading through the selected records to identify cybersecurity culture definitions and constructs of existing cybersecurity culture frameworks (see Chapter 4). The data were processed according to the data sources from which they were obtained. The data from the systematic review were organised according to definitions, factors and framework (see Chapter 4), the collection and analysis of data from the questionnaire were described in Chapter 6, and the collection and analysis of data from the interviews were described in Chapter 7. The qualitative and quantitative data collected were analysed using suitable methods (see Chapters 4, 6 and 7).

- **Phase 3**

Identifying and naming concepts was described in Chapter 4. This required the important data (in the form of elements) to be highlighted in the definitions of cybersecurity culture. Additionally, several factors associated with the cybersecurity culture were found, and cybersecurity culture constructs were identified. In Chapter 6, using the total variances explained by the Exploratory Factor Analysis (EFA), cybersecurity culture factors seen from the perspective of system users were identified. Through the thematic analysis process (see Chapter 7), cybersecurity culture factors were identified from the perspective of ICT staff.

Phases 1 to 3 produce outcomes in the form of a list of competing and probably contradicting concepts (Jabareen, 2009). The list obtained from the literature review is presented in Table 4.2 and the list from public E-Health institutions can be seen in Table 7.9.

- **Phases 4 and 5**

Deconstructing and integrating the concepts was done by triangulating the data from the systematic literature review and from the quantitative and qualitative findings. The cybersecurity culture themes identified were modelled as a thematic diagram (see Chapter 7).

The development of the contextual framework started with the framework objectives and the introduction of the framework structure.

8.3 THE CONTEXTUAL FRAMEWORK OF THE STUDY

The proposed framework was the CCSCF for public E-Health institutions. CCSCF is a basic structure designed to guide stakeholders of public E-Health institutions on how the identified factors can be used to cultivate and manage cybersecurity culture.

The framework development process was based on: (1) knowledge gained from the examination of literature on existing frameworks (cybersecurity culture, HFD and STOPE), guidelines, definitions, and factors proposed by various authors (Alhogail et al., 2015; Da Veiga, 2019; ENISA, 2017; Georgiadou et al., 2020b; Huang & Pearlson, 2019; Leenen & Van Vuuren, 2019). (2) The analysis of surveys and interviews, qualitative data collected from studies on factors associated with cybersecurity culture in public hospitals (see Chapters 6 and 7).

8.3.1 THE CCSCF OVERVIEW DIAGRAM

The design and development of the overall framework, including an implementation plan, was achieved by completing the six segments depicted in the CCSCF overview diagram (see **Figure 8.2**). The overview diagram portrays how the framework's different parts fit together to create a holistic framework.

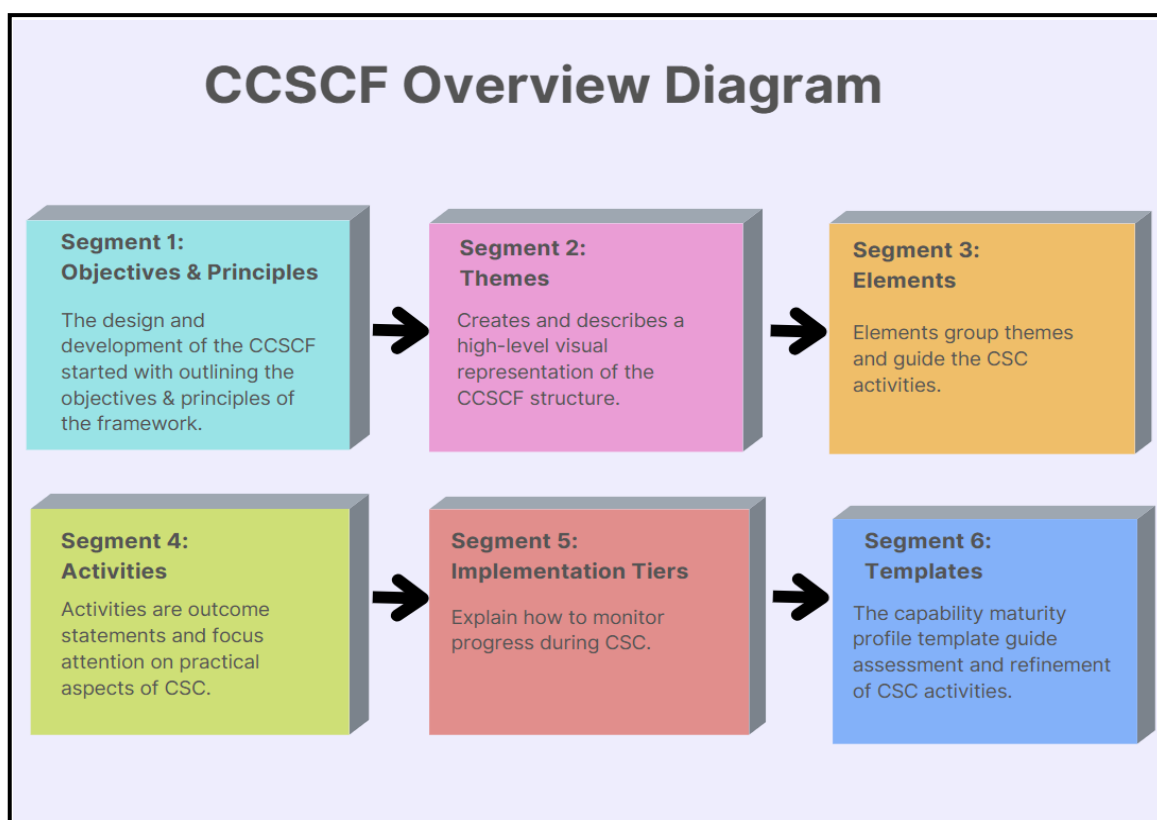


Figure 8.2: The CCSCF Overview Diagram (own source)

Figure 8.2 presents an overall view of the parts of the framework; this is intended to assist users in comprehending how the framework components fit together.

Achieving the six intermediate goals shown for the segments helps to ensure an adaptable, structured CCSCF with modular components and flexible templates, as seen in **Figure 8.2**.

8.3.2 THE SIX SEGMENTS OF THE CCSCF

This section will explain the six segments depicted in **Figure 8.2**.

Segment 1: The objective and principles. When this segment was completed, the structured mechanism that the proposed CCSCF aimed to achieve was presented. The segment identified the principles that guided framework development, such as the principle of a widely understood language.

Segment 2: The framework themes. When this segment was completed, a high-level framework structure highlighting the main themes that institutions should focus on when developing a cybersecurity culture was provided. The segment identified five core themes, namely internal organisation management (IOM), human preparedness (P) and responsibility (R), technology (TECH), and external environmental and non-organisational management (EENOM). The order of importance of the themes when developing cybersecurity culture in E-Health institutions was also indicated.

Segment 3: The elements. In this segment, the elements representing the factors each theme was comprised of were introduced. The elements of each theme are used to highlight different areas that the institution needs to pay attention to and achieve a strong cybersecurity culture.

Segment 4: Activities. This segment added framework activities and outcomes of the CCSCF. Segment 4 indicates that the activities and outcomes must be the focus of attention to meet the requirements of each element of each of the framework themes. Therefore, this segment required the activities to be defined and prioritised based on the thematic inquiry (see Chapter 7). In this segment, tables that linked the activities to relevant elements and themes were also developed.

Segment 5: The implementation tiers. This segment explained the National Institute of Standards and Technology (NIST) tiers as applied to monitor the degree of progress being made regarding the themes, elements and activities. The four implementation tiers represent unperformed, partially informed, repeatable and adaptive levels of success. The segment also indicates the concept of capability maturity level, which was introduced to monitor the framework performance regarding the activities of the themes.

Segment 6: The template. The segment shows how the capability maturity profile was used to develop a template institution can use to portray and enhance its cybersecurity culture activities. The segment shows a possible way of calculating an institution's current and intended capability profile and its associated maturity level, Capability Gap (CG), weight, and Priority (P) of an activity.

This section gave an overview of the CCSCF. The following sections provide detailed discussions of the different segments of the proposed framework.

8.4 THE FRAMEWORK OBJECTIVE AND PRINCIPLES

This section addresses segment one in the design and development of CCSCF (see **Figure 8.2**).

8.4.1 THE FRAMEWORK OBJECTIVES

Building on the insights and knowledge gathered from the literature (Chapter 4) and data collection (Chapters 6 and 7), the purpose of the CCSCF was to provide public E-Health institutions with a structured mechanism to:

- **Understand key themes and elements:** The CCSCF was intended to assist institutions in identifying core themes and associated elements necessary for establishing a robust cybersecurity culture tailored to their institutional context, and to understand the relationship between the themes.
- **Develop and outline activities:** The CCSCF was expected to help institutions to develop the activities required for achieving the various themes when developing a cybersecurity culture in an institution.
- **Identify concerns and issues:** The CCSCF should enable stakeholders to identify and prioritise the major concerns and issues in their institution related to cybersecurity.
- **Decide on the focus and target group:** The CCSCF was intended to assist institutions in deciding on the focus areas for cybersecurity culture development and the target groups for intervention efforts.
- **Leverage existing security structures:** The CCSCF should encourage institutions to capitalise on their existing security infrastructure and practices, while enhancing them to foster a culture of cybersecurity. The framework recommended complementing existing structures, practices and processes rather than replacing them.

- **Establish and manage Cybersecurity Culture:** The development of CCSCF provided a structure to serve as a guide for the establishment and management of cybersecurity culture initiatives by and with the institutions' stakeholders. It aimed to empower institutions to proactively prevent or to reduce cyber threat incidents in the long term by integrating cybersecurity into their organisational culture and operations.

By grounding the framework in the insights derived from existing literature and the survey data, the CCSCF ensured its relevance, credibility and applicability to the specific challenges faced by public E-Health institutions in cultivating a culture of cybersecurity. Although the CCSCF aimed to assist in establishing a strong culture of cybersecurity in public E-Health institutions, it is important to note that the framework may also be appropriate for use by private E-Health institutions and other organisations that intend to create a strong cybersecurity culture.

Nevertheless, the CCSCF is not a one-size-fits-all solution; how the framework can be used is likely to vary. This is because institutions are faced with unique cyber risks and threats due to the nature of their institution, the kind of ICT systems that apply to them, and the priority they place on cybersecurity. Since part of the framework structure was based on cybersecurity culture factors identified in the E-Health institutions used as cases, the framework context was particularly applicable in private and public hospitals. Any other institution that plans to adopt the framework needs to ensure it knows and understands the institution-specific contextual factors on which their framework needs to be based.

8.4.2 THE FRAMEWORK PRINCIPLES

The design and development of the CCSCF were guided by principles derived from insights obtained from existing theoretical frameworks (see Chapter 4) and practical data from studies on factors related to cybersecurity culture in public hospitals. The framework was anchored in principles which promote effectiveness, adaptability and ongoing refinement.

- Based on common and widely understood language

The CCSCF employed terminologies and concepts (the themes and elements, such as management, technology, cybersecurity awareness, attitude and security governance) that are common in literature, familiar, and were considered to be accessible to stakeholders in public E-Health institutions. This was important as employees would need to understand and use

codes associated with the elements and themes of the framework. This would help to facilitate clear communication and comprehension of cybersecurity culture objectives, concepts, guidelines and outcomes.

Using a common and generally understood language helped the diverse stakeholders (including ICT or cybersecurity professionals, medical practitioners, administrators, and policymakers) to comprehend, communicate and apply the CCSCF. This promoted alignment and collaboration across departments at all levels of the institution, enhancing the framework's usability and impact.

- Easy to understand and adaptable to other E-Health institutions

The CCSCF was designed to promote simplicity and flexibility. These should allow for easy customisation and adaptation to the contexts and requirements of various E-Health institutions beyond the initial development setting, even in different contexts. Recognising the various institutional structures, resources and levels of cybersecurity maturity in E-Health institutions, developing an easy-to-understand and adaptable framework would increase its relevance and applicability. This would promote widespread adoption and effective implementation, ultimately leading to improved cybersecurity culture outcomes in the healthcare sector.

- The CCSCF is a living document and was evaluated using a real-life participants' (stakeholders) dataset

The framework can be re-evaluated regularly and refined based on real-life datasets and feedback from participants, including those within public E-Health institutions and cybersecurity experts. This would help ensure its ability to respond to changing cybersecurity threats, challenges and organisational needs. Both Cybersecurity threats and healthcare environments are dynamic, which requires the framework to be continuously updated and refined to remain effective. By leveraging real-life participant data, such as cybersecurity incident reports, staff feedback, expert opinions, and performance metrics, the CCSCF could be continuously improved to address emerging threats, optimise resource allocation, and reduce overall cybersecurity incidents.

- It is directed by academics and public E-Health institutions

The development and evolution of the CCSCF were guided by collaboration between academic experts and stakeholders from public E-Health institutions, ensuring alignment with research, industry best practices, and the practical insights from E-Health employees. By including these

key stakeholders in the framework's development, the CCSCF benefited from diverse perspectives, interdisciplinary expertise and collective ownership. This approach fostered acceptance, credibility and sustainability, driving continuous improvement and innovation in the management of cybersecurity culture within the healthcare sector.

Accommodating these principles in the design, development and evaluation of the CCSCF enhanced its usability, relevance and effectiveness as a guiding framework for cultivating and managing cybersecurity culture in public E-Health institutions.

8.5 HIGH-LEVEL FRAMEWORK STRUCTURE

In alignment with the conceptual framework analysis (see Chapter 5), the design and development of the CCSCF were covered in Phase 6 of the conceptual framework analysis.

Since the purpose of this chapter is to synthesise and integrate the cybersecurity culture themes and factors into a cohesive framework, it can be used to guide public E-Health institutions in establishing a cybersecurity culture. **Figure 8.3** gave a high-level view of CCSCF. The provision of a high-level structure of the CCSCF was covered by the second segment in the overall framework overview diagram.

As the high-level framework structure was guided by CCSCF principles, it was designed:

- To be clear and simple to ensure it was accessible and understandable to stakeholders across public E-Health institutions;
- To be adaptable to different E-Health institutions, allowing for customisation to suit unique contexts and requirements;
- To evolve, based on real-life participant data and feedback, to ensure that the framework was able to remain relevant and to respond to the changing needs of the institution as well as emerging cybersecurity threats and challenges; and
- As a collaboration between academic experts and stakeholders from public E-Health institutions.

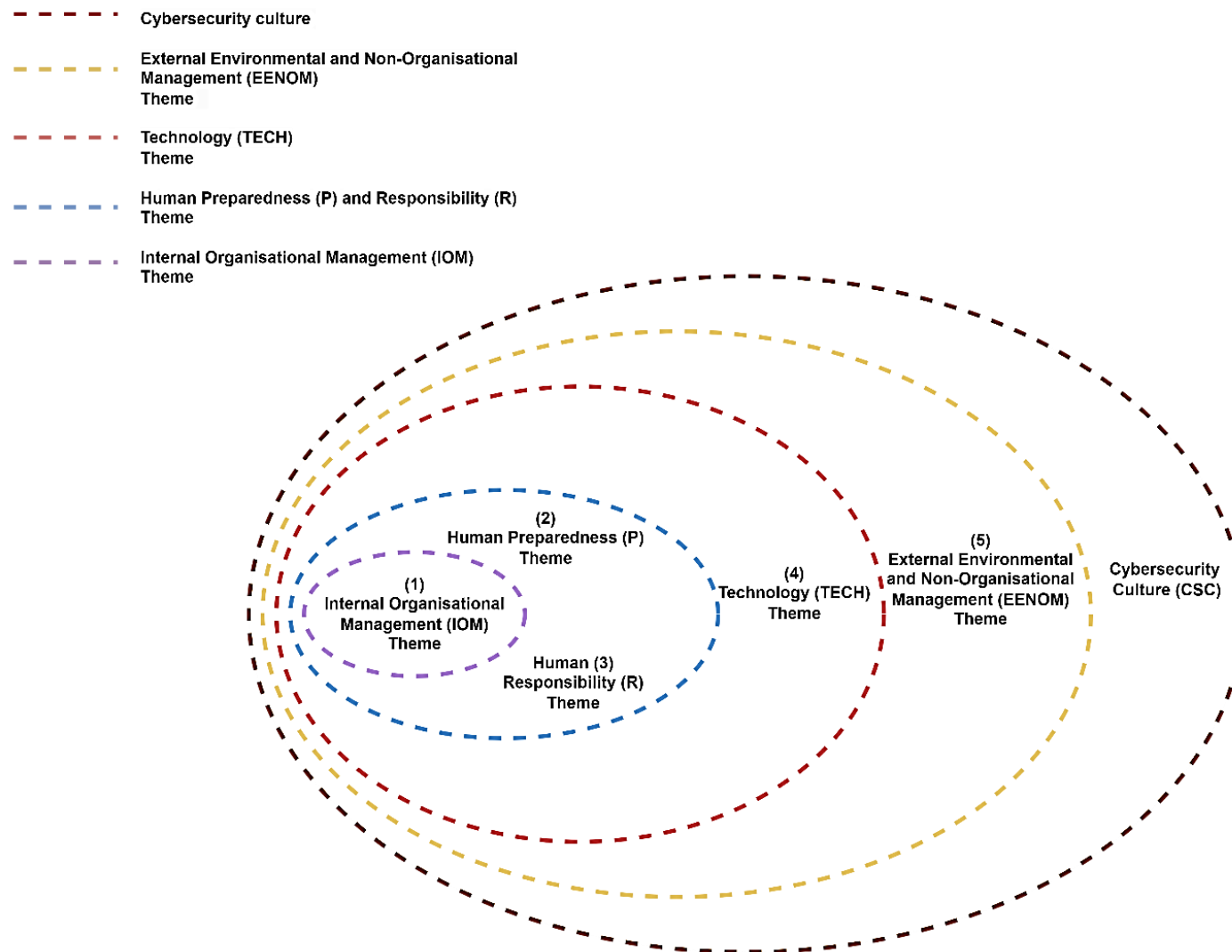


Figure 8.3: The CCSCF Themes (own source)

Hence, the framework structure needed to be consistent with the framework objectives for understanding the key themes outlined in **Section 8.5**.

Figure 8.3 provides a high-level view of the framework, which is intended to help users understand the order of the five theme layers that make up the framework.

Figure 8.3 shows that there are five main themes that public E-Health institutions should pay attention to when establishing a cybersecurity culture. The themes have been represented as layers like an onion, to show their priority in the development of cybersecurity culture. For effective and complete development of cybersecurity culture, all the themes need to be considered.

The layer labelled (1) is the theme of internal organisation management (IOM) (see **Figure 8.3**). It is the dominant theme in the development of a cybersecurity culture as it: (a) plays a substantial role in the literature, (b) correlates with and influences other themes; and (c) is prominent in the research findings as seen in the preceding chapters.

Human preparedness (P) and responsibility (R) are labelled (2) and (3) respectively. The human preparedness (P) and responsibility (R) themes are depicted as a single layer of the framework because they were jointly used to depict the people part of the framework and human characteristics, such as skills, behaviour, and attitudes. These human characteristics are those of employees in the institution and include employees at the organisation management level.

Human preparedness (P) and responsibility (R) were modelled as immediate themes to internal organisation management (IOM) due to the close association and the influences the themes have on each other. Additionally, human preparedness (P) and responsibility (R), and internal organisation management (IOM) were all originally considered to be internal themes, as they are mainly influenced by factors inside the institution and behavioural factors.

The layer labelled (4) is the technology (TECH) theme. This theme is viewed in the framework as an intermediate theme because it is situated between internal and external themes. TECH theme was placed between these two themes because it influences but can also be influenced by factors internal to the organisation and factors in the external environment of the organisation. The layer of the framework labelled (5) indicates the external environmental and non-organisational management (EENOM) theme. This was considered to be an external theme because it is mostly influenced by factors outside of the institution.

The core themes of the CCSCF can be associated with the three pillars of cybersecurity, namely people, processes, and technology. The people pillar has characteristics similar to the human preparedness (P) and responsibility (R) themes, the process pillar represents the internal organisation management (IOM) theme, and the technology pillar clearly is associated with the technology (TECH) theme. However, the CCSCF identified an additional theme, namely the external environmental and non-organisational management (EENOM) theme.

Developing a successful cybersecurity culture requires the cooperation of all employees of the institutions, including management (junior and senior). This means that the five core themes of the CCSCF are interrelated and should work collectively towards a common goal, which is to assist public E-Health institutions with the development and management of cybersecurity culture. This would, in the long run, help preserve critical assets of E-Health institutions from experiencing incidents of cyber threats.

The comprehensive exploration of the CCSCF themes introduced in this section begins with **Section 8.6**.

8.6 ELEMENTS OF THE FRAMEWORK

This section represents the third segment of the proposed framework (see **Figure 8.2**). Each theme of the CCSCF serves as an umbrella term used to categorise the different elements associated with cybersecurity culture. The elements are the consolidated factors identified in the literature and in the context of public E-Health institutions via quantitative and qualitative data. Therefore, the terms factors and elements are used interchangeably in this study. The CCSCF themes act as a link that facilitates the execution of crucial activities necessary to cultivate a strong cybersecurity culture in public E-Health institutions.

The elements linked to each theme layer denote the different areas that public E-Health institutions need to focus their attention on, or to leverage their effort to establish a cybersecurity culture. The elements discussed in this section should be incorporated to create an effective multifaceted barrier against cyber threats and crimes in public hospitals. The different framework themes and their elements are discussed in **Sections 8.6.1 to 8.6.4** starting with cybersecurity culture and followed by the layers labelled 1 to 5.

8.6.1 CYBERSECURITY CULTURE (CSC)

This research focuses on cybersecurity culture at the organisational or institutional level. In order to build a strong cybersecurity culture at an institutional level, it must be made an integral part of the organisational culture. This suggests that cybersecurity culture should be a clearly defined part of the organisational culture. Considering the changing nature that characterises organisations, cybersecurity culture needs to be continually updated as its implementation and adoption must be sustained.

In CCSCF (see **Figure 8.3**) the first two layers (internal organisation management (IOM), human preparedness (P), and responsibility (R)) represent internal themes and have bidirectional associations with cybersecurity culture and the other layers. This means that the themes can influence cybersecurity culture and can also be influenced by both the external factors and the factors of the technological theme. Therefore, internal organisation management (IOM), human preparedness (P), responsibility (R), technology (TECH), and external environmental and non-organisational management (EENOM) are considered important themes in the establishment of cybersecurity culture.

8.6.2 INTERNAL ORGANISATIONAL MANAGEMENT (IOM) ELEMENTS

The Internal Organisation Management (IOM) theme describes elements and provides guidelines for the actions and steps of management within the boundaries of the organisation to ensure a strong culture of cybersecurity. The elements of the internal organisation management (IOM) theme depicted in **Figure 8.4** include leadership, business continuity, security governance, communication channel, organisational learning and physical security. These factors need to be in place in building a cybersecurity culture.

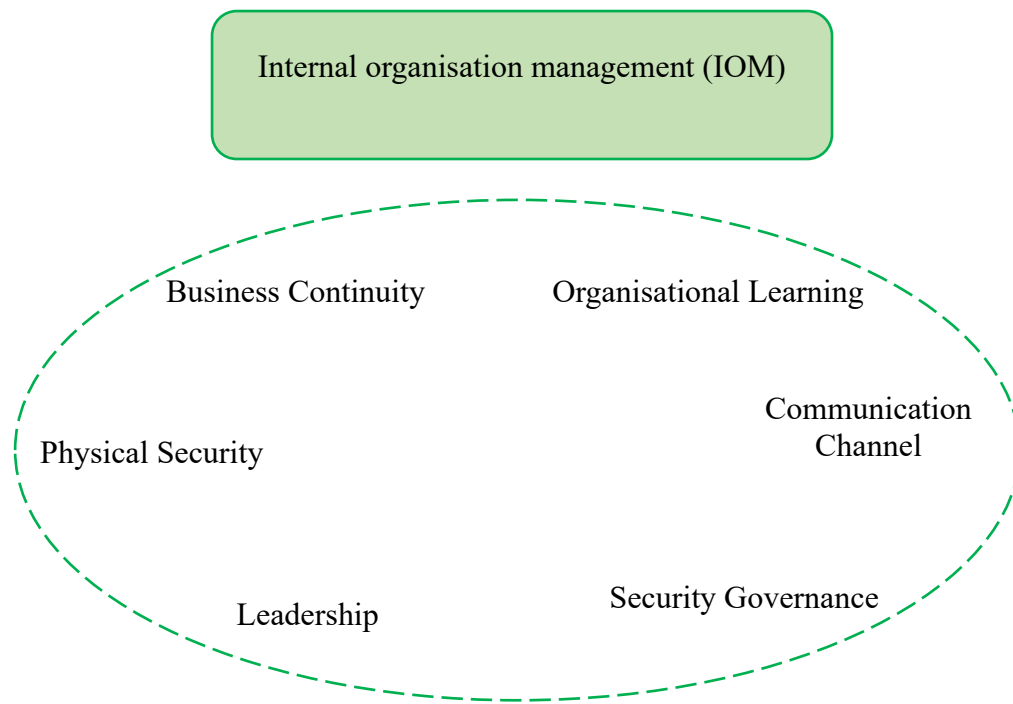


Figure 8.4: IOM Theme Elements (own source)

Figure 8.4 indicates the individual elements of the IOM theme as the first layer of the CCSCF.

The identified internal organisation management (IOM) factors are grouped into six elements. These elements also include the essential activities of other factors not depicted here. The associated activities were developed from codes that explained the factors. The associations and groundedness values of each code played a crucial part in determining the necessity of the code and its inclusion in the factor activities.

Codes with negative associations are seen as more important than those with positive associations because they are considered to be needed but lacking in the institution. For example, in the business continuity factor, negative codes related to “lack of continuous vulnerability management activities” and “no contingency plan” are more important than the positive code “existence of disaster recovery plan”. These two negative codes are integrated with the risk assessment negative code to represent business continuity element as depicted in **Figure 8.4**. This helps to reduce the number of activities for each element that is considered to be important to a reasonable number. These elements represent groups of activities performed by management at different levels in the internal organisation.

The action of identifying and discussing the elements of internal organisation management (IOM) helps to achieve the CCSCF requirements of understanding key elements and

identifying internal management concerns and issues regarding cybersecurity culture. The two objectives of deciding on the focus and target groups and leveraging the existing security structure are also satisfied by this action because these objectives require effective management and leadership. Addressing the need for top-level support and involvement in cybersecurity culture establishment, ensuring leadership commitment and direction.

The action of recognising and deliberating on the elements of internal organisation management (IOM) aligns with all four principles of the framework. The elements of the IOM theme are common terms and concepts in the literature on cybersecurity culture, and the public hospital staff are familiar with them. The data collected for the identification of the elements of the IOM involved real-life data sets from participants in the public E-Health institutions.

The six elements (organisational learning, leadership, communication channel, cybersecurity governance, business continuity, physical security) (see **Figure 8.4**) are critical in building a cybersecurity culture as explained below. The research finding that led to the identification of the IOM elements can be traced back to the quantitative data analysis as described in Section 6.5.6 and the qualitative data analysis as described in Section 7.5.

Organisational learning serves as a process for achieving purpose-driven cybersecurity-related learning (skills acquisition) at various levels (individual, team and organisational) of the institution. It is aimed at helping employees acquire, interpret, retain and distribute cybersecurity knowledge and information continuously to help create and manage the cybersecurity culture of the institution.

Leadership addresses the need for top-level support and involvement in cybersecurity culture development, ensuring leadership commitment and direction. The top leadership of any institution has the ultimate authority needed to influence the process of creating a strong cybersecurity culture, and the activities or actions of the top management provide essential support for this.

Essential leadership actions are providing financial support, management interest and involvement, and having a dedicated cybersecurity culture champion or team. The absence of top leadership in supporting such factors can make it challenging to create a cybersecurity culture in public E-Health institutions.

Communication channel facilitates effective communication of cybersecurity policies, messages and incident reporting within the institution. It helps provide methods and networks

through which the institutions can accurately and properly communicate cybersecurity messages and policies, report cyber-attack incidents, and share cybersecurity information within the institution.

An institution that uses the appropriate channels to share correct cybersecurity information with the right members of the institution communicates successfully. Hence, the quality of communication channels used for sharing and discussing cybersecurity-related issues plays an important role in building a cybersecurity culture. Communication channels include both formal and informal channels to accommodate diverse members of the organisation.

Cybersecurity governance assists institutions in establishing a cybersecurity culture to effectively plan, manage, protect and improve their assets, that is, their data and information, ICT systems, including software, and people, who are staff and patients. Through the activities of cybersecurity governance, institutions establishing a cybersecurity culture can monitor and check the compliance of their cybersecurity practice with standards, policies and regulatory requirements.

Usually, the factors of compliance, monitoring, policy and cybersecurity governance are viewed separately according to the cybersecurity culture Model dimensions (Georgiadou et al., 2020a; 2020b; Georgiadou et al., 2021a). However, based on the CCSCF developed in this study, the factors were combined and treated as part of cybersecurity governance. Hence, the activities of cybersecurity governance can be broadened to include monitoring, compliance and policy.

The absence of cybersecurity governance in an institution would mean that there is no plan to build, manage, monitor or enhance cybersecurity practices for the implementation of standards and compliance with them. This would make it challenging to create a cybersecurity culture.

Good cybersecurity governance requires a robust cybersecurity policy which provides a clear definition and clarification of cybersecurity rules, regulations, policies and procedures. These are fundamental for building a cybersecurity culture in an institution. Furthermore, the cybersecurity policy must define the responsibilities of staff members regarding cybersecurity and may provide details of wider security issues, such as information security, as well as details of privacy and data protection.

To establish a strong cybersecurity culture in public E-Health institutions, it is vital that there is a well-designed, properly communicated and understood cybersecurity policy as part of the security governance element.

Business continuity ensures the continuity of critical business functions and operations in the event of cyber-attack incidents. Creating a culture of cybersecurity requires preparing the processes, plan, tools and actions to follow, to allow proper backups of important information to be made and to be available to resume and recover operations in case of interruption due to cyber-attack incidents.

To ensure business continuity, risk assessment needs to be done properly, and people should understand its purpose. Risk assessment and managing is important in implementing a cybersecurity culture as it helps the organisation assess, understand and map the security measures of the security team by means of established processes.

This was recognised as a significant function in the creation of CCSCF due to the criticality of healthcare institutions and the impact downtime has on the lives of patients, their operations, and the reputation of the institution. Therefore, in the development of CCSCF, business continuity was used to outline how the E-Health institutions planned to ensure the continuity of critical business functions and to recover crucial business information in the event of cybersecurity threats and attacks.

Physical security is needed to create a proper cybersecurity culture, and well-established asset control measures are required for active management of the security of physical and other facilities.

In summary, under the internal organisation management (IOM) theme, institutions must have a process of equipping staff at all levels with the necessary cybersecurity skills in order to develop a cybersecurity culture. The institution's leadership should provide the necessary support, such as appointing a cybersecurity culture champion and providing sufficient financial resources. In addition, appropriate communication channels for disseminating cybersecurity information need to be established.

There is a need for a comprehensive cybersecurity policy that guides the development and maintenance of a strong cybersecurity culture and security governance that assists with asset planning and management. Finally, the institution must ensure proper security and have plans in place to ensure business continuity in case of cyber-attack incidents.

8.6.3 HUMAN PREPAREDNESS (P) AND RESPONSIBILITY (R)

The themes of human preparedness (P) and responsibility (R) represent the human characteristics of the hospital staff that influence the cybersecurity culture of their institution. In the CCSCF, the crucial factors of human preparedness (P) and responsibility (R) together represent the organisational culture. Representing organisational culture with the elements of these constructs was done to make cybersecurity culture an integral part of the organisational culture of public E-Health institutions. Organisational culture denotes the shared practices and beliefs of the institution members that affect their cybersecurity behaviour and actions inside the institution.

Figure 8.5 summarises the human preparedness (P) and responsibility (R) theme elements of CCSCF.

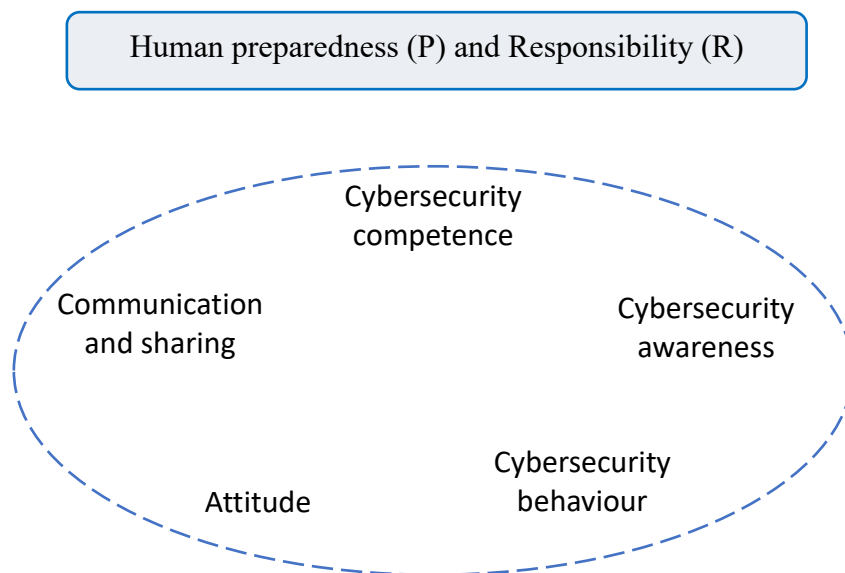


Figure 8.5: Human Preparedness (P) and Responsibility (R) Themes Elements (own source)

The elements of the human preparedness (P) and responsibility (R) theme depicted in **Figure 8.5** show the essential cybersecurity factors that E-Health institutions need to discuss with their employees as they prepare for and develop a cybersecurity culture.

The elements of human preparedness (P) are factors of cybersecurity culture in terms of individual competencies and skills. The elements of human responsibility (R) relate to factors in terms of individual behaviours, attitudes, values and beliefs, which are the basis of the unwritten rules of an organisation. Recognising and discussing human preparedness (P) and responsibility (R) elements achieves the requirement for developing an understanding of key

elements of the framework. By emphasising the importance of staff human preparedness (P) and responsibility (R) actions, the framework also addressed the objective of identifying the staff members' main concerns and issues with respect to the development of cybersecurity culture. This assists the target group in reaching decisions regarding what the cybersecurity actions should focus on. The requirement of establishing better management of cybersecurity among institutional stakeholders is also accommodated, which helps to prevent or reduce cyber threats in the long term.

Furthermore, the discussion of the elements of human preparedness (P) and responsibility (R) supports all the principles of the framework. For example, the elements of human preparedness (P) and responsibility (R) framework are common and widely understood because the concepts are shared in the literature and are familiar to the staff, easily understandable and adaptable as the elements can be customised and adapted to the unique settings, and real-world participants were used for the data set.

The elements of human preparedness (P) and responsibility (R) themes displayed in **Figure 8.5** are discussed in the subsequent sections.

8.6.3.1 Human preparedness (P) elements

According to **Figure 8.5**, the factors of human preparedness (P) that were considered critical in the CCSCF include cybersecurity competency (comprising training and education, as well as knowledge), cybersecurity awareness, and communication and information sharing. All the human preparedness (P) factors identified in this study are integrated into the factors discussed in this section because the activities of other factors are contained in one way or another in the factors discussed here.

The three elements of human preparedness (Cybersecurity awareness, Cybersecurity competency and Communication and information sharing) are crucial in establishing cybersecurity culture. The research results that led to the identification of the human preparedness elements can be traced back to the quantitative data analysis as described in **Section 6.5.6** and the qualitative data analysis as described in **Section 7.5**.

Cybersecurity awareness contributes to building a strong cybersecurity culture by creating an awareness programme that is used to assess how well employee know, comprehend, and can recognise issues and solutions related to cybersecurity in general and in the context of their institution.

In establishing a culture of cybersecurity, creating an awareness programme as an element of CCSCF can be used to educate and train staff on cyber threats and cybersecurity practices of their institutions. This empowers them to take positive action toward ensuring cybersecurity, assists with creating cybersecurity consciousness among employees, encourages employee compliance with their institution's cybersecurity practices, policies and promotes cybersecurity.

Attention to training and education is important at both the management and individual levels of an institution. On the one hand, the management of institutions must create an enabling environment for cybersecurity training and education, and on the other hand, employees need to show commitment and make themselves available for the training.

Cybersecurity competency identifies, defines and documents the current and future skills, abilities and knowledge of E-Health employees regarding cybersecurity. Cybersecurity competency can be achieved by offering courses and formal and informal exercises to help staff members with the acquisition of cybersecurity knowledge and skills.

Communication and information sharing serve to educate, update and keep employees' consciousness of cybersecurity issues threatening their institution.

This element can help create an enabling environment where cybersecurity responsibilities can be discussed with role players, and feedback can be received from the different stakeholders. Information sharing with the stakeholders, through formal security structures and a steering committee, allows the sharing of knowledge of potential cyber threats and vulnerabilities.

8.6.3.2 Human responsibility (R) elements

The human responsibility (R) elements are covered by attitudes and security behaviour (see **Figure 8.5**). These two elements of human responsibility (R) are discussed below. Likewise, in IOM and human preparedness, other human responsibility (R) factors not depicted in **Figure 8.5** are integrated in the factors discussed in this section by incorporating the essential activities of the factors. The research results that led to human responsibility elements can be traced back to the quantitative data analysis as described in Section 6.5.6 and the qualitative data analysis as described in Section 7.5.

Attitude is used to assess the feelings, perceptions and beliefs of employees (both management and non-management) towards cybersecurity in general, including the cybersecurity practices and issues of their institution.

This element is also used to evaluate employees' satisfaction with the cybersecurity practices exhibited by their institutions that have a direct impact on the cybersecurity attitude of colleagues who directly influence them (negatively or positively).

The attitude of employees, particularly top management's attitude toward cybersecurity, can be an indication of the importance that the institution places on cybersecurity in its core operations. Where security is considered essential in an institution, its employees make it a priority.

The nature and purpose of healthcare institutions have a direct impact on the priority that the institutions and their employees place on the activities of the institution. The institutions tend to focus their attention entirely on the central purpose of their existence, which is to provide healthcare to patients. As a result, the institutions may pay insufficient attention to cybersecurity issues, thereby making it difficult to maintain cybersecurity.

Cybersecurity behaviours. This factor assesses employees' daily intentional and unintentional cybersecurity activities and actions that can have a positive or negative impact on the general cybersecurity outlook of the institution. The factor evaluates employees' cybersecurity-conscious behaviour in their institution.

From the perspective of human preparedness (P) and responsibility (R), developing cybersecurity culture in E-Health institutions must start with a full understanding of how prepared the institutions are in terms of their employee's knowledge and awareness of cybersecurity. Institutions also need to assess whether the employees will act responsibly, by understanding their attitudes, actions and behaviours toward the organisation's mandate and cybersecurity practices.

Knowledge and awareness are created by providing members of staff with training and education, in addition to other ways of communicating and sharing cybersecurity information. Ensuring access to relevant information can help to change the mindset, attitude and behaviours of employees and will make employees less resistant to change. Hence, the employees would be more inclined to change old security practices.

8.6.4 TECHNOLOGY (TECH) ELEMENTS

Establishing a cybersecurity culture in public E-Health institutions needs to accommodate the three elements: ICT infrastructures, frequent changes in ICT, and outsourcing of ICT systems

(see **Figure 8.6**). This will contribute to achieving the objective related to the understanding of key CCSCF themes and elements.

The TECH theme is positioned as an intermediate theme between the internal and external factors, as there are elements of technology that fall into both. This theme acknowledges the influence of technology on cybersecurity culture and hence aligns with the objective of identifying technological concerns and issues related to achieving a culture of cybersecurity and leveraging existing security structures and practices while also adapting processes to align with technological advancements. The technology (TECH) elements discussed here accommodate the fundamental principles of CCSCF.

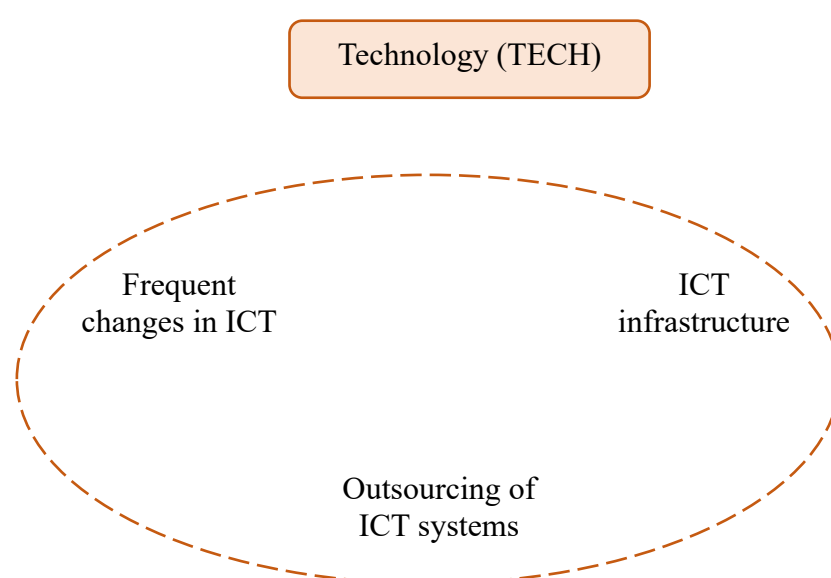


Figure 8.6: Technology (TECH) Theme Elements (own source)

Figure 8.6 outlined the three technology (TECH) elements (ICT infrastructure, Outsourcing of ICT systems and Frequent changes in ICT) that characterised Technology. The findings that guide the technology (TECH) elements can be traced back to the quantitative data analysis as described in Section 6.5.6 and the qualitative Section 7.5. These are discussed below.

ICT infrastructure assists with the assessment, documentation and management of the technologies that E-Health institutions use to enable their daily operation. A strong cybersecurity culture cannot be created unless the ICT infrastructure and technologies that will support cybersecurity practice and activities of the institution are protected; otherwise, the effort made and responsibility shouldered by people regarding cybersecurity is wasted. Lack of or insufficient ICT infrastructure will result in the institution having outdated technology.

Outsourcing of the ICT system is used to employ and manage the resources of external third parties that assist with the institution's cybersecurity operations. Outsourcing ICT systems can help E-Health institutions achieve a cybersecurity culture by giving them access to specialised cybersecurity knowledge and related ICT systems and security tools. Such entities would monitor the IT systems outsourced to them to ensure they conform to the E-Health sector's standards. However, the outsourcing of IT systems can also negatively impact the achievement of a cybersecurity culture. This happens when the outsourced entities are not experts, cannot provide the essential experience or security tools, and cannot undertake consistent monitoring of the institution's cybersecurity.

Frequent changes in IT are an important factor. Due to the dependence of healthcare institutions on ICT systems, establishing a strong cybersecurity culture requires conscientious monitoring and management of the rapidly changing technology that might have an impact on the ICT systems of the institution. Awareness of changes in ICT contributes to the cultivation of a cybersecurity culture because it prompts institutions to acquire ICT devices and processes that are capable of managing and countering the changing cyber threats, thus maintaining a robust cybersecurity culture in the institution.

8.6.5 EXTERNAL ENVIRONMENTAL AND NON-ORGANISATIONAL MANAGEMENT (EENOM) ELEMENTS

The external environmental and non-organisational management (EENOM) theme encompasses factors arising from the external environment which are beyond the control of the organisation. How prepared and responsible public E-Health institutions are, and their internal management practices, depend to some extent on external environmental and non-organisational management (EENOM) factors. The CCSCF highlighted rules and regulations, the hospital location, legal aspects and litigation, natural culture and reputational damage as important elements of this theme (see **Figure 8.7**).

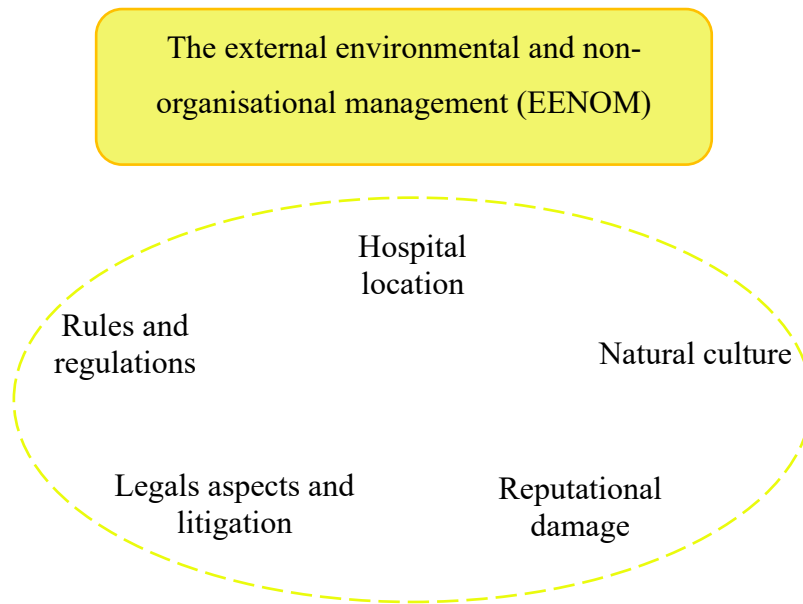


Figure 8.7: EENOM Theme Elements (own source)

Figure 8.7 is intended to help users obtain an overview of the EENOM theme elements. An understanding of how the elements of EENOM were generated can be obtained by referring back to a description of the quantitative data analysis (see Section 6.5.6) and of the qualitative (see Section 7.5). These are discussed below.

By considering these external environmental factors, the framework addresses the objective of understanding key themes and elements required to establish a culture of cybersecurity for the institution. Additionally, knowledge of these factors helps with addressing the requirement of identifying environmental concerns and issues in relation to building a culture of cybersecurity. In line with all the elements of internal organisation management (IOM) themes, the external environmental and non-organisational management (EENOM) theme also aligns with the principles of common and widely used language, easy understanding and adaptability, living documents with real-life data sets, and being directed by academics and public E-Health institutions.

Rules and regulations, the role of this element in establishing cybersecurity culture includes checks and keeping track of mandates from external bodies like government; industry-related laws, regulations and guidelines related to the institution's information management; encouraging legal compliance; and promoting data protection by ensuring accountability among role players. All of these will ultimately improve the reputation of the organisation.

Legal aspects and litigation are a critical factor of CCSCF in the development of cybersecurity culture, as it creates awareness among employees of the institution and other stakeholders about medical claims-related risks.

The legal aspects and litigation were found to be a challenging factor for the security of E-Health data in the context of a South African public E-Health institution. This challenge can encourage institutions to establish a cybersecurity culture to minimise the risk of medical lawsuits against the institution.

Hospital location is another factor that influences the cultivation and management of cybersecurity culture in public E-Health institutions. This is because the location of a hospital can affect its ability to collaborate and share information with other healthcare institutions and external stakeholders. This can have an impact on their available resources, including finances and the availability of cyber experts, which will ultimately affect the cultivation of cybersecurity culture in the institution.

National culture includes the norms, values, beliefs and customs that are shared by a society or country. National culture emerged in the literature and from the data collected as a factor that plays a large role in creating a strong cybersecurity culture. It influences the beliefs, perceptions, and attitudes of staff towards the cybersecurity goals of confidentiality, integrity, and availability (CIA) in an institution. Therefore, for E-Health institutions to create a strong cybersecurity culture, there is a need to understand and accommodate cultural diversities that might motivate or discourage the expected security behaviour of their staff.

Reputational damage results from a lack of trust in the ICT systems used for E-Health by individuals and communities. Reputational damage emerges from cyber-attack incidents experienced by institutions due to poor implementation of cybersecurity measures. It can portray a healthcare institution as one that does not adhere to ethical healthcare practices. To address the issue of reputational damage, E-Health institutions need to consider the creation of a cybersecurity culture as a critical task and invest seriously in cybersecurity activities and practices of the institution.

Having discussed the themes of the CCSCF and the elements attributed to the themes, the following section concludes the theme components by outlining the possible activities required for each element to achieve the CCSCF themes.

8.7 FRAMEWORK ACTIVITIES AND OUTCOMES

According to **Figure 8.2**, framework activities and outcomes are represented by the fourth segment in the overall design, development and implementation of the CCSCF. The framework themes are realised by the actual performance of a collection of targeted activities and outcomes grouped to ensure the achievement of the different elements to establish a cybersecurity culture. The CCSCF themes were designed to facilitate the execution of crucial activities required for the establishment of a strong cybersecurity culture in public E-Health institutions.

This section has detailed the activities required under each framework element to achieve a culture of cybersecurity. To avoid including a long list of tables in the main part of this thesis, the activities can be seen under APPENDIX_5. The activities were determined predominantly by considering the factors that emerged from the code statements of each element in the thematic analysis of Chapter 7 in relation to factors identified in Chapter 6. To ensure comprehensiveness of the activities generated from the code statements, they were sometimes compared with the activities of similar cybersecurity culture factors in the literature.

The ranking of the activities was done using groundedness (G) from the thematic results of the codes statement according to the qualitative analysis. For example, activities of an element with the most negative value were ranked first, and those related to the highest positive value were ranked last. A positive value identifies the factors that the institutions and their staff are implementing, but these may still need improvement. A negative value signifies factors that are definitely deficient in terms of implementation, though the institution may have recognised the need for the factor and its importance. A negative value is also used to make visible cybersecurity culture concepts and associated threats recognised by the institution, but that are unknown to its stakeholders. A negative value (particularly a high negative value), therefore, signifies the urgency of implementing and making the importance of factors known.

On a similar note, ranking the priorities of the framework elements (as shown in column 2 of Table 8.1 to Table 8.7) were done using the total groundedness (G) value of each element. The element or elements with the highest negative total groundedness (G) value are given a priority ranking of 1, while the element with the highest positive groundedness (G) value is indicated to be least urgent and placed last in the list. The total groundedness (G) of an element is the sum of all the groundedness (G) values. The idea of using a number of code connections was adopted from the use of respondent numbers (Jääskeläinen & Roitto, 2015).

Table 8.1, and Table 8.3 to Table 8.7 summarise the themes and elements of the framework in a Table using a unique identifier (ID) together with the reference number of related activities. The ID was developed as a combination of the theme's first letters together with the associated element's first letters. For example, IOM_L is used to identify the leadership element of the internal organisation management (IOM) theme. The ID is used as a tool to link a framework theme and its elements to the activities required to achieve it.

The development of the activities (see APPENDIX_5) required for the achievement of CCSCF elements addresses the objectives of developing and describing activities, identifying concerns and issues, as well as leveraging existing security structures.

8.7.1 IOM ACTIVITIES

The activities that were found to be critical to assisting E-Health institutions to achieve their purpose in the internal organisation management (IOM) theme were detailed in APPENDIX_5A. Table 8.1 summarises elements of the internal organisation management (IOM) theme with the corresponding activities reference numbers that link the elements to the activities in APPENDIX_5A.

Table 8.1: Internal Organisation Management (IOM) Elements and Related Activities

Theme: Internal Organisation Management (IOM)		
Elements	ID	Activity ref no
1. Leadership	IOM_L	IOM_L (1)
		IOM_L (2)
		IOM_L (3)
		IOM_L (4)
		IOM_L (5)
		IOM_L (6)
		IOM_L (7)
		IOM_L (8)
		IOM_L (9)
2. Cybersecurity governance	IOM_CSG	IOM_SG (1)
		IOM_SG (2)
		IOM_SG (3)
		IOM_SG (4)

Theme: Internal Organisation Management (IOM)		
Elements	ID	Activity ref no
		IOM SG (5)
		IOM SG (6)
		IOM SG (7)
		IOM SG (8)
		IOM SG (9)
3. Business continuity	IOM_BC	IOM BC (1)
		IOM BC (2)
		IOM BC (3)
		IOM BC (4)
		IOM BC (5)
		IOM BC (6)
4. Organisational learning	IOM_OL	IOM OL (1)
		IOM OL (2)
5. Physical security	IOM_PS	IOM PS (1)
		IOM PS (2)
		IOM PS (3)
6.Communication channels	IOM_CC	IOM CC (1)
		IOM CC (2)
		IOM CC (3)

Table 8.2 uses only two of the leadership activities shown in Table 8.1, namely “activity ref no”, IOM_L_ (1) and IOM_L_ (2) to provide examples that make it easy to follow and interpret the activities tables in APPENDIX_5A to 5D.

Table 8.2: IOM Relation Example of Activity Ref No Column and Activities

Theme: Internal Organisation Management (IOM)			
Elements	ID	Activity ref no	Activities
1. Leadership	IOM_L	IOM_L_ (1)	(1) Develop (example through keeping records of CS incidents) the interest and attention of top leadership in cybersecurity by making them understand its significance and need.
		IOM_L_ (2)	(2) Provide sufficient and appropriate-sized resources (including ICT staff capacity and other resources) for business necessities and to ensure CS.

8.7.2 P AND R ACTIVITIES

Table 8.3 shows how reference numbers are used to connect the activities required to achieve the elements that characterise the themes of human preparedness (P) and responsibility (R) of CCSCF. The human preparedness (P) and responsibility (R) activities are given in APPENDIX_5B. For institutions currently without human preparedness (P) and responsibility (R) programmes related to cybersecurity awareness programmes, the activities listed in APPENDIX_5B should help them develop appropriate cybersecurity training, awareness and behavioural characteristics.

Table 8.3: Human Preparedness (P) and Responsibility (R) Elements and Related Activities

Theme: Human Preparedness (P) and Responsibility (R)			
Themes	Elements	ID	Activity ref no
Human Preparedness	1. Cybersecurity competency	P_cybersecurity competency (P_CSC)	P cybersecurity competency (1)
			P cybersecurity competency (2)
			P cybersecurity competency (3)
			P cybersecurity competency (4)
			P cybersecurity competency (5)
			P cybersecurity competency (6)
			P cybersecurity competency (7)
			P cybersecurity competency (8)
	2. Cybersecurity awareness	P_CSA	P CSA (1)
			P CSA (2)
	3. Communication and information sharing	P_CIS	P CIS (1)
			P CIS (2)
			P CIS (3)
Human Responsibility	1. Cybersecurity attitude	R_CSA	R CSA (1)
			R CSA (2)
			R CSA (3)
	2. Cybersecurity behaviour	R_CSB	R CSB (1)
			R CSB (2)
			R CSB (3)
			R CSB (4)
			R CSB (5)
			R CSB (6)

Table 8.4 uses only two of the Preparedness activities shown in Table 8.3, namely “activity ref no”, P_CSC_ (1) and P_CSC_ (2) and one Human Responsibility activity shown in Table 8.3, namely R_CSA_ (1) to provide examples that make it easy to follow and interpret the activities tables in APPENDIX_5B.

Table 8.4: P & R Relation Example of Activity Ref No Column and Activities

Theme: Human Preparedness (P) and Responsibility (R)			
Elements	ID	Activity ref no	Activities
Cybersecurity competency	P_CSC	P_CSC_ (1)	(1) Assess, create and document employees’ cybersecurity training and education programmes, and ensure development of appropriate courses where they are lacking to safeguard and increase employees’ (including ICT staff) cybersecurity abilities (G-36). The assessment should identify the levels of employees’ cybersecurity education. Cybersecurity training and education should be prioritised based on employees' cybersecurity education.
		P_CSC_ (2)	(2) Assess, develop, and grow employees’ knowledge and understanding of CS threats in general and threats that particularly attack healthcare institutions.
Awareness	R_CSA	R_CSA_ (1)	(1) Motivate for positive mindset towards a culture of CS.

8.7.3 TECH ACTIVITIES

The activities vital to the achievement of the technology (TECH) theme of CCSCF are detailed in APPENDIX_5C. Table 8.5 provides the reference numbers of technology elements that connect them to the activities shown in APPENDIX_5C.

Table 8.5: Technology (TECH) Elements and Related Activities

Theme: Technology (TECH)			
Theme	Elements	ID	Activity ref no
Technology	1. ICT Infrastructure	T_ICTI	T_ICTI_ (1)
			T_ICTI_ (2)
			T_ICTI_ (3)
	2. Frequent changes in IT	T_FCIT	T_FCIT_ (1)
			T_FCIT_ (2)
	3. Outsourcing of IT systems	T_OITS	T_OITS_ (1)
			T_OITS_ (2)

Table 8.6 uses two of the ICT infrastructure activities shown in Table 8.5, namely “activity ref no”, T_ICTI_ (2) and T_ICTI_ (2) to provide examples that make it easy to follow and interpret the activities tables in APPENDIX_5C.

Table 8.6: TECH Relation Example of Activity Ref No Column and Activities

Theme: Technology (TECH)			
Elements	ID	Activity ref no	Activities
1. ICT infrastructure	T_ICTI	T_ICTI_ (1)	(1) Map a plan to phase out, improve and/or replace old and outdated IT devices, software, and slow network connections with the latest technology to ensure security
		T_ICTI_ (2)	(2) Ensure sufficient and appropriate ICT infrastructures and technology that will support cybersecurity practices and activities of the institution

8.7.4 EENOM ACTIVITIES

The activities required to achieve the elements of the external environmental and non-organisational management (EENOM) theme are given in Table 8.7. The activities statements in APPENDIX_5D were intended to assist E-Health institutions to initiate cybersecurity actions that would assist them to address the issues identified by the external environmental and non-organisational management (EENOM) theme. Table 8.7 shows external environmental and non-organisational management (EENOM) reference numbers that link the EENOM elements to the activities.

Table 8.7: EENOM Elements and Related Activities

Theme: External Environmental and Non-Organisational Management (EENOM)			
Theme	Elements	ID	Activity ref no
EENOM (Environment)	1. Legal aspects and litigation	EENOM_LL	EENOM_LL (1)
			EENOM_LL (2)
	2. National culture	EENOM_NC	EENOM_NC (1)
	3. Hospital location	EENOM_HL	EENOM_HL (1)
			EENOM_HL (2)
	4. Rules and regulations	EENOM_RR	EENOM_RR (1)

Theme: External Environmental and Non-Organisational Management (EENOM)			
Theme	Elements	ID	Activity ref no
			EENOM_RR_(2)
			EENOM_RR_(3)
	5. Reputational damage	EENOM_RD	EENOM_RD_(1)

Table 8.8 uses two of the Legal litigation activities shown in Table 8, namely “activity ref no”, EENOM_LL_(1) and EENOM_LL_(2), to provide examples that make it easy to follow and interpret the activities tables in APPENDIX_5D.

Table 8.8: EENOM Relation Example of Activity Ref No Column and Activities

Theme: External Environmental and Non-Organisational Management (EENOM)			
Elements	ID	Activity ref no	Activities
1. Legal litigation	EENOM_LL	EENOM_LL_(1)	(1) Make sure employees understand the channels of communication and information sharing outside the organisation.
		EENOM_LL_(2)	(2) educate employee about the implications of legal suits on their institution

This section concludes the description of the development of the CCSCF. The section was used to explain the way in which activities were linked to each element of the framework to promote the creation of a cybersecurity culture. APPENDIX_5 lists the activities. Table 8.1 and Table 8.3 to Table 8.7 were developed and used to demonstrate the linking of activities, via the “activity ref. no”, as per the example in Table 8.2. **Section 8.8** follows with a discussion on how the CCSCF is to be implemented.

8.8 THE FRAMEWORK IMPLEMENTATION TIERS

The design and development of CCSCF were explained in **Sections 8.3 to 8.7** starting by giving the objectives and principles of the framework and continuing to list the activities belonging to various framework elements. This section looks at Segment 5 in the CCSCF overview diagram (see **Figure 8.2**). The purpose of this section is to document how the framework can be implemented. Establishing cybersecurity culture is not a once-off event but is a process. Therefore, it is necessary to find ways of recording cybersecurity culture states (current and future), for instance, through a scoring system, to monitor progress. Monitoring progress while

implementing cybersecurity culture is essential, as it helps E-Health institutions compare their current state with their intended state.

The framework implementation tiers in this study indicate how far a public E-Health institution has progressed in establishing the practices related to the themes, elements and activities explained in the framework. This is achieved by identifying implementation tiers using the capability maturity level approach. This approach calculates progression scores and associated stages of institution in the process of implementing cybersecurity culture.

There are various cybersecurity capability maturity models, including Cybersecurity Capability Maturity Model (C2M2), Electricity Subsection of Cybersecurity Capability Maturity Model (ES-C2M2), Cybersecurity Framework National Institute of Standards and Technology (CSF-NIST), National Initiative for Cybersecurity Education (NICE), Capability Maturity Model (CMM) (National Institute of Standards And Technology, 2018; U.S. Department of Energy, 2014, 2022; U.S. Department of Homeland Security, 2014). However, the implementation tiers applied in this study for the implementation of cybersecurity culture was adapted from the National Institute of Standards and Technology (NIST) (National Institute of Standards And Technology, 2018). The knowledge gained from the NIST framework was supported by information obtained from the framework's implementation use cases (including Intel) (Casey et al., 2015). The definitions and other adaptations of the implementation tier were tailored to the context of this research.

The NIST implementation tier framework was chosen for its flexibility in applying qualitative descriptors, allowing for a nuanced assessment of cybersecurity culture implementation with different levels of difficulty. The NIST framework provided widely adopted implementation tiers for cybersecurity (Dedeke & Masterson, 2019; Frayssinet Delgado et al., 2021; Saritac et al., 2022). Additionally, the Intel implementation use case of the framework was appropriate for this study as it could assist with a resources (people, process and technology) development roadmap. These resources align with the CCSCF themes; human Preparedness (P) and responsibility (R) represent 'people', internal organisation management (IOM) represents 'process', and technology (TECH) obviously indicates 'technology' (Casey et al., 2015; Dedeke, 2017).

The tiers are aligned with four maturity stages, Tiers 1 to 4 (see **Figure 8.8**). Each new tier indicates the series of improvements that have taken place for each of the CCSCF themes.

Figure 8.8 shows that the tiers apply independently to each theme of the CCSCF; an institution can be implementing themes which are in different tiers.

The tier indicates the degree of rigour, the effectiveness of the integrated cybersecurity culture decisions, and the extent to which E-Health institutions share and receive information that assists them in maintaining a cybersecurity culture. Tiers were used to minimise negative influences in internal organisation management (IOM), human preparedness (P) and responsibility (R), technology (TECH), and external environmental and non-organisational management (EENOM) factors as they apply to the implementation and management of cybersecurity in public E-Health institutions. Negative influences cannot be eliminated, but can be managed, hence the use of tiers to minimise them.

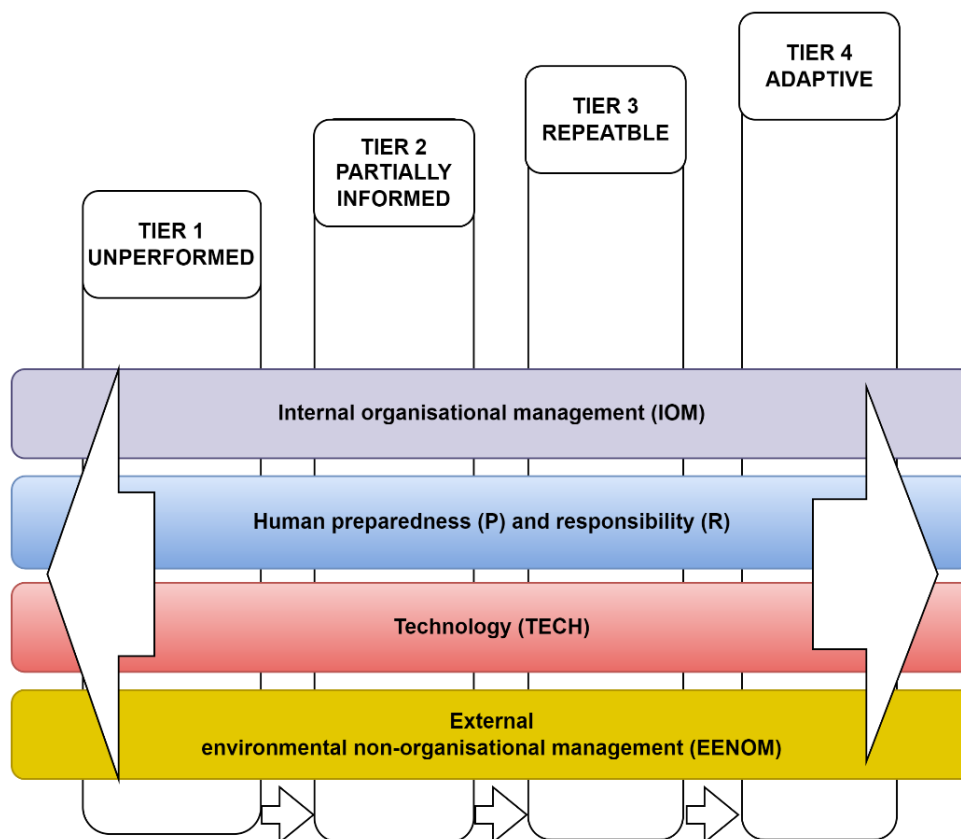


Figure 8.8: CCSCF Implementation Tiers (Adapted from Casey et al., 2015; National Institute of Standards and Technology, 2018)

To promote better understanding of the CCSCF implementation, **Figure 8.8** depicts the different maturity stages (tiers) for each of the CCSCF themes.

Tier 1: Unperformed asserts that there is no formalised cybersecurity culture within the institution. It is characterised by the absence of internal organisation management, cybersecurity practices, and limited or no preparation in terms of cybersecurity competency and awareness. Examples are no awareness, inappropriate cybersecurity attitude and behaviour, lack of attention on cybersecurity technological issues and external environment factors. Institutions at this tier level demonstrate reactive rather than proactive approaches to cybersecurity, leaving them vulnerable to threats.

Tier 2: Partially informed is characterised by recognition of the problem, but ad hoc and inconsistent practices to try to address it. Management recognises internal organisation management cybersecurity practices, but do not demonstrate a consistent approach to improve them or the establishment of an institutional-wide policy. Practices usually happen on an ad hoc basis. There is awareness of the human preparedness and responsibility actions that constitute a culture of cybersecurity throughout the institution, but there is no formalisation of action to introduce these, or the prescribed actions have not been acted upon. Awareness of technological issues about cybersecurity receives limited attention, or reports are obtained on an informal basis. Hence, it is not a recurring process, and the remedial actions are not carried out at all institutional levels. There is awareness about the influence of factors from the external environment on implementing a culture of cybersecurity, but there is no action in response. In essence, this tier is characterised by recognition, awareness and knowledge, but it lacks action and consistent implementation.

Tier 3: Repeatable denotes a more advanced degree of cybersecurity culture maturity. Formally approved internal organisation management cybersecurity practices and procedures, written and well-understood roles and regulations, as well as regularly updated cybersecurity policy, all exist. There is an understanding of the importance of a positive employee attitude, adherence to approved security behaviour, and implementation of human preparedness factors to strengthen cybersecurity, such as establishing training and awareness programmes. Technological issues affecting the establishment of a cybersecurity culture are monitored accurately by the institution. The institution collaborates regularly with the external environment to ensure compliance. This tier is characterised by proactive engagement with external entities, well-informed policies, and organisational-wide practices that demonstrate a strong cybersecurity culture.

Tier 4: Adaptable. This is the peak of cybersecurity culture maturity. Institutions at this tier level continually review and adjust their management cybersecurity practices, leveraging past experiences and consulting predictive indicators to create an even stronger culture of cybersecurity. Agreements are carefully crafted and communicated regarding human preparedness practices, such as training and awareness; an institutional cybersecurity culture budget is allocated. The fourth-tier level can show that there is continuous analysis of technological and external environment issues. This tier also indicates that there is integration of advanced technologies and policies to address evolving threats.

8.8.1 IMPLEMENTATION TIERS: CAPABILITY MATURITY LEVELS

Monitoring the extent to which public E-Health institutions perform necessary themes outcomes pertaining to the achievement of cybersecurity culture is determined by applying the concepts of capability maturity levels using a scoring method. Therefore, the function associated with capability maturity levels is achieved in this study by using the implementation tiers (see **Section 8.8**) together with a way of obtaining a scoring level (Casey et al., 2015; Chrissis et al., 2003; Dedeke, 2017; Paulk et al., 1993).

Table 8.9 shows the capability maturity levels of the CCSCF implementation tier. Information contained in the grids was obtained from the implementation tiers definitions (see **Section 8.8**). The rows of the Table display the CCSCF themes, and the columns exhibit the maturity levels and the applicable score ranges in points. Hence, each grid centres around a theme and shows high-level CCSCF practices of institutions required to achieve a specific maturity level.

The idea of allocating a score range to each of the capability levels was adapted from (Christopher et al., 2014). According to those authors, there are 4 score ranges, namely, 0 to 25%, 26 to 50%, 51 to 75%, and 76 to 100%, and these represent partial, somewhat, large, and full implementation, respectively. In this study, the same score ranges were adopted, but they represent the four tiers, which have been named unperformed, informed, repeatable, and adaptive (see **Figure 8.8**).

The scores in the columns of Table 8.9 were allocated to CCSCF themes based on whether the themes were being performed by the institution (positive score) or lacking (negative score), and the groundedness of the themes to the framework elements (that is, the amount of positivity and negativity emphasised on the activities). See Chapter 9 for more details on how the score ranges are allocated to the CCSCF activities.

Table 8.9: Implementation Tiers Capability Maturity Level

CCSCF THEMES	implementation tier capability maturity level			
	Tier 1: unperformed (1–25 points)	Tier 2: partially informed (26–50 points)	Tier 3: repeatable (51–75 points)	Tier 4: adaptive (76–100 points)
Internal organisation management (IOM)	There are no CS management practices, for instance: -there is no leadership interest and attention to CS -there are no resources such as ICT staff -No CSC champion and/or hub -No management involvement	There are recognitions but inconsistent considerations or approval of CS management practices	CS management practices are regularly done and updated using an organisation-wide approach. CS management practices, knowledge, and skills are applied to specific roles and responsibilities. There is a written communication concerning CS management practices	CS management practices use past experiences, lessons learned, or predictive indicators or adapt to changing threats. CS management practices are clearly understood and considered promptly and effectively.
Human preparedness (P)	CSC preparedness practices like training and, education, awareness are done in an ad hoc manner	Awareness of CS preparedness practices, but it is unformalized and not repeatable.	Consistent methods of CSC preparedness practices are applied in implementing preparedness factors.	There is a formal agreement documented as part of CS preparedness practices, and there is an institutional budget to take care of preparedness practices
Human responsibility(R)	There are no appropriate CS responsibility practices	CS responsibility practices are known by management but not formally established and or approved by organisational-wide policy and, as such they are not repeatable	CS responsibility practices are understood, regularly updated, and implemented as intended. CS responsibility practices are accurately monitored within the organisation	CS responsibility practices are adapted to changing threats.
Technology (TECH)	There is unaware or no attention to CS technological issues	CS technological issues are not formally established, therefore, not approved by organisational wide policy	Senior management gives attention to CS technological issues by example monitoring technological issues accurately	CS technological issues are continuously analysed and resolved among employees both internally and externally. Issues are also resolved to adapt to changing technological threats
External environment non-organisation (EENOM)	CS external environment factors are not managed	There are inconsistent considerations of CS external environment factors. There is awareness of external factors but no action on them	Non-CS executives communicate regularly, and they aware of CS external environment factors	CS external environment factors are clearly understood and considered. There are formal agreements documented with regard to CS external environmental factors

These score ranges helped map the implementation tiers to the capability maturity level. For instance, institutions in Tier 1 are not meeting the cybersecurity culture activities required to achieve cybersecurity culture implementation. The benefit of linking the implementation tier to the capability maturity level is that it clearly shows progress in the implementation of cybersecurity culture, as the institution improves in terms of the different elements within the CCSCF themes. Using the national culture element as an example, Table 8.13 shows that Tier 1 represents institutions that have 0%, that is, have no understanding of national culture factor differences that can influence them (have reached the least successful level). Institutions in tier level 4 clearly understood the natural cultural difference and took it into consideration.

8.8.2 ACTIVITIES-BASED IMPLEMENTATION TIER MATURITY LEVEL

Table 8.9 gives a high-level view of what each of the four implementation tiers covers. Table 8.10 to Table 8.13 show the activity-based implementation tier maturity levels obtained from the data for all the elements of the framework. This shows the direct links between the implementation tiers and associated maturity levels to the activities discussed in **Section 8.7**.

The ranges of the scores for the activities associated with CCSCF elements (depicted in Table 8.10 to Table 8.13) are also assigned based on whether the activities are practised in the institution (a positive score) or not (a negative score), and the grounding of the activities to the framework elements (the degree of the activity's positivity or negativity). The grounding indicates the importance and emphasis placed on whether the activities are being practised or not. Hence, negative cybersecurity culture activities are listed in column one (indicating score range of 1 to 25 points) or column two (26 to 50 points). The positive activities are in columns three or four, with scores ranging between 51 and 75 points or 76 and 100 points.

The cybersecurity culture activities that are seriously at risk and needing urgent attention (shown by high negative groundedness) will be in the first range (1 to 25 points). While the activities with relatively small negative groundedness are in the second range (26 to 50 points). A similar process is applied to positive activities. Low positive activities have scores in the range of 51 to 75 points, and high positive activities are in the 76 to 100 points range. Chapter 9 contains more detail on the allocation of the score range to the CCSCF activities.

Depending on the number of activities associated with each element of the framework, a maximum of 5 and a minimum of 2 activities were used to create a relationship between the activities and the implementation tier maturity level.

8.8.2.1 IOM Activities Implementation Tier Maturity Level

The activities of internal organisation management (IOM) elements are linked to an implementation tier maturity level using the information depicted in Table 8.10. The grids of Table 8.10 centred around the activities of elements of CCSCF. The grids show the activities institutions need to carry out to achieve a given maturity level.

Table 8.10 shows which institutions are at Tier 1 for the leadership element; these institutions have little to no interest in cybersecurity culture, no cybersecurity culture champions and lack sufficient resources to allow them to achieve a strong cybersecurity culture. On the other hand, institutions at Tier 4 have demonstrated a wide-ranging interest in and attention to cybersecurity culture and have champions and available resources.

Table 8.10: IOM Activities Implementation Tiers Capability Maturity Level

CCSCF themes& elements	Implementation tier capability maturity level			
	Tier 1: unperformed (1–25 points)	Tier 2: partially informed (26–50 points)	Tier 3: repeatable (51–75 points)	Tier 4:adaptive (76–100 points)
Internal organisation management (IOM)				
Leadership	No IOM_L_ (1). Insufficient IOM_L_ (2). Absence of IOM_L_ (3). Lack of IOM_L_ (4). No IOM_L_ (5).	Inconsistent IOM_L_ (1). Approved IOM_L_ (2) are unrepeatable. IOM_L_ (3) & IOM_L_ (4) not formally established. IOM_L_ (5) not approved.	Consistent IOM_L_ (1). Approval of IOM_L_ (2). IOM_L_ (3) & IOM_L_ (4) formally established by institution-wide policy. IOM_L_ (5) is approved by management.	Widespread IOM_L_ (1). Effective & timely IOM_L_ (2). IOM_L_ (3) adapted previous & current practices. IOM_L_ (4) is an integral part of the institution. Institutional-based IOM_L_ (5).
CS governance	Absence of IOM_CSG_ (1). No IOM_CSG_ (2). Little IOM_CSG_ (3). Absence of IOM_CSG_ (4). Lack of IOM_CSG_ (5). limited IOM_CSG_ (6).	Incomprehensive IOM_CSG_ (1). IOM_CSG_ (2) not formally known. IOM_CSG_ (3) & IOM_CSG_ (4) not consistently applied & repeatable. IOM_CSG_ (5) not informally known & obtained. Inconsistent IOM_CSG_ (6).	IOM_CSG_ (1) is frequently updated. Approved IOM_CSG_ (2). IOM_CSG_ (3) plan approved & implemented. IOM_CSG_ (4) updated & implemented as intended. IOM_CSG_ (5) are understood by all. Accurate monitoring & evaluation of IOM_CSG_ (6).	Timeous & all-inclusive IOM_CSG_ (1). IOM_CSG_ (2) is based on lessons learned. IOM_CSG_ (3) adapt CS activities. IOM_CSG_ (4) include innovative practices. There are institution-wide strategies for IOM_CSG_ (5). Practices-based IOM_CSG_ (6).

Business continuity	No IOM_BC_ (1). No activities on IOM_BC_ (2). Limited IOM_BC_ (3) are conducted. No effort on IOM_BC_ (4). Absence of IOM_BC_ (5).	Inconsistent IOM_BC_ (1). IOM_BC_ (2) approved but lacks establishment by institution-wide policy. IOM_BC_ (3) not reoccurring or repeatable. Inconsistent consideration of IOM_BC_ (4) as objectives at all institution levels. IOM_BC_ (5) lacks information sharing and is not repeatable	IOM_BC_ (1) & IOM_BC_ (3) are regularly updated, implemented & monitored. There are defined procedures for IOM_BC_ (2). IOM_BC_ (4) are monitored & regularly updated. IOM_BC_ (5) implemented as intended.	IOM_BC_ (1) are continuously analysed. IOM_BC_ (3) adapts to CS practices & changing threats. IOM_BC_ (2) adapts practices based on previous & current activities. Achieve IOM_BC_ (4) base on lessons learned. Execute IOM_BC_ (5) timeously & in an effect manner.
Organisational learning	Lack of IOM_OL_ (1). No IOM_OL_ (2) in the institution.	The importance of IOM_OL_ (1) is recognised but not approved. IOM_OL_ (2) are not established by the institution-wide policy.	IOM_OL_ (1) is defined & approved. Procedures for IOM_OL_ (2) approved & repeatedly updated via organisation-wide approach.	IOM_OL_ (1) & IOM_OL_ (2) are clearly understood & considered.
Physical security	Absence of IOM_PS_ (1). Lack of IOM_PS_ (2). No IOM_PS_ (3).	Inconsistency in IOM_PS_ (1). IOM_PS_ (2) & IOM_PS_ (3) are not consistently applied.	IOM_PS_ (1) & IOM_PS_ (2) are defined & monitored. IOM_PS_ (1) implemented as approved & intended.	Use role based understanding & policies to IOM_PS_ (1). IOM_PS_ (2) are incessantly analysed. IOM_PS_ (3) implemented effectively.
Communication channels	No IOM_CC_ (1). 0% IOM_CC_ (2) & IOM_CC_ (3).	Unofficial IOM_CC_ (1). Informal knowledge of IOM_CC_ (2). Inconsistency in the IOM_CC_ (3).	Formally approved & well-understood IOM_CC_ (1), IOM_CC_ (2), & IOM_CC_ (3).	IOM_CC_ (1) cover both internal & external. There is formal agreement on IOM_CC_ (2). Use real time IOM_CC_ (3).

8.8.2.2 P and R Activities' Implementation Tier Maturity Level

Table 8.11 depicts the implementation tier maturity level linked to the activities of human preparedness (P) and responsibility (R) elements of CCSCF. Each grid of Table 8.11 contains the various activities associated with the human preparedness (P) and responsibility (R) elements. Performance on these activities qualifies institutions to achieve a specific maturity level in their cybersecurity culture implementation.

For the themes depicted in Table 8.11 for instance, the element of CS competency shows that institutions in tier level 1 create no opportunity for CS training and keep no records of staff CS training and education. while institutions in tier level 4 prioritised such activities.

Table 8.11: Human Preparedness and Responsibility Activities Implementation Tiers Capability Maturity Level

CCSCF themes& elements	Implementation tier capability maturity level			
	Tier 1: unperformed (1–25 points)	Tier 2: partially informed (26–50 points)	Tier 3: repeatable (51–75 points)	Tier 4:adaptive (76–100 points)
Human preparedness (P)				
CS competency	No P_CSC_ (1). Ad hoc P_CSC_ (2) & P_CSC_ (3). Unsupported P_CSC_ (4). Lack of P_CSC_ (5).	Inconsistent & no formalised way to achieve P_CSC_ (1) & P_CSC_ (2). There is recognition for P_CSC_ (3), but action are not taken. P_CSC_ (4) is not well established. No established process for P_CSC_ (5).	P_CSC_ (1) is formally approved. P_CSC_ (2) is consistently & regularly developed. Defined procedures for & develop understanding of P_CSC_ (3). Create approved environment for P_CSC_ (4). Consistent method applied to ensure P_CSC_ (5).	P_CSC_ (1) is prioritised. P_CSC_ (2) is done timeously. Apply organisation wide approach in achieving P_CSC_ (3). P_CSC_ (4) is developed based on formal agreement & lessons learned. Apply formal mechanism & organisation wide approach in P_CSC_ (5).
CS awareness	No P_CSA_ (1). There is lack of P_CSA_ (1).	Limited P_CSA_ (1). No approved & formal way to achieve P_CSA_ (2). Low cognition of CS practices.	Sufficient P_CSA_ (1). There is a formal & regular way of P_CSA_ (2). High cognition & application of CS practices.	Robust P_CSA_ (1). P_CSA_ (1) is reviewed & improved. Recognition of CS practice is prioritised.
Communication and information sharing	No platform that inspire P_CIS_ (1). Absence of P_CIS_ (2). Lack of P_CIS_ (3).	Inconsistent in achieving P_CIS_ (1). Importance of P_CIS_ (2) is recognised but not established. P_CIS_ (3) is approved but informally established.	Consistent in P_CIS_ (1). Written agreement on P_CIS_ (2). There is an establishment & consistency in P_CIS_ (3).	Real-time communication of P_CIS_ (1). P_CIS_ (2) are understood. P_CIS_ (2) are done timeously & continuously.

Human responsibility(R)				
CS attitude	No R_CSA_ (1). R_CSA_ (2) & R_CSA_ (3) are not performed.	No approved & established way to achieve R_CSA_ (1) & R_CSA_ (2). R_CSA_ (3) is not formalised.	R_CSA_ (1) is implemented as intended. R_CSA_ (2) is formal approval & monitored accurately to inform decisions. Collaborate with other in R_CSA_ (3).	R_CSA_ (1) is informed by understanding & lesson learned. R_CSA_ (2) is effectively done. R_CSA_ (3) is done & responded to timeously.
CS behaviour	No R_CSB_ (1). 0 effort in R_CSB_ (2). lack of R_CSB_ (3). R_CSB_ (4) are not evaluated.	Inconsistency in doing R_CSB_ (1). R_CSB_ (2) is not formally established. No formal R_CSB_ (3). R_CSB_ (4) is not formally evaluated.	R_CSB_ (1) is formally approved & regularly done. R_CSB_ (2) are checked & monitored. R_CSB_ (3) is formally done & implemented. R_CSB_ (4) are formally approved.	R_CSB_ (1) is done timeous. Continuous analysis of R_CSB_ (2). There is an agreement on R_CSB_ (3). R_CSB_ (4) are done thoughtfully & are based on lessons learned.

8.8.2.3 TECH Activities' Implementation Tier Maturity Level

The implementation maturity level for activities related to technology (TECH) elements is depicted in Table 8.12 and each grid in the table shows the cybersecurity culture activities to be performed to achieve a specific maturity level.

The information in Table 8.12 shows that institutions with a score of 0% have no plan at all in place to guide the phasing out or replacement of their ICT; these institutions are in Tier 1. On the other hand, institutions that have well-established strategies (that can be adapted to suit cybersecurity practices and changing technology), explaining how they plan to phase out or replace their ICT, have obtained tier level 4.

Table 8.12: Technology Activities Implementation Tiers Capability Maturity Level

CCSCF themes& elements	Implementation tier capability maturity level			
	Tier 1: unperformed (1–25 points)	Tier 2: partially informed (26–50 points)	Tier 3: repeatable (51–75 points)	Tier 4:adaptive (76–100 points)
Technology (TECH)				
ICT Infrastructure	0% plan to T_ICTI_ (1). Lack of T_ICTI_ (2). No motivation for T_ICTI_ (3).	T_ICTI_ (1) follows no formal process. No approved institution policy for T_ICTI_ (2). Inconsistent motivation for T_ICTI_ (3).	Established processes for T_ICTI_ (1). The importance of T_ICTI_ (2) is recognised & its implementation is supported. T_ICTI_ (1) is motivated & implemented.	T_ICTI_ (1) adapts CS practices & changing technology. Prioritised T_ICTI_ (2). T_ICTI_ (3) is often analysed & considered.
Frequent changes in IT	No T_FCIT_ (1). Ad hoc T_FCIT_ (2).	Inconsistent & unrepeatable T_FCIT_ (1). T_FCIT_ (2) approved but no execution.	Routine T_FCIT_ (1) are defined & monitored. Methods are applied to T FCIT_ (2).	Timeous & effective T_FCIT_ (1). Institution-wide approach applied to T FCIT_ (1).
Outsourcing of IT systems	Lack of T_OITS_ (1). No T_OITS_ (2).	T_OITS_ (1) is defined. Needs for T_OITS_ (2) is acknowledged but lack establishment.	T_OITS_ (1) is regularly done & monitored. Procedure for T_OITS_ (2) is defined & regularly monitored.	T_OITS_ (1) is regularly reviewed. Develop & maintain strong relationships for easy T OITS_ (2).

8.8.2.4 EENOM Activities Implementation Tier Maturity Level

The final Table 8.13 showed the activity-based implementation tier maturity level related to external environmental and non-organisational management (EENOM). According to Table 8.13 the focus of each grid is on an element, and it displays CCSCF activities that help to classify institutions to a given maturity level.

Table 8.13: EENOM Activities Implementation Tiers Capability Maturity Level

CCSCF themes& elements	Implementation tier capability maturity level			
	Tier 1: unperformed (1–25 points)	Tier 2: partially informed (26–50 points)	Tier 3: repeatable (51–75 points)	Tier 4:adaptive (76–100 points)
External environment and non-organisation management (EENOM)				
Legal litigation	Lack of EENOM_LL_ (1) & EENOM_LL_ (1).	Unapproved EENOM_LL_ (1). EENOM_LL_ (2) is not formalised	EENOM_LL_ (1) is approved & understood. Formalised & regular messages on EENOM_LL_ (1).	Formal agreement on the EENOM_LL_ (1). Impact of EENOM_LL_ (2) is clearly understood.
National culture	0% identification of EENOM_NC_ (1)	Needs are identified for EENOM_NC_ (1) but action is lacking.	Established EENOM_NC_ (1) identification.	EENOM_NC_ (1) is clearly understood & considered.
Hospital location	Lack of EENOM_HL_ (1) & EENOM_HL_ (2).	Inconsistency in achieving EENOM_HL_ (1) & EENOM_HL_ (2).	There is a collaboration to achieve EENOM_HL_ (1) & EENOM_HL_ (2).	There is a mechanism for strong relationships with EENOM_HL_ (1) & EENOM_HL_ (2)..
Rules and regulations	No attention to EENOM_RR_ (1). No action on EENOM_RR_ (2) & EENOM_RR_ (3)	Unestablished consequences with lack/adherence to EENOM_RR_ (1), EENOM_RR_ (2), & EENOM_RR_ (3).	Process, procedures, & impacts are clearly defined for EENOM_RR_ (1), EENOM_RR_ (2), & EENOM_RR_ (3).	Continuous analysis of EENOM_RR_ (1), EENOM_RR_ (2), & EENOM_RR_ (3).
Reputational damage	0 effort on EENOM_RD_ (1).	No consistency on EENOM_RD_ (1) across all areas.	Regular communication on the essence & procedures for EENOM_RD_ (1).	Formal agreement on roles towards the EENOM_RD_ (1).

This section discusses framework implementation tiers adapted from the NIST and Intel maturity-oriented frameworks (Casey et al., 2015; National Institute of Standards and Technology, 2018) as the implementation approach that would be used for the CCSCF developed in **Sections 8.5 and 8.6**. This included the definitions of the different implementation tiers and their capability maturity levels (both the high-level and activity-level views). The next section presents the conclusion of the chapter.

8.9 CONCLUSION OF THE CHAPTER

Chapter 8 achieved Phase 6 of the conceptual framework analysis. This chapter seeks to answer Research Sub-Question 5.

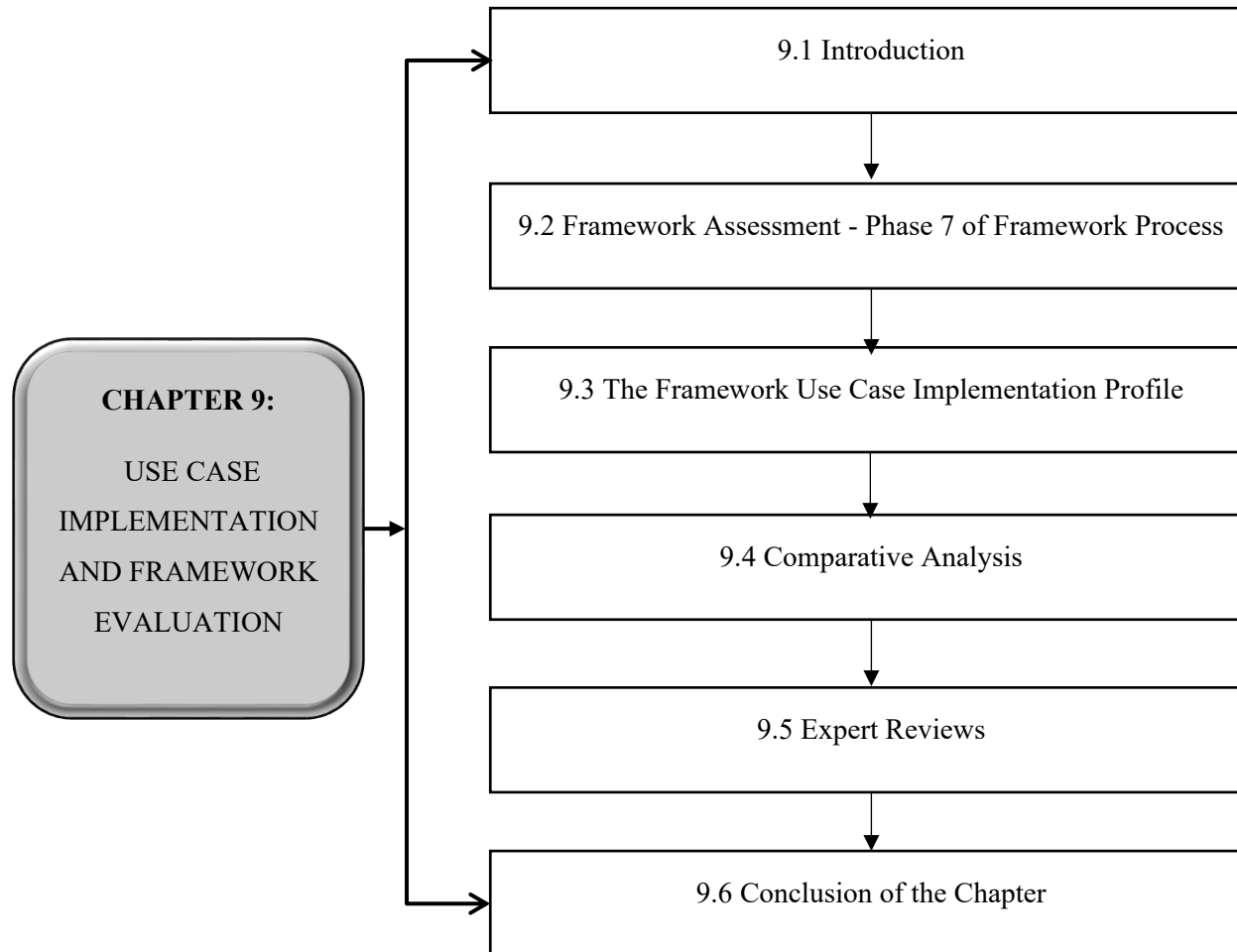
Research Sub-Question 5: *How can the identified factors be used to design and develop a contextual framework for establishing cybersecurity culture in public E-Health institutions in South Africa?*

To answer this question, the chapter presented the design and development of the CCSCF to assist public healthcare institutions with the establishment of a cybersecurity culture. The chapter highlighted the high-level CCSCF themes and their priorities in relation to the development of a cybersecurity culture.

The chapter presented the elements of each framework theme based on the research findings. It also outlined the essential activities required under each of the elements for the establishment of a cybersecurity culture. Finally, the chapter discussed framework implementation tiers adapted from existing framework implementation tiers to present how the CCSCF can be implemented.

The next chapter will focus on the seventh phase of the conceptual framework technique, which is the validation phase.

CHAPTER 9: USE CASE IMPLEMENTATION AND FRAMEWORK EVALUATION



9.1 INTRODUCTION

The previous chapter presented the design and development of the CCSCF for establishing cybersecurity culture in public E-Health institutions. This was done following Phases 5 and 6 of the conceptual framework analysis (Jabareen, 2009).

This chapter presents Phase 7 of the conceptual framework analysis, which aims to evaluate the CCSCF. CCSCF was evaluated using a use case implementation profile, comparative analysis and expert review.

Phase 7 of the conceptual framework analysis addressed Research Sub-Question 6 and achieved its Research Sub-Objective 6 as stated in Chapter 1 of this research study.

Research Sub-Question 6: *“How can the Contextual Cybersecurity Culture Framework be evaluated for relevance, uniqueness and appropriateness?”*

Research Sub-Objective 6: *“To explore how the Cybersecurity Culture Framework that is developed can be evaluated for relevance, uniqueness and appropriateness?”*

The remainder of the chapter has five sections. Phase 7 of the conceptual framework analysis is explained in **Section 9.2**. This is followed by **Section 9.3**, which presents the framework use case implementation profile. Comparative analysis and expert reviews, as the two remaining CCSCF evaluation methods, are discussed in **Sections 9.4** and **9.5**. The chapter is concluded in **Section 9.6**.

9.2 FRAMEWORK ASSESSMENT: PHASE 7 OF THE FRAMEWORK PROCESS

Chapter 5 introduced conceptual framework analysis as one of the methods used in this research. Conceptual framework analysis was used to design and develop the CCSCF framework. Chapter 8 described in detail how the phases of conceptual framework analysis were followed until the proposed CCSCF was developed in Phase 6.

Figure 9.1 depicts the last step of the conceptual framework analysis (step 3) (modelled in Chapter 5).

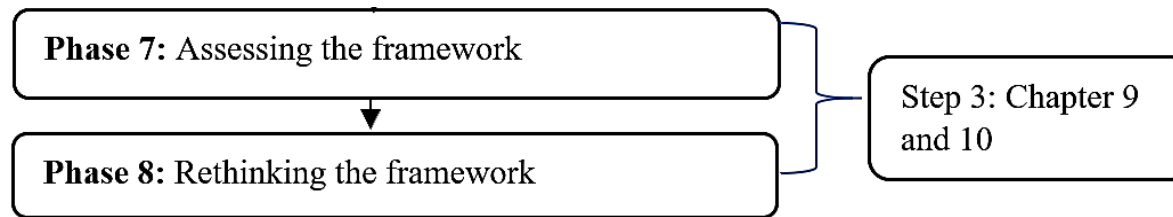


Figure 9.1: Step 3 (Phases 7 and 8) of the Adapted Framework Technique (Adapted from Jabareen, 2009)

This chapter presents Phase 7 of the process as the method that guided the evaluation of the CCSCF. This phase evaluates an artefact with the assistance of experts (other researchers and practitioners) and ensures that it makes sense to others (Jabareen, 2009). It was used in this research to verify the value of the proposed CCSCF. However, an assessment of a framework starts with the researcher before seeking views and opinions from others.

The framework evaluation process began with a use case implementation profile, achieved using the capability cybersecurity maturity profile. A comparative analysis was conducted to compare the elements of CCSCF with the factors or components of other cybersecurity culture frameworks. Comparing the frameworks highlighted similarities and differences between the CCSCF and the existing frameworks. Finally, expert reviews were conducted to evaluate the CCSCF. When evaluating the framework, the experts attempted to determine the extent to which the framework's principles, objectives, comprehensiveness, and adaptability are satisfied.

A thorough evaluation of the framework can ensure that a credible theory is offered to the Information Systems research community and researchers investigating the fast-growing phenomenon of cybersecurity culture. **Figure 9.2** depicts the three evaluation methods conducted in the study.

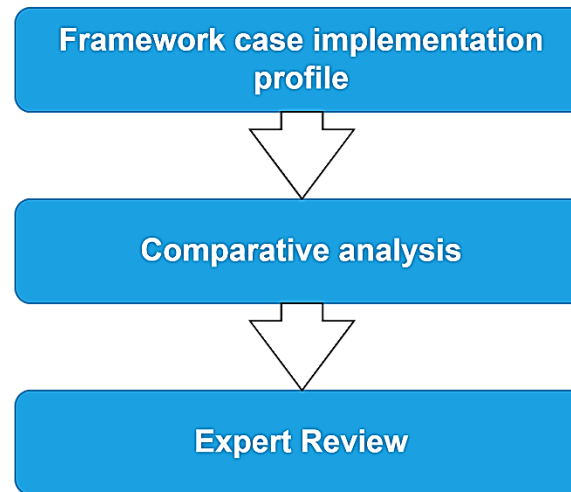


Figure 9.2: Evaluation Methods for CCSCF (own source)

9.3 THE FRAMEWORK USE CASE IMPLEMENTATION PROFILE

The use case implementation profile was designed to assist E-Health institutions and other organisations to understand the CCSCF implementation scenarios and activities needed to establish a strong cybersecurity culture. This was approached in this study by mapping the activities to factors related to business processes or internal mechanisms, people, ICT systems, and the external environment of the institution, see **Figure 9.3**.

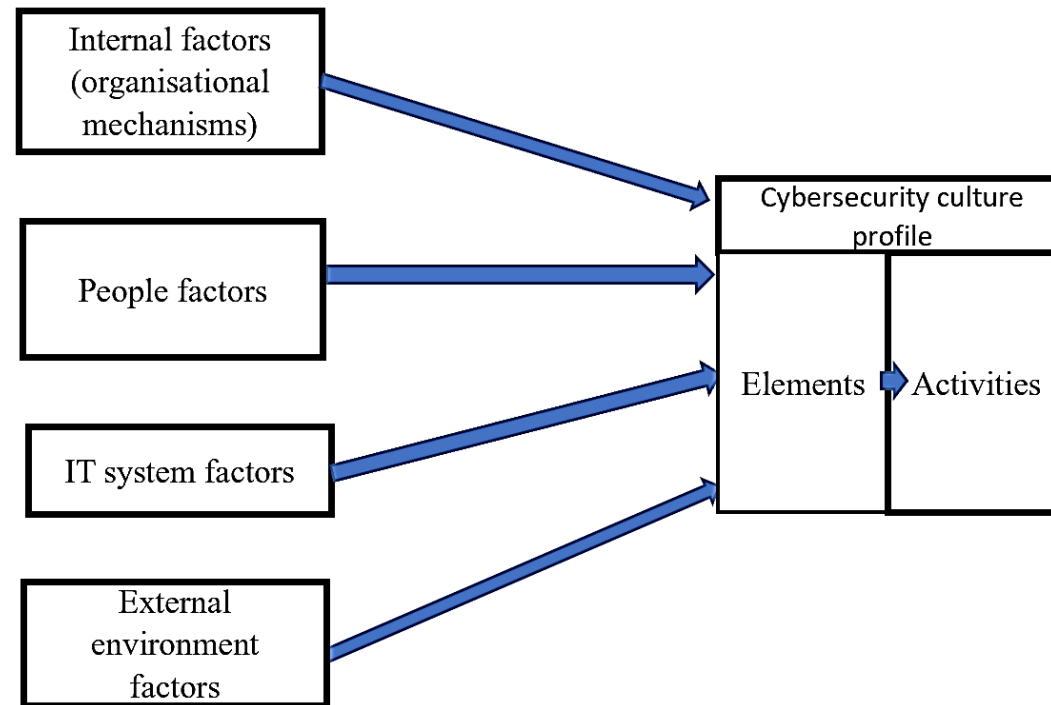


Figure 9.3: Mapping Framework Use Case Profile (own source)

The components to the right of **Figure 9.3** are consistent with the themes of CCSCF (depicted in Chapter 8) and the elements of the E-Health ecosystem (described in Chapter 2). Applying the framework profile was intended to help practitioners by making the alignment of the fundamental aspects of the E-Health ecosystem with the CCSCF activities visible.

The purpose of CCSCF is to assist E-Health institutions in establishing a strong cybersecurity culture. The capability maturity profile was applied to the CCSCF activities to help institutions a) determine the maturity level of their current cybersecurity culture activities, b) set a target, and c) prioritise the future activities which are needed to establish a cybersecurity culture.

9.3.1 E-HEALTH CYBERSECURITY CULTURE CAPABILITY MATURITY PROFILE

The concept of the capability maturity profile is introduced in this chapter to aid the implementation of the CCSCF. The concept has been applied successfully in other studies (Chrissis et al., 2003; Dedeke, 2017).

The capability maturity profile was used to develop a template to guide the cybersecurity culture activities and practices of E-Health institutions in the given context. The development of the capability maturity profile template that was used in this study corresponds with the sixth and final segment of the framework overview diagram (**Figure 8.2**). It was used to assist institutions in identifying their capability gaps (in terms of their cybersecurity culture activities), that is, to measure the difference between their current capability levels and the desired level. This was expected to help the province to monitor how the E-Health institutions in their context performed the necessary activities for achieving a cybersecurity culture.

The capability gap can be used to indicate the strengths and weaknesses of E-Health institutions regarding the introduction and performance of cybersecurity culture activities. This ultimately guides their efforts to establish a cybersecurity culture. Each capability would be assessed based on its maturity level and weighted priority, highlighting areas that require improvement.

Table 9.1 gives an example of the capability maturity profile template covering the activities of the elements of the internal organisation management (IOM) themes. For human preparedness (P) and responsibility (R), Technology (TECH), and external environmental and non-organisational management (EENOM) themes template see APPENDIX_6 (6A to 6C).

The key terms used in Table 9.1 are defined below:

Elements are the fundamental factors of cybersecurity culture identified via literature, surveys and interview data collection. The term element is used interchangeably with factors.

Activities' keywords are keywords used to summarise the activities that define each element.

Present capability profile and maturity are the current capability profile of a case and its maturity level. (See **Section 9.3.1.1** for the formula for the calculations of the current capability profile.)

Intended capability profiles and maturity are the institution's desired capability profile and its maturity level.

Capability Gaps (CG) is a gap revealed by comparing the current and intended capability profiles. CG is the difference between the intended and current capability.

Weight (W) is the ability to achieve a significant outcome.

Priority (P) is the level of importance linked to specific cybersecurity culture activities in the institution's maturity steps.

Table 9.1 shows an example of a capability profile template for the activities of internal organisation management (IOM) elements.

Table 9. 1: Capability profile template for the activities of IOM elements

Elements	Activities keywords & Groundedness (G)	Present		Intended		Capability gap (CG)	Weight (W)	Priority (W * CG)
		Capability Profile	Maturity	Capability Profile	Maturity			
Leadership	Leaders interest & attention [G]	[]	[]	[]	[]	[]	[]	[]
	provision of resources [G]	[]	[]	[]	[]	[]	[]	[]
	CSC Champion/team [G]	[]	[]	[]	[]	[]	[]	[]
	Management involvement & support [G]	[]	[]	[]	[]	[]	[]	[]
	CS sub-budget [G]	[]	[]	[]	[]	[]	[]	[]
CS governance	Simulated activities [G]	[]	[]	[]	[]	[]	[]	[]
	CS Policy [G]	[]	[]	[]	[]	[]	[]	[]
	CS governance structure [G]	[]	[]	[]	[]	[]	[]	[]
	User restrictions & password management [G]	[]	[]	[]	[]	[]	[]	[]
	CS plan towards CSC [G]	[]	[]	[]	[]	[]	[]	[]

Elements	Activities keywords & Groundedness (G)	Present		Intended		Capability gap (CG)	Weight (W)	Priority (W * CG)
		Capability Profile	Maturity	Capability Profile	Maturity			
	Compliance monitoring & evaluation [G]	[]	[]	[]	[]	[]	[]	[]
Business continuity	Vulnerability management [G]	[]	[]	[]	[]	[]	[]	[]
	Contingency plan [G]	[]	[]	[]	[]	[]	[]	[]
	Risk assessment [G]	[]	[]	[]	[]	[]	[]	[]
Organisational learning	Learning process levels [G]	[]	[]	[]	[]	[]	[]	[]
	Build and retain CS [G]	[]	[]	[]	[]	[]	[]	[]
Physical Security	Data protection measures [G]	[]	[]	[]	[]	[]	[]	[]
	Server network integrity [G]	[]	[]	[]	[]	[]	[]	[]
	Access to assets [G]	[]	[]	[]	[]	[]	[]	[]
	Channel and network [G]	[]	[]	[]	[]	[]	[]	[]

Elements	Activities keywords & Groundedness (G)	Present		Intended		Capability gap (CG)	Weight (W)	Priority (W * CG)
		Capability Profile	Maturity	Capability Profile	Maturity			
Communication channel	Intranet & websites [G]	[]	[]	[]	[]	[]	[]	[]
	Meetings [G]	[]	[]	[]	[]	[]	[]	[]

The capability profile template for the activities of human preparedness (P) and responsibility (R), technology (TECH), and the external environmental and non-organisational management (EENOM) elements of CCSCF. (These are depicted in APPENDIX_6 (6A to 6C).

Sections 9.3.1.1 to 9.3.1.3 explain how the various essential terms of the capability profile template were determined. (see Table 9.1 and APPENDIX_6B to 6C).

9.3.1.1 The Current Capability Profile

Using the Mpumalanga Health Department as a use case, a scale was formulated to consistently calculate the current capability profile values for each activity of the framework elements. The scale was formulated using groundedness (G) values from the thematic analysis of Chapter 7. The groundedness value can be regarded as the value obtained by assessing the institution's state related to the various activities of CCSCF elements (or factors).

Groundedness was scaled to the implementation tiers indicated in Table 8.9 to obtain the capability level of the activities. The activities were based on the cybersecurity culture factors identified from the literature and the quantitative and qualitative study described in Chapters 4, 6 and 7.

The researcher developed the scale by applying the equation depicted below.

$$\text{Current capability level} = \left[\frac{G + 100}{2} \right]$$

G represents the value of groundedness used to obtain the capability level. The capability level is used to determine the maturity and ranges from 1 to 4. The 4-score scale, which represents all possible groundedness values developed as a result, is as follows: a groundedness value between 51 and 100 is represented by tier 4, 1 to 50 is represented by tier 3, -49 to 0 is represented by tier 2, and -100 to -50 is represented by tier 1.

The maturity value assigned to the current capability profile is based on the institution's implementation tier capability level (see Table 8.9). The current capability profile was calculated using the groundedness (G) value obtained by the elements during thematic analysis from the interview results (given in Chapter 7).

The maturity value of activities with negative G values, in the range -100 to -50 (see Table 9.1 and **APPENDIX_6 (6A, 6B and 6C)**) will be placed under tier 1 (0 to 25%) of the capability maturity level in Table 8.9. This shows that the activities are not being performed at all or are very poorly performed. Negative G values in the range -49 to 0 is in tier 2 (26 to 50%), representing activities performed on an ad hoc basis but not carried out as a matter of routine, or activities that the institutions are aware of but are not consistently implemented.

A positive G value, in the range +1 to +50, is allocated to tier 3 (51% to 75%), representing the institution's formally approved cybersecurity culture activities. Activities with the highest positive G value, that is, in the range +51 to +100 (see Table 9.1 and **APPENDIX_6 (6A, 6B and 6C)**) will be in tier 4 (76% to 100%) capability maturity level (see Table 8.9). Activities at this level of maturity optimise cybersecurity culture implementation.

9.3.1.2 Intended Capability Profile

The intended capability profile and its associated maturity level is institution specific. This means that the circumstances of the institution, like objectives towards cybersecurity, size, and resources, need to be considered.

Depending on an institution's current capability profile values and maturity level on the cybersecurity culture activity, the minimum desired capability that the organisation should aim to achieve should be to move the critical activity value to the more desirable end of the range at its current level or to progress up one level from its current maturity level.

This makes the cybersecurity culture activities realistic and achievable for organisations with resource constraints. More well-resourced organisation can boost their desired capability target depending on their goal.

For example, if an institution is presently in the entry or middle-value range in maturity level 2, after the current capability profile calculation, the minimal goal would be to move the activity to the best end of the range in maturity level 2.

For demonstration purposes, the following percentage ranges are depicted in Table 9.2 were developed to determine intended capability values and their associated maturity.

Table 9.2: Intended Capability Percentage Range

Value Range	Percentage
-40 to -31	75%
-30 to -21	65%
-20 to -11	55%
-10 to -1	45%
0 to 10	35%

Value Range	Percentage
11 to 20	25%
21 to 30	15%
31 to 40	5%

Looking at the groundedness values, the worst negative value is in fact -36, but this value is rounded off to the nearest multiple of 10, which is -40. This rounding is also applied to positive values to get a range that will cover all the G values obtained from the data collected.

To obtain the intended capability values, the current capability values of activities with negative G values between -40 and -31 and -30 and -21 were increased by 75% and 65%. For activities with negative G values between -20 and -11 and -10 and -1, 55% and 45% of their current capability values were added to obtain the intended capability. It is important to reiterate that a negative value denotes activities that need urgent attention, either because they are not attended to at all, are performed on an ad hoc basis, or are recognised activities that have not been established as part of a routine.

Intended capability profiles for positive G value activities ranging between 1 to 10, 11 to 20, 21 to 30, and 31 to 40 were determined by adding 35%, 25%, 15%, and 5% to the current profile. A positive value shows that the cybersecurity culture activities are being performed reasonably consistently in the institution, although they might still need improvement.

The intended capability profile is calculated as follows:

$$\text{Intended capability} = \left[\frac{\%}{100} \times \text{current value} \right] + \text{current value}$$

This means that an activity-intended capability profile is obtained by increasing the current capability value by the required percentage (see Table 9.3).

9.3.1.3 Priority and Weight Values

Priority is used to reveal the most urgent activities of the framework elements that need attention in establishing a strong cybersecurity culture in the Mpumalanga Department of Health. Priority is the product of the capability gap (CG) and weight (W). Capability gap is the difference between the current capability and the desired capability profile of an institution.

Priority is calculated as follows: $\text{Priority} = (W * \text{CG})$

A score is generated by multiplying the gap and weight, enabling the E-Health institutions' management to allocate resources, commencing with the activities with the highest weight and largest gap as they will have a high priority score and hence need to receive urgent attention.

Using the capability gap and weight to determine the urgent activities in the CCSCF was recommended by existing research (Dedeke, 2017; National Institute of Standards And Technology, 2018). In related research, weight is categorised (0 - unimportant, 1 - valuable, 2 - important and 3 - critical) (Dedeke, 2017; National Institute of Standards and Technology, 2018). Drawing from this, in this study, weight is categorised as 1 - Optimal (no attention required), 2 - managing (some attention required), 3 - Urgent (high attention required), and 4 - critically urgent (very high attention required).

As defined in Table 9.3, a weight is allocated to each capability gap based on the activities' groundedness (G) range. For example, activities with a very negative G value (-40 to -21) are assigned a weight of 4, while activities with less serious negative G (-20 to -1) are allocated a weight of 3. Similarly, the high positive activities are allocated a weight of 1, while activities with lower positive values are given a weight of 2. A separate but important influence that can possibly affect the weight percentage allocated is the size of the institution. The size can affect resource and funding availability, and the capability of the workforce that would be involved in implementing the activities.

Table 9.3: Weight Percentage Range

Value Range	Percentage	Weight
-40 to -31	75%	4
-30 to -21	65%	
-20 to -11	55%	3
-10 to -1	45%	
0 to 10	35%	2
11 to 20	25%	
21 to 30	15%	1
31 to 40	5%	

9.3.2 USE CASE IMPLEMENTATION

To demonstrate how an E-Health institution can implement the activities of CCSCF to determine its maturity towards the establishment of a cybersecurity culture, a case reference is used as an example. A single case implementation example is considered appropriate because the study did not follow a design science research process, which requires demonstrating and analysing multiple cases or scenarios (McLaren et al., 2011).

The case of the Mpumalanga Province (MP) Department of Health, used for the demonstration in this chapter, was also used during the data collection. The research interviewed the same participants as for the qualitative data collection. As a result, the same criteria were adhered to for participant selection as in the qualitative study described in Chapter 7. The case evaluation of CCSCF used information obtained from ICT personnel, namely the manager, as well as the support, system and server administrative staff. The participants had to be ICT personnel of the MP Department of Health, have experience (have worked in the environment for two years and above), and have a good understanding of the ICT-related issues of that department.

The Mpumalanga Department of Health was chosen as the implementation case because the ICT staff who participated in the interview emphasised the importance of having a strong cybersecurity culture that guides the healthcare institutions in the province.

Additionally, the interviewees indicated the importance of staff being aware, knowledgeable, and willing to adopt a positive attitude to cybersecurity and cybersecurity-compliant behaviour. This indicates a willingness to broaden their focus instead of focusing almost exclusively on providing medical care as the department currently does.

As in other provinces, the Mpumalanga Department of Health must protect its critical resources like ICT systems, data and patients' lives from cyber-attacks. According to the security reports by the South African Department of Health, the Mpumalanga Department of Health is one of the provinces with the lowest security score (Department of Health, 2012c, 2012d).

There is global agreement that security is the responsibility of the government of every nation (International Telecommunication Union (ITU), 2008a, 2021; Wamala, 2011). The South African government confirm this by indicating that national security cannot be achieved if there is no culture of cybersecurity. This resulted in the country developing and approving the National Cybersecurity Policy Framework (NCPF) (State Security Agency, 2015).

The NCPF re-emphasised the importance of a cybersecurity culture to achieve national security; hence, one of its key objectives is to “promote a culture of cybersecurity” (State Security Agency, 2015). Mpumalanga is one of the provinces that received a poor assessment in the Healthcare Security Audit Reports (Department of Health, 2012c, 2012d). This implies that the province's Department of Health is failing to lead and be accountable for implementing a cybersecurity culture to achieve national security in South Africa.

To address this, the province's health department needs to be aware of the severe cost, operational and reputational implications that cyber threats could have on them. This requires them to share information widely about the importance of having a cybersecurity culture that meets basic cybersecurity activities.

Considering the many factors that influence the cultivation of cybersecurity culture (Branley-Bell et al., 2021; Huang & Pearlson, 2019; Uchendu et al., 2021), the growing cyber threats targeting healthcare institutions (Coventry & Branley, 2018; e-Estonia, 2018), and the significance of cybersecurity culture in terms of national security (State Security Agency, 2015), the province's department of health should not allow the current state of poor information security and cybersecurity to continue.

Mpumalanga needs to be seen as a province that strives to contribute to the nation's security through its efforts to achieve a strong cybersecurity culture. Therefore, in their attempt to promote cybersecurity culture, the province's Department of Health should determine the maturity level of their cybersecurity culture by implementing the CCSCF.

Table 9.4 to

It can be challenging for E-Healthcare institutions to improve the elements of EENOM, like rules and regulations, as they are not in direct control of their activities. However, the institutions can strategically focus interest on improving compliance with the activities of the element to achieve and optimise a culture of cybersecurity.

The activity scores of external environmental and non-organisational management (EENOM) elements had reputational damage and Healthcare industry rules as the activities with the lowest priority (see Table 9.7). Most of the activities of the external environmental and non-organisational management (EENOM) had identical high-priority scores. The Healthcare industry's current capability level was 51, and its intended capability was 68.8.

Table 9.7 shows Mpumalanga province's Department of Health capability profiles, maturity level, gap, associated weight and priorities based on the activities of CCSCF elements. The elements pertaining to IOM (see Table 9.4) are leadership, cybersecurity governance, business continuity, organisational learning, physical security and communication channel.

Table 9.5 and

Table 9.6 depict the human preparedness and responsibility, and the technology elements covered. These are cybersecurity competency, cybersecurity awareness, communication and information sharing, cybersecurity attitude, cybersecurity behaviour, ICT infrastructures, frequent change in ICT, and outsourcing of ICT systems. The EENOM elements covered in

It can be challenging for E-Healthcare institutions to improve the elements of EENOM, like rules and regulations, as they are not in direct control of their activities. However, the institutions can strategically focus interest on improving compliance with the activities of the element to achieve and optimise a culture of cybersecurity.

The activity scores of external environmental and non-organisational management (EENOM) elements had reputational damage and Healthcare industry rules as the activities with the lowest priority (see Table 9.7). Most of the activities of the external environmental and non-organisational management (EENOM) had identical high-priority scores. The Healthcare industry's current capability level was 51, and its intended capability was 68.8.

Table 9.7 are legal aspects and litigation, national culture, hospital location, rules and regulations and reputational damage.

The implementation shown in this chapter is based on qualitative data. The results of CCSCF activities in Table 9.4 to

It can be challenging for E-Healthcare institutions to improve the elements of EENOM, like rules and regulations, as they are not in direct control of their activities. However, the institutions can strategically focus interest on improving compliance with the activities of the element to achieve and optimise a culture of cybersecurity.

The activity scores of external environmental and non-organisational management (EENOM) elements had reputational damage and Healthcare industry rules as the activities with the lowest priority (see Table 9.7). Most of the activities of the external environmental and non-organisational management (EENOM) had identical high-priority scores. The Healthcare industry's current capability level was 51, and its intended capability was 68.8.

Table 9.7 were based on the interview data from ICT respondents.

Table 9.4 shows scores related to the activities of internal organisation management (IOM) elements. These scores were used to identify the cybersecurity culture activities that needed to have the highest priorities as such priorities alert management that the item (activity) requires urgent action. Items with low priority indicate activities that need less urgent action.

Table 9.4: MP Department of Health Capability Profile for the Activities of IOM Elements

Elements	Activities keywords & Groundedness (G)	Present		Intended		Capability gap (CG)	Weight (W)	Priority (W * CG)
		Capability Profile	Maturity	Capability Profile	Maturity			
Leadership	Leaders interest & attention [-29]	[35.5]	[2]	[58.5]	[3]	[23.0]	[4]	[92]
	Provision of resources [-24]	[38]	[2]	[62.7]	[3]	[24.7]	[4]	[98.8]
	cybersecurity culture Champion/team [-18]	[41]	[2]	[63.7]	[3]	[22.5]	[3]	[67.5]
	Management involvement & support [-16]	[42]	[2]	[65.1]	[3]	[23.1]	[3]	69.3]
	CS sub-budget [-16]	[42]	[2]	[65.1]	[3]	[23.1]	[3]	[69.3]
CS governance	CS Policy [-7]	[46.5]	[2]	[67.4]	[3]	[20.9]	[3]	[62.7]
	Simulated activities [-6]	[47]	[2]	[68.1]	[3]	[21.1]	[3]	[63.3]

Elements	Activities keywords & Groundedness (G)	Present		Intended		Capability gap (CG)	Weight (W)	Priority (W * CG)
		Capability Profile	Maturity	Capability Profile	Maturity			
	CS governance structure [-6]	[47]	[2]	[68.1]	[3]	[21.1]	[3]	[63.3]
	User restrictions & password management [-6]	[47]	[2]	[68.1]	[3]	[21.1]	[3]	[63.3]
	Plan towards cybersecurity culture [-6]	[47]	[2]	[68.1]	[3]	[22.0]	[3]	[66]
	Compliance Monitoring & evaluation [-2]	[49]	[2]	[71.0]	[3]	[19.0]	[3]	[57]
Business continuity	Vulnerability management [-9]	[45.5]	[2]	[65.9]	[3]	[20.4]	[3]	[61,2]
	Contingency plan [-6]	[47]	[2]	[68.1]	[3]	[21.1]	[3]	[63.3]
	Risk assessment [-4]	[48]	[2]	[67.6]	[3]	[21.6]	[3]	[64.8]
Organisational learning	Learning process levels [-7]	[46.5]	[2]	[67.4]	[3]	[20.9]	[3]	[62.7]
	Build & retain CS [-4]	[48]	[2]	[69.6]	[3]	[21.6]	[3]	[64.8]
Physical Security	Data protection measures [+1]	[50.5]	[3]	[68.1]	[3]	[17.6]	[2]	[35.2]
	Server network integrity [+2]	[51]	[3]	[68.8]	[3]	[17.8]	[2]	[35,6]
	Access to assets [+3]	[51.5]	[3]	[69.5]	[3]	[18.0]	[2]	[36]
Communication channel	Channel and network [-4]	[48]	[2]	[69.6]	[3]	[21.6]	[3]	[64.8]
	Intranet & websites [+2]	[51]	[3]	[68.8]	[3]	[17.8]	[2]	[35.6]

Elements	Activities keywords & Groundedness (G)	Present		Intended		Capability gap (CG)	Weight (W)	Priority (W * CG)
		Capability Profile	Maturity	Capability Profile	Maturity			
	Meetings [+9]	[54.5]	[3]	[73.5]	[3]	[19.0]	[2]	[38]

As seen in (Table 9.4) the activity with the highest priority (98.8) was the provision of resources. This is an activity under the leadership element of internal organisation management (IOM). Leaders' interest and attention activity, also a leadership element, with a priority of 92, was the second most urgent. The lowest priority was found to be data protection measures, an activity belonging to the physical security element. The current capability profile for the provision of resources was 38, with a capability target of 62.7. The current capability profile of data protection measures was 50.1, with a capability target of 68.1.

For cybersecurity culture to be implemented effectively, there was an urgent need for improvement in the provision of resources and leaders' attention. It is of interest that all the other activities of the leadership element also seemed to require quite urgent action for effective cybersecurity culture implementation. This was followed by the various activities associated with the CS governance, business continuity and organisational learning elements.

Although the data security measure was the activity with the lowest priority score among the elements of the internal organisation management (IOM) theme, institutions still needed to improve it and the activities of physical security, leadership and communication channel that had fairly low priorities.

Table 9.5: MP Department of Health Capability Profile for the Activities of Human Preparedness (P) and Responsibility (R) Elements

Elements	Activities keywords & Groundedness (G)	Present		Intended		Capability gap (CG)	Weight (W)	Priority (W * CG)
		Capability Profile	Maturity	Capability Profile	Maturity			
CS competency	CS training & education [-36]	[32]	[2]	[56]	[3]	[24]	[4]	[96]
	Knowledge & understanding of threats [-20]	[40]	[2]	[66]	[3]	[26]	[3]	[78]
	Knowledge of national policy frameworks [-5]	[47.5]	[2]	[68.8]	[3]	[21.3]	[3]	[63.9]
	Informal education [-1]	[49.5]	[2]	[71.7]	[3]	[22.2]	[3]	[66.6]
	Collaboration & engagement CS training [-1]	[49.5]	[2]	[71.7]	[3]	[22.2]	[3]	[66.6]
CS awareness	purpose, policy, roles & threats [-34]	[33]	[2]	[57.7]	[3]	[24.7]	[4]	[98.8]
	Old & new practice [-4]	[48]	[2]	[69.6]	[3]	[21.6]	[3]	[64.8]
Communication and information sharing	Platform [-6]	[47]	[2]	[68.1]	[3]	[21.1]	[3]	[63.3]
	CS incident record [-4]	[48]	[2]	[69.6]	[3]	[21.6]	[3]	[64.8]
	Right channels [+2]	[51]	[3]	[68.8]	[3]	[17.8]	[2]	[35.6]
CS attitude	Positive attitude [-8]	[46]	[2]	[66.7]	[3]	[20.7]	[3]	[62.1]
	Willingness [-7]	[46.5]	[2]	[67.4]	[3]	[20.9]	[3]	[62.7]

Elements	Activities keywords & Groundedness (G)	Present		Intended		Capability gap (CG)	Weight (W)	Priority (W * CG)
		Capability Profile	Maturity	Capability Profile	Maturity			
	Resistance to change [-4]	[48]	[2]	[69.6]	[3]	[21.6]	[3]	[64.8]
CS behaviour	Inappropriate CS behaviours [-6]	[47]	[2]	[68.1]	[3]	[21.1]	[3]	[63.3]
	CS priorities [-6]	[47]	[2]	[68.1]	[3]	[21.1]	[3]	[63.3]
	Simplification of CS concept, behaviour & expectations [-3]	[48.5]	[2]	[70.3]	[3]	[21.8]	[3]	[65.4]
	Consciousness [-1]	[49.5]	[2]	[71.7]	[3]	[22.2]	[3]	[66.6]

The scores related to the activities of human preparedness (P) and responsibility (R) elements are depicted in Table 9.5. The activities' purpose, policy, roles & threat and CS training & education from the CS awareness and competency elements showed the highest priority values. The activities scored 98.8 and 96, respectively, as their priority. The communication and information-sharing activity, namely the right channel, had the lowest priority score of 35.6.

The current and target capability profiles of the purpose, policy, roles & threat activity were 33 and 57.7. The current and target capability profiles of CS training & education were 32 and 56. The current capability level was 51, and the intended capability was 68.8 for the right channel activity.

The highest priority scores on the CS awareness and CS competency elements reflected that critical actions were needed to improve members' cybersecurity skills and knowledge to create a culture of CS. However, it was still necessary to maintain and improve work on communication and sharing of CS information to create a better culture, even though the activity was reported to have the lowest priority.

Additionally, continual reinforcement and alignment with best practices remain necessary to mitigate potential risks from human factors. Generally, there was a need for improvement to achieve the desired targets for the activities of human preparedness (P) and responsibility (R) elements, although they showed reasonably good and very similar scores.

Table 9.6 depicts the scores of activities associated with technology (TECH) elements. All the activities of technology (TECH) elements, except for the legacy system, obtained notable and almost equal priority scores. Old and outdated ICTs had the lowest priority score, with a minimal margin compared to other technology (TECH) elements.

The results indicated that all technology (TECH) activities need equal improvement action to implement a cybersecurity culture successfully. For example, actions like investment in ICT infrastructure, management of stakeholder requirements, stability, and adaptability measures to minimise disruptions and ensure seamless operations.

Table 9.6: MP Department of Health Capability Profile for the Activities of Technology (TECH) Elements

Elements	Activities keywords & Groundedness (G)	Present		Intended		Capability gap (CG)	Weight (W)	Priority (W * CG)
		Capability Profile	Maturity	Capability Profile	Maturity			
ICT infrastructures	Legacy system [-3]	[48.5]	[2]	[70.3]	[3]	[21.8]	[3]	[65.4]
	Adequate ICT infrastructures [-2]	[49]	[2]	[71]	[3]	[22.0]	[3]	[66]
	ICT budget [-2]	[49]	[2]	[71]	[3]	[22.0]	[3]	[66]
Frequent changes in IT	Software update & maintenance [-1]	[49.5]	[2]	[71.7]	[3]	[22.2]	[3]	[66.6]
	Continuous investment [-1]	[49.5]	[2]	[71.5]	[3]	[22.0]	[3]	[66]
Outsourcing of the IT system	Standards & outcomes [-1]	[49.5]	[2]	[71.7]	[3]	[22.2]	[3]	[66.6]
	CS requirement assessments [-1]	[49.5]	[2]	[71.7]	[3]	[22.2]	[3]	[66.6]

It can be challenging for E-Healthcare institutions to improve the elements of EENOM, like rules and regulations, as they are not in direct control of their activities. However, the institutions can strategically focus interest on improving compliance with the activities of the element to achieve and optimise a culture of cybersecurity.

The activity scores of external environmental and non-organisational management (EENOM) elements had reputational damage and Healthcare industry rules as the activities with the lowest priority (see Table 9.7). Most of the activities of the external environmental and non-organisational management (EENOM) had identical high-priority scores. The Healthcare industry's current capability level was 51, and its intended capability was 68.8.

Table 9.7: MP Department of Health Capability Profile for the Activities of EENOM Elements

Elements	Activities keywords & Groundedness [G]	Present		Intended		Capability gap (CG)	Weight (W)	Priority (W * CG)
		Capability Profile	Maturity	Capability Profile	Maturity			
Legal aspects and litigation	External communication lines [-1]	[49.5]	[2]	[71.5]	[3]	[22.2]	[3]	[66.6]
	Legal implications [-1]	[49.5]	[2]	[71.5]	[3]	[22.2]	[3]	[66.6]
National culture	National differences [-4]	[48]	[2]	[69.6]	[3]	[21.6]	[3]	[64.8]
Hospital location	External connection [-1]	[49.5]	[2]	[71.5]	[3]	[22.2]	[3]	[66.6]
	Internal departments [-1]	[49.5]	[2]	[71.5]	[3]	[22.2]	[3]	[66.6]
Rules and regulations	Government laws & regulations [-5]	[47.5]	[2]	[68.8]	[3]	[21.3]	[3]	[63.9]
	Healthcare industry rules [+2]	[51]	[3]	[68.8]	[3]	[17.8]	[2]	[35.6]
Reputational damage	Trust [0]	[50]	[2]	[67.5]	[3]	[17.5]	[2]	[35]

Addressing the highest priority scores across the activities of external environment and non-organisational management (EENOM) elements implies that critical actions are needed across those activities. This will help guide against the negative impact of the element in the process of implementing cybersecurity culture.

It is necessary for institutions to focus their strategies, resource allocation, and organisational alignment on activities that are of high priority. This is predicted to be instrumental in enhancing overall resilience, cybersecurity posture and operational effectiveness, thereby helping to achieve a strong cybersecurity culture in the institution.

In addition to focusing on high-priority activities, an institution's allocation of resources plays a critical role in deciding which of the other activities to focus on. For example, institutions with limited resources may focus on only a small number of activities, those with very high priorities. On the other hand, well-resourced institutions could focus on all the activities with any priority or above a particular stipulated priority.

The previous section presented the use case implementation profile as the first evaluation method of the proposed framework. The following section presents a comparative analysis of the second CCSCF evaluation method.

9.4 COMPARATIVE ANALYSIS

Comparative analysis focuses on identifying the similarities and differences between the variables or cases being compared (Pickvance, 2001). This study conducted a comparative analysis to assess the similarities and differences between the CCSCF developed in Chapter 8 and related frameworks. Hence, the comparative analysis evaluated the CCSCF.

Conducting a comparative analysis helped to portray aspects of the developed framework that were lacking (weaknesses) or not indicated by other cybersecurity culture frameworks (strengths) (see Chapter 4). Hence, in this case, the comparative analysis compared the usefulness of the CCSCF against other similar frameworks.

The measures for the comparative analysis are presented in **Section 9.4.1**.

9.4.1 COMPARISON MEASURES

The comparative measures are based on the cybersecurity culture components and their associated factors (which can be regarded as the requirements for the components) derived during data collection and analysis (see Chapter 6 and Chapter 7).

Figure 9.4 presents an overview of the CCSCF. The themes of the framework are Internal Organisational Management (IOM), human preparedness (P) and responsibility (R), Technology (TECH), and External Environmental and Non-Organisational Management (EENOM).

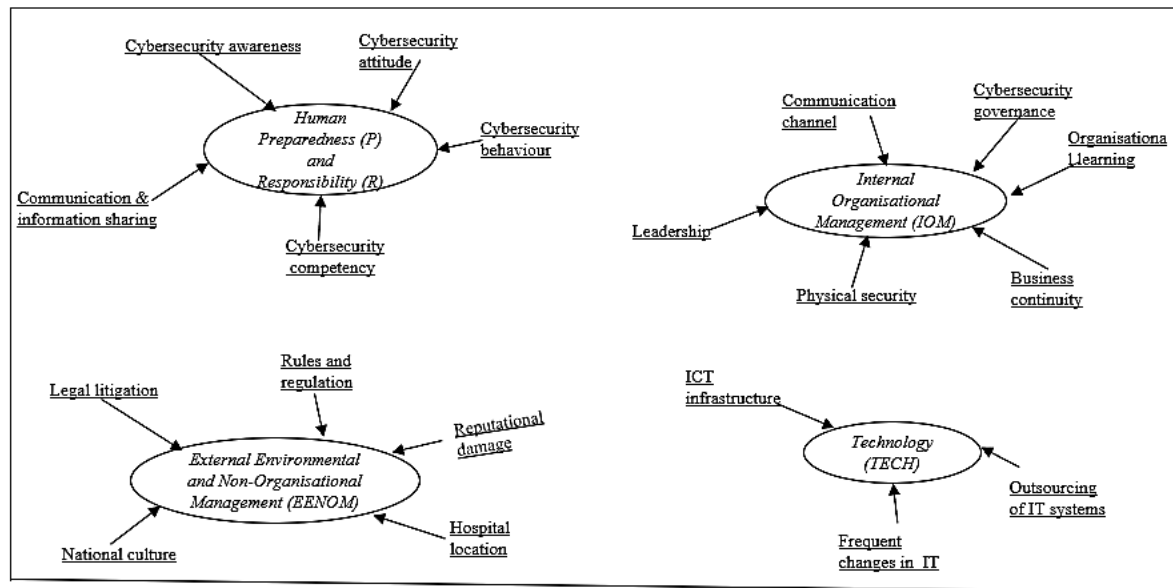


Figure 9.4: Overview of CCSCF Elements for Comparison (own source)

- Regarding the human preparedness (P) and responsibility (R) themes, the CCSCF was compared with existing frameworks by examining the following elements: cybersecurity awareness, cybersecurity competency, communication and information sharing, attitude, and cybersecurity behaviour.
- When the focus of the comparative analysis was on the Internal Organisational Management (IOM) theme, the comparison was between the elements: leadership, business continuity, cybersecurity governance, communication channels, organisational learning, and security.
- For the Technology (TECH) theme, the CCSCF was compared with other frameworks according to the following: frequent changes to IT, ICT infrastructure issues, and outsourcing of IT systems.
- For the External Environmental and Non-Organisational Management (EENOM) theme, rules and regulations, external body, hospital Location, national culture, and reputational damage were compared.

9.4.2 COMPARATIVE ANALYSIS AGAINST EXISTING FRAMEWORKS

This section compares the critical elements of CCSCF against the existing frameworks. Table 9.8 to Table 9.10 compared the existing framework with the various factors of the proposed framework components. Table 9.8 compares critical internal organisational management (IOM) factors with the frameworks discussed in Chapter 4.

Table 9.8: IOM Comparative Factor Analysis for the Proposed Framework

Factors Frameworks	Leadership	Business continuity	Communication channels	Cybersecurity governance	Organisational learning	Physical security
	Internal Organisational Management (IOM)					
CCSCF	√	√	√	√	√	√
CSC FAOR	√	√#	√	√	√	√
SCM	√#	√	√	√	√	x
Ocybersecurity culture	√#	x	√	√	√	x
HFD	√#	x	√	√	x	x
STOPE	√#	x	√	√	x	x
Legend	√ = addressed X = not addressed				√# = partly addressed ? = not known	

Table 9.8 shows that all frameworks supported or partly supported features related to leadership and cybersecurity governance. This shows the importance of the factors in establishing and maintaining an institution's culture of cybersecurity. This finding reaffirms the significance of these Internal Organisational Management (IOM) factors as the starting point of cybersecurity culture development in E-Health institutions. The partly addressed symbol under leadership indicates that a particular framework may not support all the elements that make up the leadership factor, but it does support other elements.

CSC FAOR accommodated the business continuity, cybersecurity governance and physical security factors. SCM supported business continuity and cybersecurity governance, while Ocybersecurity culture used only cybersecurity governance. All frameworks supported the communication channel factor. Organisational learning was not supported by either the HFD or STOPE frameworks.

Table 9.9 compares human preparedness and responsibility factors with other frameworks.

Table 9.9: Human Preparedness and Responsibility Factor Comparative Analysis

Factors Frameworks	Awareness	Cybersecurity competency	Communication and information sharing	Attitude	Cybersecurity Behaviour
	Human Preparedness (P) and Responsibility(R)				
CCSCF	√	√	√	√	√
CSC FAOR	√	√	x	√	√#
CSCM	√	√#	√	√	x
Ocybersecurity Culture	√	√	x	√	√#
HFD	√	√	x	x	√
STOPE	√	√	√	x	√#
Legend	√ = addressed X = not addressed			√# = partly addressed ? = not known	

Table 9.9 shows that the other frameworks included significant factors of the human preparedness (P) and responsibility (R) themes. However, none of these contained *all* the factors that characterise human preparedness (P) and responsibility (R). For example, priority given to medical tasks is an element under cybersecurity behaviour, but none of the existing frameworks accommodate it. Hence, the cybersecurity behaviour elements of all the frameworks are indicated as being only partly addressed.

Communication and information-sharing elements were supported by SCM and STOPE but not by the other frameworks. Since none of the frameworks supported the element of priority given to medical tasks, it is clear that the focus of these frameworks was not on E-Health institutions. This strongly emphasises the importance of context in cybersecurity culture.

Other factors not supported by some frameworks were attitude and cybersecurity behaviour. In the OCybersecurity Culture Framework, the human behaviour factor was not explicitly highlighted. Instead, human characteristics that influence behaviour, such as beliefs and values, supported the factor.

Table 9.10: Human Preparedness and Responsibility Factor Comparative Analysis

Factors Frameworks	ICT infrastructure	Frequent change in ICT	Outsourcing of ICT systems	Legal aspects and litigation	Hospital location	External body	Rules and regulation	Reputational damage	National culture
	Technology (TECH)			External Environmental and Non-Organisational Management (EENOM)					
CCSCF	√	√	√	√	√	√	√	√	√
CSC FAOR	√	x	x	x	x	√	x	√	√
SCM	x	√	x	x	x	x	√	√	x
Ocybersecurity Culture	x	x	x	x	x	x	√	√	√
HFD	x	x	x	x	x	x	√	x	√

STOPE	√	x	√	x	x	x	√	x	√
Legend	√ = addressed X = not addressed			√# = partly addressed ? = not known					

Table 9.10 compares Technology (TECH) and External Environmental and Non-Organisational Management (EENOM) factors with the components of existing frameworks. For the comparison of technology (TECH) factors, it is evident that none of the frameworks covered frequent change in ICT, except for SCM. However, the factor was only accommodated as a component of environmental influence in the SCM framework.

The same goes for the outsourcing of ICT systems. None of the frameworks supported it other than STOPE. STOPE supported all technology factors but did not mention a frequent change in ICT. The CSC FAOR, Ocybersecurity culture and HFD frameworks did not refer to technology at all.

Based on the factors of the EENOM theme identified in this study, rules and regulations and national culture appeared as the favoured elements of the external environment theme. This was supported by the number of frameworks that supported the factor. The factor of reputational damage followed as the factor supported frequently (second) by most of the frameworks. Neither of the frameworks supported the factor of location of the hospital, while the external body is only supported by CSC FAOR.

9.4.3 SUMMARY OF THE FRAMEWORK COMPARISON

In summary, the comparison (see Table 9.8 to Table 9.10) showed that none of the frameworks specify all the factors that characterise the framework of this study, CCSCF. Among the factors not supported by other frameworks or only supported by one framework are *priority on medical, business continuity, risk assessment, security governance, physical security, frequent change to IT, outsourcing, hospital location, legal aspects and litigation, and external body*. These re-emphasise the significance of context in the development of cybersecurity culture.

These factors, among others, are essential to cybersecurity culture. However, the fact that other frameworks, particularly cybersecurity culture frameworks, do not define or support all the features included in the CCSCF renders them unsuitable for being adopted without supplementation to establish cybersecurity culture in the public E-Health institutions investigated.

Comparative analyses focus on identifying the similarities and differences between the variables or cases being compared (Pickvance, 2001). In this study, a comparative analysis was conducted to evaluate the CCSCF developed in Chapter 8 against existing cybersecurity culture frameworks, highlighting both strengths and weaknesses. The evaluation considered four main themes of the CCSCF: Internal Organisational Management (IOM), Human Preparedness and Responsibility (P and R), Technology (TECH), and External Environmental and Non-Organisational Management (EENOM), and measures were derived from the components and associated factors identified (see Chapters 6 and 7).

For IOM the analysis considered leadership, business continuity, cybersecurity governance, communication channels, organisational learning, and physical security; for P and R the analysis considered cybersecurity awareness, competency, communication and information sharing, attitude, and cybersecurity behaviour; for TECH the analysis considered frequent changes in IT, ICT infrastructure, and outsourcing; and for EENOM the analysis considered rules and regulations, external bodies, hospital location, national culture, reputational damage, and legal aspects (Siponen et al., 2014).

The comparison revealed that while frameworks such as CSC FAOR, SCM, Ocybersecurity culture, HFD, and STOPE each addressed some of these factors (see Tables 9.8 to 9.10), none of them encompassed all elements of the CCSCF. Notably, leadership and cybersecurity governance were widely supported by those existing frameworks, but business continuity, priority given to medical tasks, frequent IT changes, outsourcing, hospital location and legal considerations were largely neglected. This reflected gaps in contextual applicability to E-Health institutions (Alshaikh et al., 2020). Moreover, the CCSCF uniquely integrates factors; for example, human behaviour is influenced by medical task prioritisation and external environmental influences, but these influencing factors are either absent or only partially addressed in other frameworks.

This comprehensive inclusion enhanced the contextual relevance and practical utility of the CCSCF, distinguishing it from previous models and reinforcing the importance of developing cybersecurity culture frameworks tailored specifically for public E-Health institutions (Hadlington, 2018; Siponen et al., 2014). Overall, the comparative analysis demonstrated that the CCSCF provides a more complete and contextually appropriate framework for establishing cybersecurity culture than currently available alternatives.

Now that the second evaluation method has been discussed, the chapter presents evaluation results derived from expert reviews. The expert reviews aimed to get cybersecurity experts' views on the CCSCF developed in this study to establish a cybersecurity culture in public E-Health institutions.

9.5 EXPERT REVIEWS

An expert review is used as the third evaluation approach for the CCSCF. It is an evaluation process that uses experts in the field of study to evaluate or review the developed artefacts to affirm or improve them (Offermann et al., 2009; Salah et al., 2014). The experts should include those not involved in creating the artefacts (Salah et al., 2014). The use of expert review as an approach to evaluating the viability of artefacts was also supported by Peffers et al (2012, 2014).

As depicted in **Figure 5.10** in Chapter 5, the expert review was the research instrument outlined for achieving Round 3 data collection in this study. Additionally, expert review is a recommended evaluation approach for case study research due to the limited sample size (Offermann et al., 2009). Hence, the researchers undertaking this study deemed it appropriate to use expert reviews as an additional approach for evaluating the proposed framework. The objective was to have the cybersecurity or cybersecurity culture experts assess the CCSCF and give their opinions and contributions to improving the framework.

9.5.1 EXPERT REVIEWS INSTRUMENT

The expert's evaluation was achieved through semi-structured one-on-one interviews. The interview provided respondents the opportunity to ask the interviewer questions freely during the interview process. The interview questions (see Google Forms footnote link) were developed before the interviews with the participants commenced.

The interview was used to collect qualitative data from cybersecurity experts as strategic participants for the review of the CCSCF. This was because the experts were an appropriate group to speak to regarding the topic of cybersecurity culture addressed in this study.

Google Forms was the software employed to develop the Round 3 data collection instrument and to analyse the data. Google Forms² is a free service for online survey administration offered by Google. The platform enabled the researcher to develop the instrument, which was shared with the interviewee during the interview.

The questions answered in the expert review interviews were grouped under five main headings: principles, objectives, comprehensiveness, relevance and applicability. Each had a minimum of one and a maximum of five questions. This excluded the first question, which was used to gather the reviewers' profiles.

The different aspects covered in the questions used to obtain the participants' views on the framework were:

- **Evaluation aspect 1: Principles.** This section asked questions to assess the framework's core principles. The principal aspect consisted of five questions.
- **Evaluation aspect 2: Objectives** was made up of three questions. The questions asked in this section collected the opinions and perceptions of the cybersecurity experts on the objectives of CCSCF.

² https://docs.google.com/forms/d/1_P7Y-1LViPFP2nZbD6uqaclbeY1eVeFmO5aqlzAihz0/viewform?edit_requested=true#responses

- **Evaluation aspect 3:** This section solicited the opinions of the experts on the comprehensiveness of the framework. Three questions were placed under this section.
- **Evaluation aspect 4:** This section used five questions to obtain the experts' views on the framework's relevance and applicability.
- **Evaluation aspect 5:** This section was used to encourage the interviewee to add general comments and suggestions on how the framework can be improved.

9.5.2 SELECTION OF EXPERTS

Purposive sampling (see Chapter 5) was applied to select the expert review participants. The sample included people working in the area of cybersecurity or cybersecurity culture in the academic and industry sectors. The sample had content experts and those with experience in cybersecurity who could provide informed and insightful answers to the questions for the evaluation of the CCSCF.

The following were considered before a participant was selected:

- The participant's area of expertise. Only participants whose area of expertise was cybersecurity or cybersecurity culture were selected.
- Availability of the expert participant;
- Participant's willingness to take part in the evaluation, and
- Participants' years of experience in the research area (must have at least five years' experience working in cybersecurity or the cybersecurity culture domain).

A total of ten experts were approached telephonically or via email to seek their willingness to participate in the one-on-one interview to evaluate the framework. Nine out of the 10 participants approached indicated their willingness to assist with the evaluation. However, only eight out of the nine were available and participated in the interview. After the interview, one participant withdrew, citing a lack of necessary expertise for the research area, resulting in seven as the final number of participants.

The number of selected participants falls within the range (one to thirty) considered to be a sufficient number of data sources (Fridlund & Hildingh, 2000). The concept of saturation also influenced the number of experts selected and who participated in the review (Dworkin, 2012; Marshall, 1996; Mason, 2010).

Table 9.11 depicts the summary of experts that participated in the one-on-one interview.

Table 9.11: Expert Review Participants

Reviewers	Sector	Expert job title and area	Organisations
Expert 1	Industry	Expert in cybersecurity	National: Air Traffic and Navigation Services (ATNS)
Expert 2	Academia	Professor in the area of cybersecurity awareness	National: University of South Africa (UNISA)
Expert 3	Academia	Associate Professor Cybersecurity Forensic	International: Mountain Top University and Cybersecurity Experts Association of Nigeria (CSEAN)
Expert 4	Research Institute	Research group leader in cybersecurity governance and privacy	National: Council for Scientific and Industrial Research (CSIR)
Expert 5	Industry & Academia	Expert in cybersecurity	National: ATNS and University of Johannesburg (UJ)
Expert 6	Academia	Associate Professor in cybersecurity and Cybersecurity Culture	National: Nelson Mandela University (NMU) and founder of the Cyberculture Foundation
Expert 7	Industry & Academia	Expert in cybersecurity	International: Cybersecurity for Society (iCSS) University of KENT UK and cybersecurity banking & consulting

Table 9.11 shows that the participants were selected from different sectors. They possessed diverse job titles and came from various organisations. This ensured that the framework was evaluated based on the broad understanding of diverse expert participants and helped produce a varied and comprehensive evaluation of the framework.

9.5.3 INTERVIEW PROCESS

This section documents the process followed in conducting the interviews with the experts, answering the questions, and submitting the responses.

- Communication and formal letter

After an expert was identified, the researcher established communication with them by sending an email or having a phone conversation to confirm their willingness to participate in the review. After that, a formal letter that contained detailed information on the review and a high-level overview of the framework was sent to the expert. The letters requested the experts to respond with an indication of a date and time when they were available for an interview.

- Interview platform and consent letter

The interview was conducted virtually through the Microsoft Teams platform because the experts came from a variety of cities, provinces and countries. The online Teams platform allowed the researcher to record the interview and obtain a transcription later.

An informed consent document was sent to the participants on the interview day. Only participants who gave consent received the Google link containing the interview questions to enable them to answer them. The consent letter was sent to the interviewee 10 to 15 minutes before the commencement of the interview. The participants were reminded that participation in the interview was voluntary and that they were free to withdraw at any point during the interview.

- Interview duration

The interview took a maximum of one hour. The researcher used the first 30 minutes to provide the expert with an overview of the CCSCF. The purpose was to help them understand the framework and its context and to ask any questions for clarification. The interviewee used the remaining 30 minutes to complete the interview questions, which had been designed based on the framework's objectives, principles, comprehensiveness, relevance and applicability.

- Completion and submission of interview questions

The participants completed the questions by clicking the Google link emailed during the interview. Both the researcher and interviewee remained online while the questions were being completed. The interviewee could also ask further clarification questions while completing written responses to the questions.

The participant's responses were submitted automatically to a Google spreadsheet, where all the data were captured. The Google sheet arranged answers in rows and used diagrams to summarise some questions. Each row represented a response from a participant. Using Google Forms made it easy to capture all responses in one spreadsheet, which helped with analysing the responses.

The results of the interview are discussed in the next section.

9.5.4 ANALYSIS OF EXPERT REVIEWS

As indicated in Chapter 4, the method used to analyse the data from expert reviewers was qualitative content analysis, allowing the researcher to derive meaning from textual data collected, and hence to draw conclusions from the evaluation of the CCSCF (Krippendorff, 2004).

The data collected was cleaned by removing the responses of the participants who withdrew from participation and by identifying incomplete answers, incorrectly spelt words and any other errors.

The results obtained from the reviews are discussed below, starting with the participants' profiles.

- Participants profiles

Table 9.12 depicts the profiles of the expert reviewers who participated in the evaluation.

Table 9.12: Participants' Sector, Job and Area Frequency

Number Reviewers	Sector	Job title	Area
1	Industry	Cybersecurity expert	Cybersecurity
3	Academia	Professor and associate Professors	Cybersecurity awareness, cybersecurity forensics, and Cybersecurity Culture
1	Research Institute	Cybersecurity expert	Cybersecurity
2	Industry & Academia	Research leader	Cybersecurity governance and privacy

Table 9.12 shows that participants were from industry, academia, research institutions and a combination of industry and academia. Table 9.12 also shows that the reviewers hold different job titles; there were Professors, Associate Professors, Research Leaders and general experts in cybersecurity. The reviewers gave their main areas of interest as cybersecurity awareness, governance, forensics and cybersecurity culture.

Selecting participants from more than one sector, with different job titles and areas of interest, helped ensure the CCSCF was evaluated by a variety of experts with a broad knowledge base. This assisted in producing a multifaceted and comprehensive evaluation of the framework.

Table 9.13: Number of Participants per Organisation Type

Number of Expert Reviewers	Type of Organisations	Name of Organisation
3	South African university	University of South Africa (UNISA), Nelson Mandela University (NMU), and University of Johannesburg (UJ)
2	University not South African	Mountain Top University and Cybersecurity for Society (iCSS) University of KENT UK
1	South African research institute	Council for Scientific and Industrial Research (CSIR)
1	South African institute	Air Traffic and Navigation Services (ATNS)

Table 9.13 shows that the reviewers came from different organisations within South Africa and internationally. Three reviewers were from universities within South Africa: Unisa, NMU, and UJ. Two were from international universities, Kent, United Kingdom (UK) and Mountain Top University, Nigeria. One came from a research institution, CSIR, and the remaining one was not affiliated with any university. The combination of participants from different locations was essential for this research as it helped provide an evaluation from a diverse group of cybersecurity experts.

Table 9.14: Reviewers' Qualifications and Years of Experience

Num Reviewers	Qualification	Years of experience
5	PhD	10 to 25 years
2	Master's busy with PhD	9+ year

Table 9.14 depicts the qualifications and years of experience of the reviewers. Table 9.14 shows that the CCSCF was evaluated by experts with many years of experience in cybersecurity. The majority (five) of the reviewers hold PhD qualifications, while the other two were busy studying towards a PhD. This information is crucial as it shows that the reviewers possess considerable knowledge, skill and experience in cybersecurity and positions them as appropriate participants to evaluate and contribute positively to the proposed CCSCF.

As indicated in **Section 9.5.1**, the review questions examined five aspects of principles: objective, comprehensiveness, relevance, applicability and general. The results obtained from the questions are discussed below.

9.5.4.1 Evaluation Aspect 1: Principles

“Does the Contextual Cybersecurity Culture Framework (CCSCF) use commonly understood themes and elements, avoiding unnecessary technical jargon?”

The result revealed that all the reviewers agreed that CCSCF used commonly understood themes and elements. The review indicated that the themes and elements were named and explained suitably, and their relationships were presented using an academic method and layout. The review was satisfied that the framework themes and elements were all-encompassing and easy for end-users, who are not necessarily experts in cybersecurity or technical topics, to understand.

Reviewer 6 suggested that the framework could emphasise the human behavioural aspects more strongly to clearly indicate the purpose of the framework as being specifically related to cybersecurity culture. The reviewer was of the view that terms like preparedness and responsibility currently used in the framework do not depict culture. As such, the reviewer believed that highlighting the aspects of human behaviour would make the cultural elements more prominent and relatable.

“Are the key themes and elements within the CCSCF well-defined and consistently used?”

There was an overwhelming agreement among the reviewers that the CCSCF themes and elements were defined well and used consistently. For example, the reviewers indicated that well-defined themes were used to develop the framework and were well explained, with the figures presenting the elements.

Reviewer 6 suggested that there was room for improvement in the presentation of the framework and proposed an overview illustration or diagram that could help users understand how the components fit together, ensuring consistent use throughout the implementation.

“Is the CCSCF simple to understand and use?”

Reviewers' feedback on this question was predominantly positive. This indicates that the framework provides a clear methodology for rating each theme and is a simple acronym. The reviewers noted that the CCSCF was developed in stages and that each stage built upon the previous one, allowing users to understand how the framework could be used, taking a layered approach. The reviewers thought that the clarity of the framework would make it easy to follow once demonstrated or explained.

The review indicated that the framework was not too complicated, as it was broken down into different views and explained using supporting text and diagrams. It was further noted that the language of the framework was appropriate, which makes it simple to understand and use.

Reviewer 6 was of the view that, currently, the framework's complexity makes it challenging to use. This reviewer argued that the framework does not fully meet the principles of ease of use and simplicity without the addition of a clear roadmap or step-by-step guide. Therefore, a suggestion was made that a simplified step guide should be included, as this would enhance the framework's usability significantly.

“Does the CCSCF include examples, case studies, or templates to facilitate understanding and implementation of the framework?”

The reviewers' responses to this question confirmed the existence of a case study and templates which facilitated easy understanding and implementation of the framework. Based on the reviewers' feedback, an example was used to show how to identify areas that should be prioritised. It was mentioned that the implementation process of the framework was discussed at a high level.

There was agreement that the case study supported the intended use of the framework (E-Health) and that the case study demonstrated the success of using the framework in a critical healthcare domain. One reviewer was of the opinion that the CCSCF included beneficial templates as they provided clear guidance on what anyone implementing the framework needed to focus on. The reviewer noted that this made the process relatively easy and straightforward. One N/A response was received.

“Is the CCSCF flexible enough to adapt to different institutions beyond the initial development setting for E-Health institutions?”

Positive feedback based on the reviewers' opinions confirms the flexibility of CCSCF, making it adaptable to other institutions. There was appreciation for the fact that the framework did not use themes related only to E-Health. This was highlighted as a desirable feature of the framework, making it possible to adapt it to institutions other than E-Health.

One of the reviewers raised the point that the framework can be adapted to other South African institutions, as it was developed based on our culture and not a foreign culture. The reviewers agreed that the framework's flexibility was well explained and could be practically implemented by the management to suit the requirements of different organisations. According to a reviewer, the general design of the framework made it easily extendable because the same high-level view could be used for any domain.

In addition to the positive remarks, various other comments and suggestions were made. The view of one reviewer was that the framework would need to be tested for different environments, and the themes might need to be altered depending on the domain before implementation, but in general, the framework was described as quite adaptable to other institutions. Reviewer 7 raised the point that some of the activities in the framework might be hard to achieve in an SME where funds are limited and staffing is small. Reviewer 6 suggested that the framework's objectives, principles, themes, elements, activities, tiers and templates need to be portrayed holistically to show how all the moving parts fit together. Doing this would ensure a framework with an adaptable structure with modular components and adaptable templates, making it easier to determine its adaptability to various settings. Reviewer 5 recommended a checkbox list that could be used by managers to utilise the CCSCF.

9.5.4.2 Evaluation Aspect 2: Objectives

“Does the CCSCF assist institutions with understanding the elements necessary to establish a Cybersecurity Culture?”

The framework was commended for its use of themes and elements as these covered aspects that could be easily followed and applied. It was acknowledged that the themes of the framework, as well as its elements, were clearly explained, and hence would guide the institutions in creating and cultivating a culture for cyber safety. Additionally, the elements of the framework showed the order of prioritisation. It was clear that the framework's activities contained specific actions or steps needed to achieve a cyber-culture.

Reviewer 6 also noted that the framework assisted institutions in understanding the elements necessary to establish a cybersecurity culture. However, this reviewer suggested that the framework could benefit from more specific emphasis on the human and behavioural aspects that clearly constitute a culture. This would make it clear what makes the framework specifically a CCSCF. This suggestion is the same as the recommendation on the first question of evaluation aspect 1.

“Does the CCSCF provide a structure with the necessary components (themes), elements, and activities to guide the cultivation of a Cybersecurity Culture?”

There was overall agreement from the reviewers that the CCSCF structure contained the necessary themes, elements and activities that direct the cybersecurity culture cultivation. It was noted that within the themes, there was a precise alignment of elements, and the activities were outlined and seemed to be distinct and easy for an organisation to check and implement. The reviewers commended the scoring-based approach used in the implementation as this meant that an organisation could use it to evaluate performance and to improve culture if necessary.

Reviewer 6 indicated that the framework provided the necessary components. However, this reviewer's previous suggestion regarding an overview diagram was re-emphasised as a way to show an integrated view of how these parts fit together. The reviewer believed that an overview diagram would help illustrate the relationship between components and guide users.

“Does the CCSCF provide clear and measurable objectives for assessing the effectiveness of the Cybersecurity Culture?”

There was consensus that the objectives of CCSCF were clear and measurable in measuring the effectiveness of the cybersecurity culture. For instance, one reviewer noted that the framework could be measured effectively through the tiers and the maturity modularity model information.

However, although Reviewer 6 believed that the objectives of CCSCF were essential and relevant, as currently phrased, they lacked specific metrics or criteria for measuring how an organisation progressed from one tier to another. This reviewer's view was that the explanations provided in this version of the framework did not mention key performance indicators (KPIs) that would allow for a clear and measurable assessment of progress and effectiveness. Reviewer 6 proposed that this could be easily addressed in the write-up by explicitly speaking about how these goals are measured or how the tiers indicate measurability.

9.5.4.3 Evaluation Aspect 3: Comprehensiveness of the Framework

Does the CCSCF address core themes and elements of a cybersecurity culture, such as:

- *Internal and external themes*
- *Leadership commitment and visibility?*

- *Employee awareness and training?*
- *Communication and feedback mechanisms?*

The reviewers confirmed that the framework addressed Cybersecurity Culture's core themes and elements. Reviewers indicated that the five themes of the CCSCF covered the core elements of a cybersecurity culture and that all themes and elements of the framework were well explained. It was also noted that the framework was comprehensive in its coverage, and each crucial element was explored within the onion layer of the framework.

Reviewer 6 suggested that risk assessment or management be considered as a separate element. This reviewer was of the opinion that the only area that should be considered for additional emphasis was risk management to ensure it was fully integrated into the framework.

“Does the framework guide the integration of cybersecurity considerations into existing organisational culture and values?”

There is unanimous agreement among reviewers that the CCSCF handles the incorporation of cybersecurity into the values and culture of the organisation. There was an opinion that management support and the provision of resources were key considerations that determine what is essential in the organisation. This, in turn, influences culture, and the framework accommodates them, which is a positive feature. It came out in the review that the framework considered the existing culture, as it contained a theme of internal organisation management within the onion layer.

In addition, it was highlighted that the tiers of the framework guided the integration of cybersecurity considerations into the existing culture and values of the organisation. It allowed organisations to assess their current state and provided opportunities for them to progressively improve their cybersecurity posture through their maturity levels.

“Does the framework emphasise the importance of stakeholder engagement, including leadership and employees at all levels?”

Based on the feedback from reviewers, the CCSCF was viewed as a framework that outlined the significance of engaging stakeholders at all levels in cybersecurity culture. The reviewers considered this quality to be very important as it would encourage stakeholder and employee buy-in and facilitate implementation of the framework.

Information from the data led to the conclusion that the framework included elements and sufficient activities that focused on obtaining leadership buy-in, employees' training at different levels and the involvement of all stakeholders.

9.5.4.4 Evaluation Aspect 4: Relevance and Applicability of the Framework

“Is the Contextual Cybersecurity Culture Framework (CCSCF) relevant for the purpose for which it was developed?”

Reviewers voiced overwhelmingly positive responses, which affirm the relevance of CCSCF for establishing a cybersecurity culture in E-Health institutions. It was indicated that the framework was urgently needed in a time of numerous serious cyber threats and cybersecurity challenges. The reviewers believed that the CCSCF addressed the maturity and measuring aspects of a cyber safety culture well.

There was strong support for the view that the framework was relevant because it provided a good foundation made up of items to consider upon which to build when developing a cyber-culture. Further, the framework was acknowledged to have identified areas that needed to be enhanced to improve and maintain a strong cybersecurity culture in E-Health institutions.

Further, the framework was viewed to be very relevant as it clearly addressed the critical need for establishing a cybersecurity culture. It provided comprehensive guidelines and structured activities that would help organisations understand and implement effective cybersecurity practices. It was considered essential to embed this awareness in the organisations and the sector it was designed for.

“Are the CCSCF themes and elements relevant?”

The reviewers confirmed the relevance of the framework's themes and elements. For example, it was noted that the CCSCF themes were all-encompassing. They cover a wide range of issues that determine the cybersecurity culture in organisations. It was further noted that each theme contained activities pertinent to the E-Health domain.

Reviewer 6 proposed that it would be beneficial to add a human aspect to the themes of preparedness (P) and responsibility (R) to enhance their relevance. This reviewer emphasises the significance of this by reiterating it as a recommendation across several evaluation aspects and questions.

“Would you add any themes or elements to the CCSCF? If so, please explain what and why.”

Six of the seven reviewers believed that no new themes or elements should be added to the CCSCF at this stage. Instead, they recommended that a regular re-evaluation schedule be adopted, followed, if necessary, by updates or a stronger focus on themes or activities. They believed the items the framework already covered were sufficient as they contained all important aspects, especially the people aspect.

Reviewer 5 highlighted a need to constantly update the themes and elements of the framework as cybersecurity changes because this is a domain that currently updates and changes. Reviewer 1 suggested adding the level of cybersecurity education of employees. This reviewer indicated that it might be useful in addressing the knowledge gap. Reviewer 6 proposed that it would be beneficial to include a stronger focus on human risk management and behavioural aspects by adding the term “human” to the themes of preparedness (P) and responsibility (R). In this reviewer's opinion, this would enhance the relevance of individual and collective behaviour in cybersecurity.

“Are the recommended cybersecurity practices (activities) realistic and achievable for organisations with varying resource constraints? Please explain if you would recommend any further activities; what and why?”

Four reviewers indicated that the CCSCF activities were achievable, realistic and attainable by organisations with different resource constraints. One of the four reviewers added that organisations might need to see the benefits of the process first and would eventually add resources for effective implementation. However, Reviewer 7 responded differently to this question. This reviewer believed organisations with limited human or financial resources, like SMEs, would not easily implement this framework.

Suggestions: Reviewer 3 thought that more information was needed to link the recommendation to resource constraints. This reviewer believed that this could be discussed more fully. Reviewer 7 suggested that, perhaps, it needs to be refined for adaptability.

“Does the CCSCF offer an implementation option to accommodate diverse organisation sizes, industries, and security risk profiles?”

There was overall agreement that the framework implementation accommodated different types of organisations. CCSCF was viewed as a customisable solution designed to fit the needs of any organisation. The reviewers noted that the CCSCF themes covered elements common in organisations of different sizes. There was a view that the framework provided several tier levels that linked to organisations' maturity levels. The tier levels refer to the themes and offer a wide range of implementation guidance.

Furthermore, in support of the view offered that the CCSCF implementation option was versatile, Reviewer 6 indicated that although the framework was created for the E-Health environment, it had the potential to work in other industries as well. This was because the elements were not unique to the health industry but were applicable in various industries. Additionally, Reviewer 6 believed that the different tiers within the framework allowed any organisation to implement it, even those starting from scratch in Tier 1. This reviewer indicated that this tiered approach made the framework adaptable to organisations of different sizes and security risk profiles, and from diverse industries.

Reviewer 7 was the only one who replied ‘no’ to this question, saying that the flexibility of the implementation does not come out sufficiently clearly in the activities, maturity model and framework.

9.5.4.5 Evaluation Aspect 5: General Comments and Suggestions

“Do you have any comments or suggestions on improving the Contextual Cybersecurity Culture Framework (CCSCF)?”

General comments from reviewers indicated that the CCSCF was well-defined, academically sound, and contributed to the overall body of knowledge in the field of cybersecurity culture. There was a belief that it offered a better way of addressing cybersecurity culture in organisations. There was a view that, given that the overall security posture of organisations is determined by culture, cultural issues must be addressed. Hence, this framework makes a significant contribution.

The following reviewers provided additional suggestions. Reviewer 4 proposes that it would be ideal to have effective performance management processes instead of relying on the maturity model for evaluation. Reviewer 5 suggested including another test case, if possible, to demonstrate the value of the framework for another E-Health facility.

9.5.5 QUANTIFYING EXPERT CONSENSUS

Table 9.15 depicts the percentage of agreement among cybersecurity or cybersecurity culture expert reviewers on the aspects of the CCSCF that were evaluated.

Table 9.15: Expert Consensus

Aspect no	Aspects name	Aspects Items assessed	% Agreement Consensus	Consensus Interpretation
1	Principles	Q1 to Q5	82.8%	Strongly Agree
2	Objectives	Q1 to Q3	95.2%	Strongly Agree
3	Comprehensiveness	Q1 to Q3	90.4%	Strongly Agree
4	Relevance & Applicability	Q1 to Q5	80%	Strongly Agree

Table 9.15 used an agreement scale with four levels covering the four quartiles; 4 indicated Strongly Agree (76% to 100%), 3 indicated Agree (51% to 75%), 2 indicated Disagree (26% to 50%), and 1 indicated Strongly Disagree (0% to 25%). These were used to calculate the consensus for the items related to four aspects of the CCSCF, namely Principles, Objectives, Comprehensiveness, Relevance and Applicability.

Expert reviewers demonstrated consensus at the level of Strongly Agree on all the aspects used for the framework evaluation. Two evaluation aspects (Principles and Relevance and Applicability) achieved 82.8% and 80% consensus according to expert reviewers. This indicated that the

CCSCF adequately met its expected principles and was relevant and should be applicable in another environment as well. Two further evaluation aspects (Objectives and Comprehensiveness) achieved 95.2% and 90.4% consensus agreement, indicating the CCSCF sufficiently achieved the objectives it was planned to attain and was developed in full comprehensiveness.

9.5.6 IMPROVING THE FRAMEWORK AS RECOMMENDED

In acknowledgement of the responses received from the reviewers involved in this evaluation exercise, this section presents an improvement to the final design and development of the CCSCF based on those recommendations. Table 9.16 presents the recommendations, the improvement actions made, and the reasons for implementing or not implementing the recommendations of the expert reviews. Table 9.16: Reviewers' Recommendations and Improvements

Recommendations	Improvement Actions	Reasons
The framework could further emphasise the human behavioural aspects that constitute a culture, as the terms used currently in the framework do not clearly depict culture.	Yes: “Human” is added to the elements of preparedness and responsibility to read as “Human preparedness” and “Human Responsibility.”	See Section 9.5.6.1
An overview illustration or diagram for users to understand how the framework components fit together.	Yes: The improvement action for this recommendation is the development of an overview diagram that shows an overall view of the framework parts.	See Section 9.5.6.1
A clear roadmap or step-by-step guide, or a checkbox guideline.	Yes: The CCSCF improvement action includes the development of a step-by-step guide.	See Section 9.5.6.1

Recommendations	Improvement Actions	Reasons
The language of the objectives does not mention KPI. Lack of specific metrics or criteria for measuring how an organisation progresses from one tier to another.	None	The essence of the objective was not to provide detailed written instructions or metrics of the framework but to highlight the guiding objectives. Measuring how an organisation progresses from one tier to another was done based on the framework themes, elements, and activities.
Recommendations	Improvement Actions	Reasons
The implementation tier diagram needs to reflect progression.	Yes: The improvement action was to redraw the implementation diagram Figure 8.8.	See Section 9.5.6.1
Consider risk assessment or management as a separate element.	None	No improvement changes for this suggestion. This was because risk assessment was accommodated as part of business continuity elements. This was done in this research because published research has argued that there is a close relation between risk management and business continuity. As such, viewing the terms separately is unhelpful (Engemann & Henderson, 2012). Integrating risk management as part of business continuity offers many benefits; it allows institutions to be coherent and productive in responding to threats, proactive rather than reactive, comprehensive in addressing unplanned events that can disrupt business processes, and quick and effective in responding to threats (Engemann & Henderson, 2012).

Recommendations	Improvement Actions	Reasons
To constantly update the themes and elements of the framework as cybersecurity changes.	Future work	Cybersecurity culture is characterised as being a continuous process. Therefore, the proposed framework's themes, elements, and activities are not fixed but should be continuously updated with different implementations and adoption cases to accommodate the changing nature of cybersecurity. This is considered part of future work that can be addressed with new research to accommodate the changing cybersecurity landscape. Future research can assess the framework themes, elements, and activities, and update or improve the proposed framework with the latest factors that may emerge.
Adding the level of cybersecurity education of employees.	None	This is already accommodated under the cybersecurity competency element of the human preparedness and responsibility theme. Activity P Cybersecurity Culture (1) addressed this.
I think more information is needed to link the recommendation to the resource constraints.	None	This is a suggestion that needs to be considered during the actual implementation of the framework. This falls outside the scope of this study
The framework needs to be refined for adaptability.	Yes:	See Section 9.5.6.1

Recommendations	Improvement Actions	Reasons
It would be ideal to have effective performance management processes instead of relying on the maturity model for evaluation.	None and future work	The development of CCSCF adopted the NIST framework for its implementation. As a well-known Cybersecurity Framework (CSF), NIST has been successfully used as a cybersecurity maturity model. Additionally, the scoring-based approach, as accommodated in the implementation (capability maturity profile) serve as a means for organisations to get an idea of their performance. To ensure detailed research exploration, the performance management process can be considered as a possible future work that can serve as an alternative to managing the performance of cybersecurity culture.
Inclusion of another test case if possible.	Future work: Future work will consider hospitals in different provinces as another framework test case.	This is because the ethical clearance obtained for this study is limited to the Mpumalanga province Department of Health.

Table 9.16 did not include information regarding the reasons for the recommended improvement action implemented. Instead, this is discussed in **Section 9.5.6.1**. The section presents reasons for the improvement actions implemented, section references to the chapter where the improvements were indicated, and possibly a depiction of the improvement actions.

9.5.6.1 Improvement Actions Implemented

Table 9.16 provides a summary of the recommendations obtained from the feedback from expert reviewers. Five of those were used to improve the CCSCF. This section provides details of the improvements based on those recommendations.

Suggestion: The framework could further emphasise the human behavioural aspects that constitute a culture, as the terms used currently in the framework do not clearly depict culture.

“DIAGRAM A” depict how the initial High-level framework structure diagram looked before the expert review. As indicated in Table 9.16, this suggestion was implemented by including the term “**Human**” in the CCSCF names of the elements of preparedness and responsibility. These themes were used to represent human behaviour in the proposed framework. However, the terms as originally were in the CCSCF “DIAGRAM A” did not emphasise the human aspect of the characteristic (culture). In the explanation of terms, these two terms were used to refer to the existing organisational culture, but this was not indicated in the high-level diagram that depicted the themes of the framework. The researcher, therefore, believed that the recommendation to emphasise or highlight the human behavioural aspects would improve the overall focus on culture in the proposed framework. The recommendation would also clearly differentiate the framework as a CCSCF.

Hence, the preparedness and responsibility elements in the high-level diagram (**Figure 8.3** of Section 8.5) were changed to “Human preparedness” and “Human responsibility”. **Figure 8.3** is revisited below as “DIAGRAM B”. As a result of these changes, all the related figures and tables where the preparedness and responsibility elements were initially used in Chapter 8 were changed accordingly. This change was made to all parts of the CCSCF, except the objectives and principles, because the two elements were featured in all parts. In addition to **Figure 8.3**, other figures and tables changed were **Figure 8.5** of **Section 8.6.3**, **Figure 8.8** of **Section 8.8**, Table 8.3 and Table 8.9. The original CCSCF high-level framework structure was depicted as in **Diagram A** before it was changed to **Diagram B**.

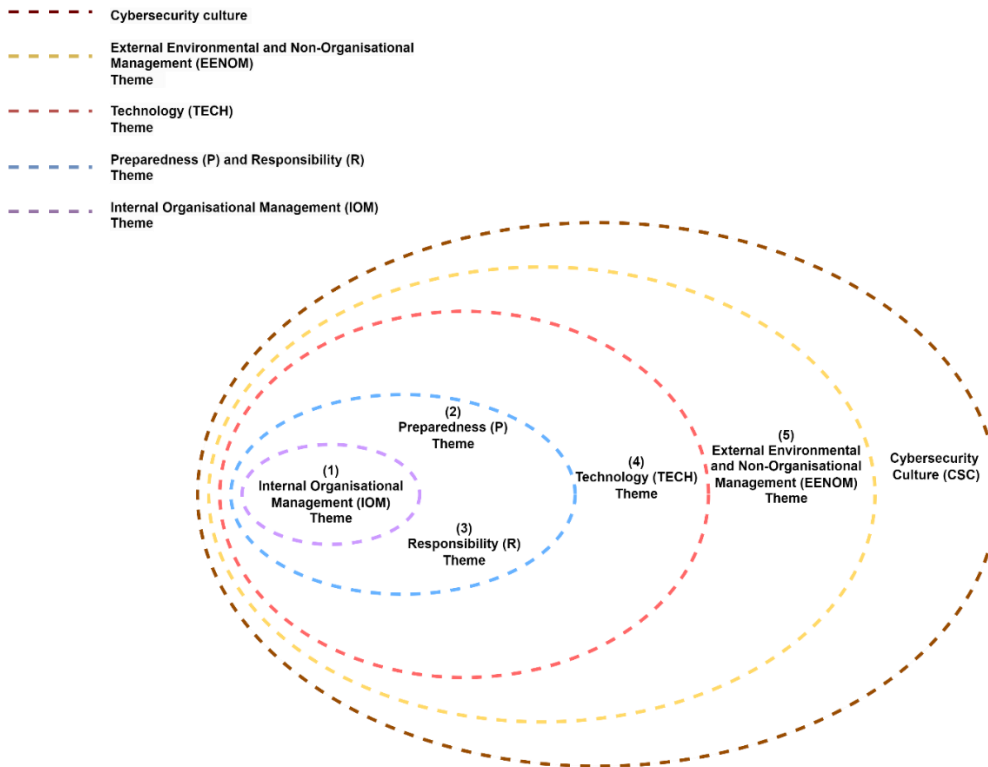


Figure 9.5: Initial high-level framework structure **DIAGRAM A** (own source)

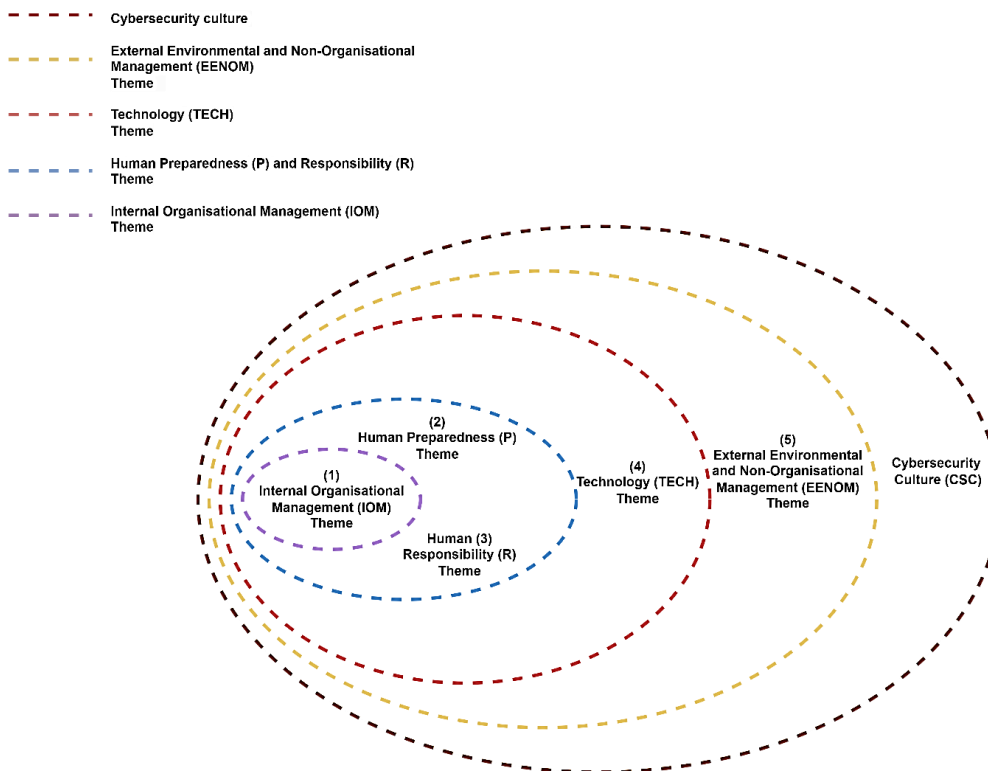


Figure 9.6: Improved high-level framework structure **DIAGRAM B** (own source)

The only difference between Diagram A and Diagram B was in the naming of the Preparedness and Responsibility themes. In Diagram A, the terms are named as “Preparedness Theme” and “Responsibility Theme”, while in Diagram B, they are named as “Human Preparedness Theme” and “Human Responsibility Theme”. The same goes for the other figures and tables in Chapter 8, hence, they are not repeated in this section.

An overview illustration or diagram for users to understand how the framework components fit together.

In response to this recommendation, the design and development of the CCSCF were improved by developing an overview diagram. The diagram illustrates how the framework objectives, principles, themes, elements, activities, tiers and templates fit together. The recommendation to include an overview diagram was seen as extremely important, as it provides a holistic view of the framework before the discussions on different parts of the framework commence. Additionally, having an overview diagram is a common practice found in frameworks like the NIST and Organisational Cybersecurity Culture (Ocybersecurity Culture) frameworks (Huang & Pearson, 2019; National Institute of Standards and Technology, 2018).

The improvement was achieved by introducing a new **Section 8.3.1 “The CCSCF overview diagram”**. **Figure 8.2** repeated below depicts the framework overview diagram.

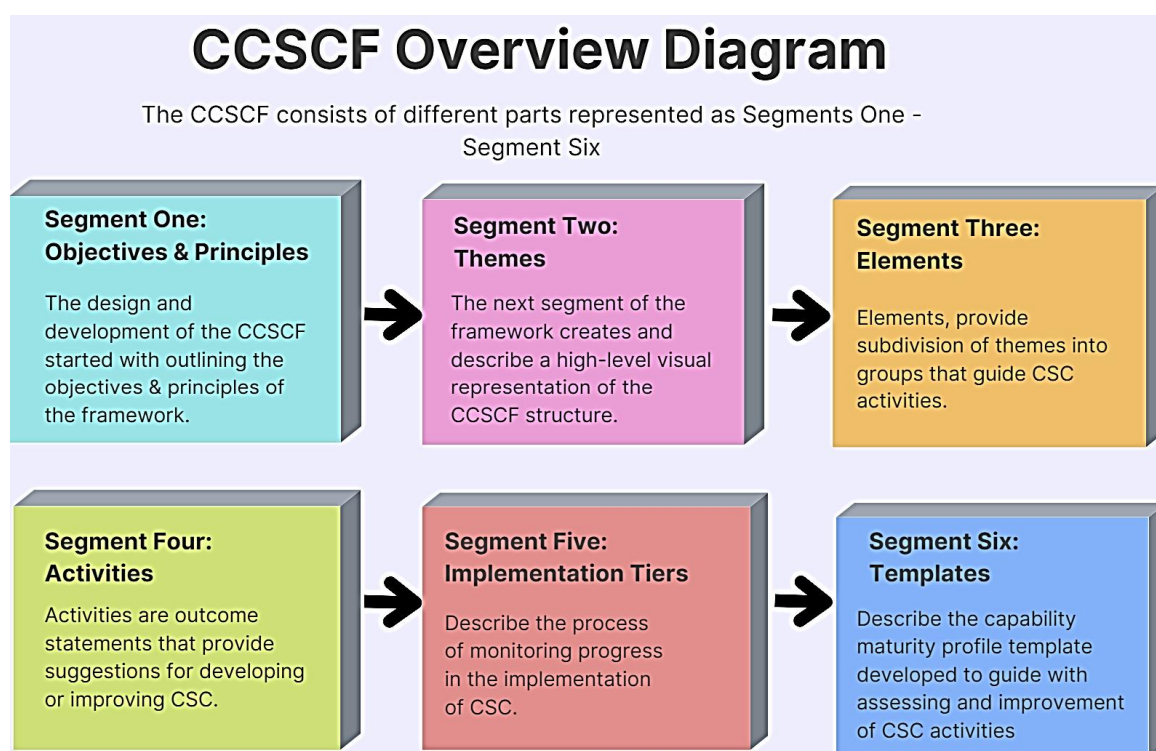


Figure 9.7: The CCSCF Overview Diagram (Revisited)

Providing an overview diagram also addressed the third suggestion. *The framework needs to be refined for adaptability.* The overview diagram, which portrays the parts of the framework holistically, helps the user and ensures the adaptable structure of the proposed framework.

Suggestion: A clear roadmap, step-by-step guide, or checkbox guideline.

The CCSCF was improved by developing a step-by-step guide, depicted below, on how to use the framework. The suggestion to include a roadmap or step-by-step guide as part of the framework was considered extremely important. This practice also exists in cybersecurity maturity models like NIST and C2M2.

- Step-by-step guide to using the CCSCF

The CCSCF is meant to help institutions establish a cybersecurity culture to mitigate the adverse effects of increasing cyber threats and challenges. **Figure 9.8** summarises the step-by-step approach for utilising the framework. Institutions can use the framework separately or as an essential part of their security to identify cybersecurity culture elements and activities, assess their current profile, define their intended capability to determine their gaps, prioritise cybersecurity culture activities, implement action and hence make improvements.

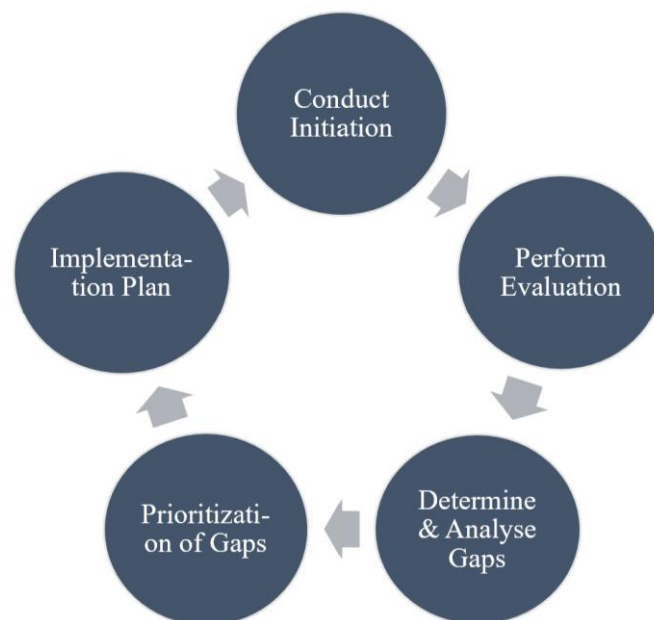


Figure 9.8: Step-by-step Guide to Using CCSCF (own source)

The five-step guide to using CCSCF, depicted in **Figure 9.8** are discussed below:

Step 1: Conduct initiation

Institutions conduct this step to enable them:

- develop an understanding of their interest and intentions, objectives, mission and priority on cybersecurity culture;
- identify and prioritise the core issues and concerns about CS in their institution;
- decide on the focus areas of the cybersecurity culture and the intended target group of their population that the cybersecurity culture interventions will focus on; and
- identify the fundamental cybersecurity culture activities and outcomes required for each element of the framework theme for developing cybersecurity culture.

Step 2: Perform evaluation

Once a good understanding of cybersecurity culture has been obtained, the next step is for the institution to develop its current capability profile. This is achieved by conducting an assessment (using a score or scale value) of each core activity of the proposed CCSCF to identify the existing capability of the institution.

The evaluation step also involves defining (using a formula) the intended capability profile and entails outlining the goals the institution wants to achieve for each of the identified cybersecurity culture activities.

Step 3: Determine and analyse gaps

The scoring used to evaluate the institution's current and intended capability can be used to determine deficiencies in the activities of the framework. Hence, the institution determines the gap by comparing its current and intended capability. Next, it analyses the gap by determining the significance and meaningfulness of the activities toward achieving a strong cybersecurity culture in the institution.

It is not ideal for an institution to aim to achieve the highest maturity tier in all activities of the framework elements. Instead, they should determine the maturity level for each activity so that they can achieve a cybersecurity culture in the most rational way to reduce or eradicate CS threats and challenges.

Step 4: Prioritisation of gap

After gap determination and analysis, the institution must prioritise framework activities that are found to be most urgent. Prioritisation is calculated as a product of Capability Gap (CG) and Weight (W). Weight is allocated to the CG based on the positive or negative scores of the activity. Other factors can also affect prioritisation; this depends on the institution's size and may include the resource availability cost for implementing the activities.

Using capability profiles to achieve prioritisation helps institutions make better-informed decisions.

Step 5: Implementation plan

In this step, institutions determine gaps and take action to address them. The actions aim to adjust current activities to meet the intended profile towards achieving a culture of CS. The step is repeated as needed by the institution for consistent evaluation and improvement of the intervention efforts.

The previous section presented the use case implementation profile as the first evaluation method of the proposed framework. The following section presents a comparative analysis as the second CCSCF evaluation method.

Suggestion: The implementation tier diagram needs to reflect progression.

As indicated in Table 9.16, to accommodate this recommendation, **Figure 8.8** was changed. The aim was for the new diagram to depict levels between the tiers as the organisation progresses. Progression was in terms of the practices of the themes, elements, and activities explained in the framework. **Figure 8.8** was changed from diagram A to diagram B as depicted below.

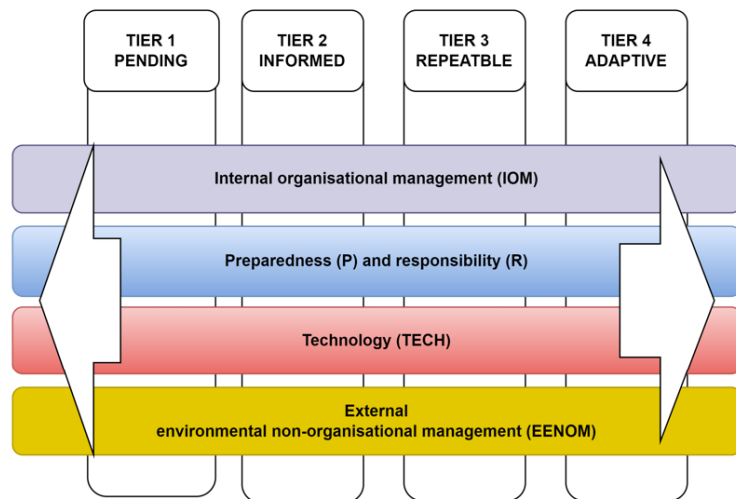


Diagram A: Old implementation tiers depiction

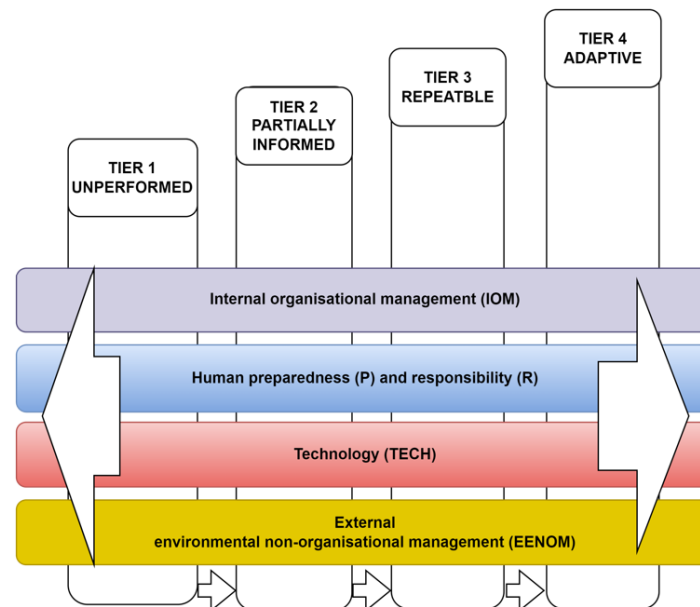


Diagram B: New implementation tiers depiction

Figure 9.9: The Implementation Tier Diagram Reflecting Progression

:

9.6 CONCLUSION OF THE CHAPTER

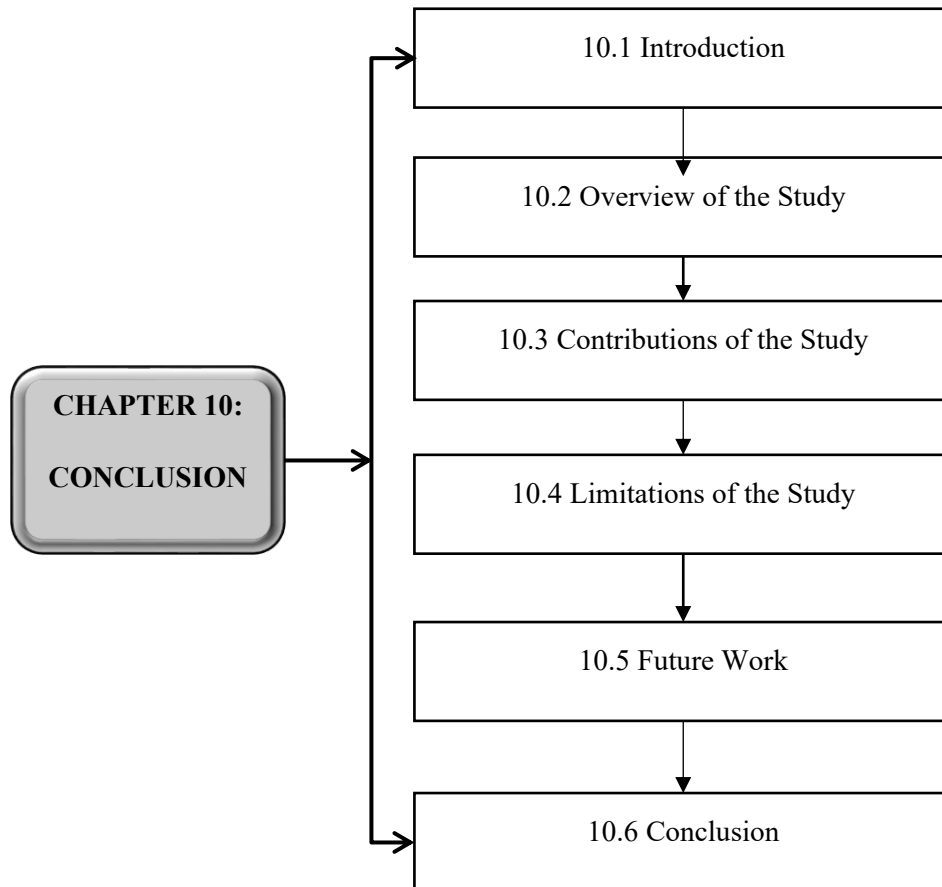
The chapter provided a use case implementation maturity profile for the proposed framework. The case implementation depicted how an institution can establish a cybersecurity culture by focusing its efforts and limited resources on the activities prioritised as most critical when building its cybersecurity culture.

The final research question of this study, **Research Sub-Question 6**, “*How can the contextual Cybersecurity Culture Framework be evaluated?*”, was answered in this chapter. This was achieved using a framework use case implementation profile, a comparative analysis and expert reviews. The comparative analysis found CCSCF to be comprehensive and holistic because it contained elements not addressed in the existing cybersecurity culture frameworks.

The findings of the expert reviews’ evaluation highlighted the CCSCF as a tool serving a clear need at a critical time of cyber threat challenges. The reviewers stressed that the framework provided a good foundation on which to build a cybersecurity culture, identified areas of enhancement for the improvement and maintenance of cybersecurity culture, and provided structured activities that would help organisations to understand and implement effective cybersecurity practices.

Finally, the expert reviewers’ recommendations were applied to enhance the final design and development of the CCSCF, as detailed in **Section 9.5.6.1**. Other recommendations that were beyond the scope of this study were noted to form part of future work that is proposed at the end of this thesis.

CHAPTER 10: CONCLUSION



10.1 INTRODUCTION

This chapter concludes the research presented in this study. As indicated in Chapter 1, this study aimed to develop a contextual framework for establishing cybersecurity culture in public E-Health institutions using South Africa as a case. This chapter revisits the research problem, the research questions, the method followed in conducting the research, the study's contributions, limitations and future work.

Discussion in this chapter starts with an overview of the study (see **Section 10.2**). **Section 10.3** presents the contribution of the study. This is followed by a reflection on the limitation of the study in **Section 10.4**. The future work and conclusion of the chapter are covered in **Sections 10.5** and **10.6**.

10.2 OVERVIEW OF THE STUDY

Cyber-attacks are increasingly targeting healthcare institutions due to the value of healthcare data, and human-related problems are a major contributing factor. The consequences of cyber-attacks are devastating for healthcare institutions and include loss of life. In addition, the financial cost of these attacks is growing at an alarming rate. Cultivating a culture of cybersecurity is very important to address the human factors contributing to cybersecurity weaknesses.

Although the importance of developing a strong cybersecurity culture has previously been noted, efforts in addressing cybersecurity challenges have focused predominantly on technical solutions. Limited research exists in cybersecurity culture and in developing a CCSCF. The development of a CCSCF in this study was based on information obtained from public E-Health institutions in the Mpumalanga province of South Africa in a single case study.

The study has contributed to the area of Information Systems research by developing a contextual framework for establishing a cybersecurity culture.

- RESEARCH QUESTIONS

The core research question that guided the investigation of cybersecurity culture was:

How can a contextual framework for establishing cybersecurity culture in the public E-Health institution in South Africa be developed and evaluated?

This main research question was decomposed into sub-questions to allow for greater understanding of the issues involved. Hence, answering the sub-questions helped the researcher understand and answer the main research question.

The research sub-questions were:

Research Sub-Question 1: *What cybersecurity threats and challenges confront E-Health institutions?*

The objective of **Research Sub-Question 1** was to determine the cybersecurity challenges E-Health institutions face when addressing the cyber threats that are targeting them. This Research Sub-Question was addressed in Chapter 3, under **Section 3.5**. Coupled with the information presented in **Section 3.4** on the reasons E-Health organisations are targeted, predominant cybersecurity culture challenges were identified.

In no particular order, examples of the challenges include a lack of resources, insufficient awareness, inadequate education and training, technological issues, human issues, lack of a security culture and governance issues. Human error emerged as one of the three major causes of cyber threats and resulting cybersecurity incidents. Based on the challenges identified, this research focused on the cybersecurity culture aspect of security culture as a possible solution to address cybersecurity challenges.

This was for the following reasons:

- (1) Limited research exists in cybersecurity culture as a measure towards addressing cybersecurity challenges.
- (2) Cybersecurity culture helps address the human problem identified as a significant challenge to cybersecurity and E-Health implementation.
- (3) The South African government is aware of the importance of Cybersecurity Culture; Hence, promoting cybersecurity culture was one of the key objectives of the National Cybersecurity Policy Framework (NCPF).

Research Sub-Question 2: *What factors are associated with cybersecurity culture in the literature?*

This research question identified cybersecurity culture as its focus to assist with countering challenges to cybersecurity. Therefore, to develop the proposed contextual framework to help

with establishing cybersecurity cultures in organisations, it was essential to gain knowledge of factors that affect the topic, cybersecurity culture, either positively or negatively.

Knowledge of cybersecurity culture factors was gained through the systematic literature review conducted in **Chapter 4**. Thirty-one cybersecurity culture factors were identified, as depicted in Table 4.2. The identified factors constituted, characterised, challenged, influenced and were used in the development of cybersecurity culture (Gcaza & von Solms, 2017b; Gundu et al., 2019; ISACA & CMMI institute, 2018).

Examples of the top cybersecurity culture factors identified from the review include Training and education, awareness, top management or leadership support, cybersecurity policy and procedures, human behaviour, knowledge, budget, and resources, roles and responsibility, cybersecurity champions or teams, and engagement and encouragement. These factors were among the most relevant cybersecurity culture factors because of their level of significance in the cultivation, implementation and maintenance of cybersecurity culture and the level of association they had with other factors. For the full details of cybersecurity culture factors identified from the systematic literature review, see Table 4.2.

Research Sub-Question 3: *What factors are associated with cybersecurity culture in public E-Health institutions?*

It was crucial to identify cybersecurity culture factors reflecting the practices observed in the case study to develop a contextual framework that would be relevant and able to guide public E-Health institutions in establishing a cybersecurity culture. The cybersecurity culture factors emerged through the triangulation of the systematic literature review result (obtained in Chapter 4) with the findings obtained from the survey (see Chapter 6) and the interviews (see Chapter 7). The triangulation of results is reported in Chapter 7.

This confirmed the choice of mixed method research (MMR) as the means for the study's data collection. Both qualitative and quantitative methods were applied to analyse the data collected. Quantitative data were analysed using Cronbach's alpha, descriptive statistics and Pearson Correlation, and qualitative data were analysed using the thematic method.

Table 10.1 depicts the final list of cybersecurity culture factors identified, and the themes under which they were categorised. These factors formed the foundation for developing the proposed CCSCF (see Chapter 8).

Table 10.1: Final List of Cybersecurity Culture Factors Used for the Proposed Framework

Cybersecurity Culture Factors	
Preparedness and Responsibility	Management
Training and Education	Leadership
Cybersecurity awareness	Interest in CS
Change of old practice**	Compliance and Monitoring
Informal education**	Cybersecurity policy
Knowledge	Discipline
Communication and information sharing	Risk assessment
Attitude	Physical security
Priority on medical tasks**	Business continuity
Change of old practice**	Change of old practice**
Defence and protective practices**	CS governance
Environment	Communication channel
Rules and regulations	Centralisation**
Ethical conduct	Organisational learning**
External body**	Technology
Location of the hospital**	ICT infrastructure**
Legals aspects and litigation**	Frequent changes to IT
National culture	Outsourcing of IT systems**
Reputational damage	

Research Sub-Question 4: *What components of existing cybersecurity culture frameworks can stimulate the design and development of a contextual framework for establishing cybersecurity culture in public E-Health institutions?*

Research Sub-Question 4 aimed to identify constructs that formed the core components, dimensions or domains of the existing framework that could stimulate the development of the proposed cybersecurity culture in public E-Health institutions. The identification of the cybersecurity culture constructs that assisted with the development of the proposed framework of this study was achieved in Chapter 4 through a systematic literature review.

Section 4.14 discussed cybersecurity culture and other theoretical frameworks. The frameworks were examined and compared with each other in **Section 4.15**. After that, the cybersecurity culture constructs from the existing frameworks were conceptualised in **Section**

4.16 and were used in the proposed framework. These constructs served as a blueprint for the design of the survey, data collection and analysis, and for questions posed in the interviews.

The conceptualised constructs used for the design and development of the CCSCF are Preparedness (P) and Responsibility (R), Internal Organisational Management (IOM), External Environment and Non-Organisational Management (EENOM), and Technology (TECH). These constructs were all considered as relevant to cybersecurity culture in this study. Therefore, the constructs measure cybersecurity culture.

Research Sub-Question 5: *How can the identified factors be used to design and develop a contextual framework for establishing cybersecurity culture in public E-Health institutions in South Africa?*

The study designed and developed the proposed CCSCF using the required cybersecurity culture factors (summarised in Chapter 7) by adhering to a strategy based on the conceptual framework analysis phases (Jabareen, 2009) (see Chapter 5).

The framework has six segments (see **Section 8.3.1** which portrays how the diverse parts of the framework were developed). Segment 1 states objectives and principles. It explains the objectives that the framework aims to achieve and the principles that directed the framework development. Segment 2 presents the themes and informs the institutions about the five main themes used in developing the CCSCF and the order of importance of the themes. Segment 3 presents the elements that contribute to each theme. The elements indicate the factors that need the institution's attention when developing a cybersecurity culture. Segment 4 prepares the institutions for the activities that need to be performed related to each element.

Segments 5 and 6 are the implementation tiers and templates. In Segment 5, the institution shows how they have applied different tier levels to monitor the progress of developing framework themes, elements and activities within their organisation. Segment six shows the templates used to portray the capability maturity profile of institutions for different activities and their associated elements.

Research Sub-Question 6: *How can the contextual Cybersecurity Culture Framework be evaluated for relevance, uniqueness, and appropriateness?*

The CCSCF developed in this study was evaluated using three methods: use-case implementation, comparative analysis and expert review. These evaluation methods were discussed in detail in Chapter 9.

The Mpumalanga Province Department of Health was used as a use case to demonstrate the template developed in Segment 6 of the framework. This segment showed how the capability maturity profiles template can be applied to create the implementation profile of the institution based on the activities of the CCSCF elements.

The profile template helps determine the current and intended capabilities of the institution, together with their associated maturity levels, by defining formulas (see **Sections 9.3.1.1** and **9.3.1.2**). The difference between the current and intended capabilities determines the capability gaps that inform the priorities assigned to CCSCF activities.

The demonstration provided in **Section 9.3.2** highlighted the provision of resources as the activity related to the Internal Organisation Management (IOM) elements that needed top priority when developing the cybersecurity culture. The activity related to awareness of cybersecurity purpose, policies, roles, and cyber-threats emerged as the most urgent (top priority) activity belonging to the human preparedness (P) and responsibility (R) elements.

Comparative analysis (see **Section 9.4**), was the second evaluation method and revealed that existing frameworks did not contain or fully support all the elements (factors) that shaped the CCSCF. The only partly supported and unique factors in the new framework highlight the importance of context when developing a cybersecurity culture. These elements are legal aspects and litigation, external body, security governance, physical security, frequent change to ICT, priority on medical, business continuity, risk assessment, and security governance.

Lack of full support for or a complete absence of these crucial cybersecurity culture factors in other frameworks makes their adaptation difficult, hence the development of the CCSCF. The CCSCF is considered a more suitable and adaptable framework because it was developed to compensate for the limitations of existing frameworks.

The CCSCF was also evaluated by experts in cybersecurity and cybersecurity culture. Interviews were held with the experts to discuss the framework with them and have them review it, ask questions, and make recommendations to improve the framework. **Section 9.5.6** summarises the expert review suggestions and indicates how the recommendations were used to improve the CCSCF.

This section looked at the research questions of this study and how they have been addressed. The following section will articulate the contributions made by embarking on this project.

10.3 CONTRIBUTIONS OF THE STUDY

Based on the arguments presented in Chapter 1 and other chapters highlighting gaps in existing knowledge, this section articulates the contributions of this research in addressing the gaps. Hence, the submission of the proposed contextual framework to inform the establishment of a cybersecurity culture.

The next section (**Section 10.3.1**) highlights the theoretical contribution of the study to the body of knowledge. After that (**Section 10.3.2**), the methodological contribution is presented, and (**Section 10.3.3**) gives an indication of the practical contribution of the study to the area of Information Systems.

10.3.1 THEORETICAL CONTRIBUTION

The following are the theoretical contributions of this research:

- The CCSCF integrated the organisational, human, technological and external environmental factors into a single context-specific framework tailored for public E-Health institutions. By doing this, the CCSCF builds on and extends existing cybersecurity culture frameworks like SCM and CSC FACR by incorporating constructs that are missing in STOPE and HRD. Also, the earlier development of SCM and CSC FACR did not include the construct (theme) of Technology, and CCSCF has been enhanced to include that theme.

In addition, CCSCF enhances HFD, STOPE and Ocybersecurity culture by combining the human behavioural factors found in HFD and in the structural dimension of STOPE with additional contextual influencing factors which had been overlooked in earlier models. These factors include national regulations, hospital location, professional task priorities, cultural norms, resource constraints, business continuity, physical security, and organisational learning. This was done by incorporating these missing contextual factors and linking them to capability measurement and prioritised action planning. The CCSCF provides a holistic, practical, and context-responsive approach for developing and sustaining a cybersecurity culture in public E-Health environments.

- The CCSCF for establishing cybersecurity culture in public E-Health institutions in South Africa, presented in this study, contributes theoretically to the Information

Systems body of knowledge. The framework's contribution is significant because it was developed based on knowledge from literature and empirical data gathered through surveys and interviews.

The framework was developed based on an understanding that contextual information and knowledge are important in developing a cybersecurity culture. The development of the framework identified factors associated specifically with cybersecurity culture in the context of E-Health, together with components (constructs) of cybersecurity culture found in existing frameworks.

The framework provides an opportunity to establish a culture of cybersecurity in the healthcare sector. Additionally, the study provided a CCSCF that was developed based on standardised and generally understood cybersecurity culture components. The CCSCF was exhibited and discussed in Chapter 8.

- Furthermore, empirical substantiation was achieved by demonstrating the framework implementation using the Mpumalanga Province Department of Health as a use case.
- The conceptual framework was developed using a qualitative process and not a quantitative process. This study extended Jabareen's (2009) conceptual framework process by showing that a mixture of processes can be used in constructing a framework by following conceptual framework techniques. This study combined qualitative and quantitative processes in developing the proposed CCSCF.
- The study published a comprehensive and consolidated list of cybersecurity culture factors that can serve as a basis for researchers in the field of cybersecurity culture. The list was developed based on a holistic, systematic review of literature specific to cybersecurity culture, and the publication has received some citations. The list of factors was published in approved accredited journals and conferences of the South African Department of Higher Education and Technology (DHET).

Other publications making contributions to the study included identifying factors to be considered in establishing cybersecurity culture in public E-Health institutions, conceptual mapping of the articulated list of cybersecurity culture factors to the HFD framework, and an empirical evaluation of the main factors of a cybersecurity culture in South African E-Health institutions using multiple linear regression. The paper was just accepted by the Journal of Cybersecurity and Information Management.

- The study adapted the National Institute of Standards and Technology (NIST) implementation tiers framework by tailoring it to meet the needs of researchers in cybersecurity culture, particularly in the context of E-Health institutions. Based on this, the NIST framework was applied during an implementation investigation by complementing it with the data collected in this study.
- The study formulated an equation that can be used to scale the implementation tiers of cybersecurity culture to the capability maturity level. This study used the equation to scale the Groundedness value to the implementation tiers (depicted in Table 8.9 to Table 8.13 of Chapter 8) to determine the maturity levels of the CCSCF activities.

In summary, this study makes several theoretical contributions to the Information Systems and Cybersecurity Culture knowledge base. Primarily, it develops the CCSCF, which demonstrates that cybersecurity culture is highly context-dependent and cannot be effectively addressed using a universal approach. The framework integrates empirically derived culture factors with standardised constructs found in existing cybersecurity culture models and adapts them specifically for the E-Health sector.

In addition, the study offers a comprehensive and systematically derived list of cybersecurity culture factors that distinguish cybersecurity from information security. This provides a foundational reference that has been published in accredited academic outlets. The study also advances conceptual framework development theory by extending Jabareen's (2009) methodological process to incorporate mixed-method knowledge integration. Furthermore, it enhances theoretical understanding of maturity assessment by adapting the NIST implementation tiers to cybersecurity culture and introducing an equation for scaling maturity levels, enabling measurable progression of cybersecurity culture implementation in institutional settings.

10.3.2 METHODOLOGICAL CONTRIBUTION

- The proposed framework demonstrated how the iterative process of conceptual framework analysis can be used in cybersecurity culture by adapting the framework to the design and development of the CCSCF. This made a new contribution to the study of cybersecurity, particularly to cybersecurity culture and the application of the conceptual framework analysis process.

- Additionally, the use of mixed methods through survey and interview (using thematic analysis) in identifying core cybersecurity culture factors established an interesting and unusual part of the study.

The methodological contribution of this study lies in demonstrating how iterative conceptual framework analysis can be systematically applied within cybersecurity culture research. The research adapted the conceptual framework analysis process to guide the design and development of the CCSCF, thereby providing a methodological model that future researchers can replicate when developing context-sensitive frameworks. Moreover, the study employed a mixed-methods strategy, combining survey data with thematic analysis of interview insights to identify core cybersecurity culture factors. This integrated approach serves as a methodological precedent for combining interpretivist and descriptive analytical techniques in cybersecurity research, illustrating how qualitative and quantitative evidence can be meaningfully aligned to inform the construction of a robust conceptual framework.

10.3.3 PRACTICAL CONTRIBUTION

The practical contributions of this study include:

- The framework can guide public E-Health institutions and other healthcare institutions in establishing a cybersecurity culture.
- The framework informs stakeholders in E-Health institutions about the core themes, elements, and associated activities needed for establishing a robust cybersecurity culture tailored to their institutional context. Specifically, the framework themes, elements, and activities guide E-Health institutions in terms of identifying and prioritising their major cybersecurity culture concerns; decision-makers in cybersecurity culture are the target group to focus on; identification of existing practices and security infrastructures of the institution should be leveraged to foster a cybersecurity culture.
- The framework provided implementation support by developing a step-by-step guideline that the management of institutions can use to utilise the CCSCF. By doing this, the guideline assists in improving the usefulness and effectiveness of the CCSCF in practical, real-world settings. The development of the guideline assists in closing a gap that might exist between the theoretical development of the framework and its

practical implementation, particularly for users with little knowledge of the framework's theoretical underpinning.

In summary, the practical contribution of this study moves beyond merely recommending best practices. The CCSCF offers a context-calibrated structure that enables public E-Health institutions to prioritise cultural interventions based on their operational realities. The implementation guidelines facilitate the production of original practical output, thereby translating theoretical constructs into actionable organisational processes, particularly for institutions without specialist cybersecurity expertise. While many frameworks suggest general awareness-building, this study provides a sequenced, maturity-scaled progression model that supports measurable improvement. Thus, its novelty lies in operationalising cybersecurity culture development in a way that is both context-sensitive and practically executable.

10.4 LIMITATIONS OF THE STUDY

Although all the research objectives in Chapter 1 of this study were achieved, the study must acknowledge some limitations.

- 1) The framework developed and evaluated in this research was limited to the context of only one South African province (where the research was conducted). The large number of and size of South African provinces, made it challenging to include other provinces. Data was only collected from Mpumalanga province, where it was convenient for the researcher to access hospitals.

Although the Mpumalanga Health Department is one of South Africa's Health Departments and contains similar hospital categories, data from Mpumalanga alone may not accurately represent all provinces' health departments in South Africa. There may be factors considered essential in other contexts that do not form part of the contextual framework developed in this research. There was an emphasis in the literature on the importance of context when developing a cybersecurity culture. The context for the proposed CCSCF of this study was on E-Health institutions in one province.

- 2) Integration challenges associated with mixed method approaches created a limitation in this study. It was difficult to integrate data collected via quantitative and qualitative methods. This was addressed by triangulation.
- 3) The investigation was limited to the use case sample from public healthcare institutions. The selected case sample was proposed because the researcher believes that public

healthcare institutions in other South African provinces would have similar cybersecurity challenges. However, in areas where the factors are not the same, adjustments can be made to the proposed framework of this research to make it applicable.

- 4) The CCSCF developed as part of the research output, only considered a use case demonstration of the framework in the E-Health sector and province (Mpumalanga). This is good because it makes the framework theoretically sound, credible, and appropriate to the real-world context. However, the actual implementation solution was not considered because the application of the framework in improving cybersecurity culture was not tested empirically.
- 5) Hospitals were reluctant to issue permission letters to conduct research in their facilities and were strict about following the authorisation process. This made it difficult for the researcher to receive ethical approval from the Mpumalanga province, Department of Health, since obtaining a permission letter depended on having approval letters from hospitals in the province. As a result, the researcher had to go through a long process of seeking approval from various hospitals.
- 6) Data collected was limited to district and tertiary hospitals (two of the hospital categories in South Africa). No data was collected from specialised or central hospitals.
- 7) The quantitative and qualitative data collection sample was purposive. The quantitative investigation was limited to E-Health system users, and the qualitative collection was restricted to ICT staff. This was applicable because participants were selected based on the large amount of information that could be obtained from their specialised experience. Similarly, the expert evaluation sampling selection technique was employed purposively.
- 8) It can also be considered a limitation that the research was conducted in the medical field, and none of the expert reviewers came from the health sector.

10.5 FUTURE WORK

Given the outcomes, contributions, and limitations of this study, this section presents the recommended future work.

- The limitations of this study listed above highlight the fact that the study was conducted in one sector and province and focused on two hospital categories. Therefore, future research should investigate other developing countries, and if conducted in South Africa, different hospital categories (like specialised and central hospitals), provinces, and sectors. Similar research in other contexts should verify

whether, and to what extent, the factors that form part of the proposed framework are applicable (similar or different) and whether essential contextual elements were omitted.

- The research field of cybersecurity culture would benefit significantly if empirical real-time implementation tests could be conducted on the effectiveness of the actual outcomes (successes or failures) of the proposed framework in establishing a cybersecurity culture. This would include a situation where a public E-Health institution uses and tests the framework for establishing a cybersecurity culture and gives feedback to the researchers.
- A future investigation should include constantly assessing, updating and improving the framework themes, elements and activities, using the information that emerges to accommodate the changing cybersecurity landscape. This is one of the recommendations from the expert reviews: *“To constantly update the themes and elements of the framework as cybersecurity changes.”*
- Future studies could explore effective performance management processes as an alternative to managing the performance of cybersecurity culture, instead of focusing only on the maturity method as an evaluation method. This was another recommendation that emerged from expert reviews.

Table 10.2 depicts a summary for the research undertaken by mapping the research objectives, findings and framework components.

Table 10.2: Objectives, Finding, and Framework Component Mapping

Research Objective	Finding	Framework components
RSO1	The cybersecurity threats and challenges confronting E-Health institutions include a lack of resources, insufficient awareness, inadequate education and training, technological issues, human issues, lack of a security culture and governance issues	None
RSO2	Thirty-one cybersecurity culture factors were identified, as depicted in Table 4.2. Examples include training and education; awareness; top management or leadership support; cybersecurity policy and procedures; human behaviour; knowledge, budget, and resources; roles and responsibility; cybersecurity champions or teams; and engagement and encouragement	Segment 2 & 3

Research Objective	Finding	Framework components
RSO3	Table 7.9 depicts the identified list of cybersecurity culture factors associated with E-Health institutions in South Africa. Examples include Training and education, awareness, knowledge, communication and information sharing, policy, leadership, discipline and attitude	Segment 2 & 3
RSO4	The components of the existing framework, conceptualised into constructs used for the design and development of CCSCF, are Preparedness (P) and Responsibility (R), Internal Organisational Management (IOM), External Environment and Non-Organisational Management (EENOM), and Technology (TECH). These constructs were all considered relevant to cybersecurity culture in this study. Therefore, the constructs measure cybersecurity culture.	Segment 2
RSO5	The study designed and developed the CCSCF using the essential cybersecurity culture factors (Table 10.1 and 7) by observing the strategy of the conceptual framework analysis phases (Jabareen, 2009)	Segments 1, 2, 3, & 4
RSO6	The CCSCF was evaluated using use-case implementation, comparative analysis and expert review.	Segment 5 & 6: Implementation Tiers and Templates

10.6 CONCLUSION

The study developed a contextual framework to guide public institutions in establishing a cybersecurity culture. The framework was developed by following the conceptual framework analysis process. A systematic literature review was conducted to identify factors associated with cybersecurity culture. The review also identified the underlying components of the existing cybersecurity culture frameworks and other frameworks applied to different ICT problems. This led to the conceptualisation of constructs used for the design, collection and analysis of quantitative and qualitative data in this study. The constructs include preparedness (P), responsibility (R), internal organisation management (IOM) (also known as management or management cybersecurity practices (MCP) or management (M)), technology (Tech), and external environmental and non-organisational management (EENOM) (also known as external environment (EE) or environment).

The findings from the systematic review and quantitative and qualitative data collection analysis were triangulated to identify the final list of factors associated with cybersecurity culture in the research context. The list of factors identified formed the foundation for the

design and development of the CCSCF proposed in this study to assist institutions to establish cybersecurity culture.

Use case implementation was done using the Mpumalanga Health Department to demonstrate the framework. Use case implementation also assisted with the evaluation of the framework. Comparative analysis and expert reviews were also used to ensure reliability and demonstrate the theoretical and practical value of the framework. Expert reviews helped to ensure that the principles, objectives, comprehensiveness, relevance and applicability of the framework were achieved. Expert reviews of recommendations reveal areas of the framework that needed improvements for efficiency and adaptability, and were used to enhance the framework.

Extensions and amendments are inevitable in any research area, including in cybersecurity culture research. As a result, new developments might have emerged since the start of this research project. Additionally, there is a limitation that the research only focused on one South African province (Mpumalanga). All these possibilities mean that future studies in other provinces should address the study limitations, and new developments can be used to improve the framework. The outcomes from demonstrating the frameworks in the Mpumalanga province provided an opportunity to compare results with those obtained at some later date in other provinces.

REFERENCES

- Abdelrady, A. H., & Akram, H. (2022). An empirical study of classpoint tool application in enhancing EFL students' online learning satisfaction. *Systems*, 10(5), 154.
<https://doi.org/10.3390/systems10050154>
- Abeyratne, R. (2016). *How not to make rules*. In *rulemaking in air transport*. 1–80, Springer.
https://doi.org/10.1007/978-3-319-44657-8_1
- Adhikari, N. K. J., Beyene, J., Sam, J., Haynes, R. B., Garg, A. X., McDonald, H., Rosas-Arellano, M. P., & Devereaux, P. J. (2005). Effects of computerized clinical decision support systems on practitioner performance and patient outcomes: a systematic review. *Journal of the American Medical Association (JAMA)*, 293(10), 1223–1238.
<http://dx.doi.org/10.1001/jama.293.10.1223>
- Ahmed, Y., Naqvi, S., & Josephs, M. (2019). Cybersecurity metrics for enhanced protection of healthcare IT Systems. In *Proceeding of the 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, Oslo, Norway. 1–9.
<http://dx.doi.org/10.1109/ISMICT.2019.8744003>
- Ahmad, G.I., Singla, J., Giri, K.J. (2021). Security and privacy of E-Health data. In: Giri, K.J., Parah, S.A., Bashir, R., Muhammad, K. (eds) *Multimedia Security: Algorithms for Intelligent Systems*. Springer, Singapore. https://doi.org/10.1007/978-981-15-8711-5_10
- Aiken, G. M. (2019). Cybersecurity and productivity: Has a cybersecurity culture gone too far? In *Proceedings of the ASBBS 26th Annual Conference*, Las Vegas, Nevada. 13–23.
<https://www.proquest.com/conference-papers-proceedings/cybersecurity-productivity-has-culture-gone-too/docview/2232455083/se-2?accountid=14648>
- Alder, S. (2016, February 18). Mobile device ransomware warnings becoming more urgent. *HIPAA Journal*. <https://www.hipaajournal.com/mobile-device-ransomware-warnings/> (Accessed 27 October 2024).
- Alder, S. (2018, January 4). Largest healthcare data breaches of 2017. *HIPAA Journal*. <https://www.hipaajournal.com/largest-healthcare-data-breaches-2017/> (Accessed 27 October 2024).

Alder, S. (2019a, September 23). Campbell County Health Ransomware attack causes major disruptions to patient services. *HIPAA Journal*. <https://www.hipaajournal.com/campbell-county-health-ransomware-attack-causing-major-disruption-to-patient-services/> (Accessed 8 July 2022).

Alder, S. (2019b, August 15). Ohio eye care provider suffers ransomware attack. *HIPAA Journal*. <https://www.hipaajournal.com/ohio-eye-care-provider-suffers-ransomware-attack/> (Accessed 27 October 2024).

Alder, S. (2019c, July 29). Kentucky Community Health Center pays \$70,000 ransom to recover PHI. *HIPAA Journal*. <https://www.hipaajournal.com/kentucky-community-health-center-pays-70000-ransom-to-recover-phi/> (Accessed 27 October 2024).

Alder, S. (2024a, August). Change Healthcare reports ransomware data breach to HHS. *HIPAA Journal*. <https://www.hipaajournal.com/change-Healthcare-responding-to-cyber-attack/> (Accessed 27 October 2024).

Alder, S. (2024b, October). *Healthcare data breach statistics*. *HIPAA Journal*. <https://www.hipaajournal.com/healthcare-data-breach-statistics/> Accessed 20 July 2025

Alder, S. (2024c, June). January 2024 Cyberattack on Lurie Children's Hospital Affects 792K Individuals. *HIPAA Journal*. <https://www.hipaajournal.com/january-2024-cyber-attack-on-lurie-childrens-hospital-affects-792k-individuals/> (Accessed 17 November 2025).

Aldosari, B. (2025). Cybersecurity in healthcare: New threat to patient safety. *Cureus*, 17(5). <https://doi.org/10.7759/cureus.83614>

Alanazi, A., Al Rabiah, F., Gadi, H., Househ, M., & Al Dosari, B. (2018). Factors influencing pharmacists' intentions to use pharmacy information systems. *Informatics in Medicine Unlocked*, 11, 1–8. <https://doi.org/10.1016/j.imu.2018.02.004>

Alharbi, N., Papadaki, M., & Dowland, P. (2017). The impact of security and its antecedents in behaviour intention of using e-government services. *Behaviour & Information Technology*, 36(6), 620–636. <https://doi.org/10.1080/0144929X.2016.1269198>

Alhogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, 49, 567–575. <https://doi.org/10.1016/j.chb.2015.03.054>

- Alhogail, A., & Mirza, A. (2014). A Proposal of an organizational Information Security Culture Framework. In *Proceedings the of the International Conference on Information, Communication Technology and System, ICTS 2024*, Surabaya, Indonesia, 243–249. <https://doi.org/10.1109/ICTS.2014.7010591>
- Alhogail, A., Mirza, A., & Bakry, S. H. (2015). A comprehensive human factor framework for information security in organizations. *Journal of Theoretical and Applied Information Technology*, 78(2), 201–211.
- Al-Maqbali, A. H., & Al-Shamsi, A. (2023). Assessment strategies in online learning environments during the COVID-19 pandemic in Oman. *Journal of University Teaching and Learning Practice*, 20(5), 8. <https://doi.org/10.53761/1.20.5.08>
- Al-Maqbali, A. H., & Hussain, R. M. R. (2022). The impact of online assessment challenges on assessment principles during COVID-19 in Oman. *Journal of University Teaching and Learning Practice*, 19(2), 73–92. <https://doi.org/10.53761/1.19.2.6>
- Al-Sharhan, S., Omran, E., & Lari, K. (2019). An integrated holistic model for an eHealth system: A national implementation approach and a new cloud-based security model. *International Journal of Information Management*, 47(2019), 121–130. <https://doi.org/10.1016/j.ijinfomgt.2018.12.009>
- Al-Shehri, Y. (2012). Information security awareness and culture. *British Journal of Arts and Social Sciences*, 6(1), 61– 69. <http://www.bjournal.co.uk/BJASS.aspx>
- Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers and Security*, 98, 102003, <https://doi.org/10.1016/j.cose.2020.102003>
- Alsowail, R. A., & Al-Shehari, T. (2022). Techniques and countermeasures for preventing insider threats. *PeerJ Computer Science*, 8, e938. <https://doi.org/10.7717/peerj-cs.938>
- Alvarez-Dionisi, L. E., & Urrego-Baquero, N. (2019). Implementing a cybersecurity culture. *ISACA Journal*, 2, 1–6. <https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/implementing-a-cybersecurity-culture>
- Alvarez, R. C. (2002). The promise of E-Health: A Canadian perspective. *Ehealth International*, 1(1), 4. <https://doi.org/10.1186/1476-3591-1-4>

AlZubi, A. A., Al-Maitah, M., Alarifi, A. (2021). Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. *Soft Computing*, 25(18), 12319-12332. <https://doi.org/10.1007/s00500-021-05926-8>

Ammenwerth, E., & de Keizer, N. (2005). An inventory of evaluation studies of information technology in healthcare: Trends in evaluation research 1982–2002. *Methods of Information in Medicine*, 44(3), 44–56. <https://doi.org/10.1055/s-0038-1633922>

An Roinn Slainte Department of Health. (2013). *eHealth strategy for Ireland*. <https://assets.gov.ie/16174/092e7c62f97b472b83cdb6dfdcdfd5c7.pdf> (Accessed 10 April 2020).

AP News. (2020, September 17). *German hospital hacked, patient taken to another city dies*. AP NEWS. <https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94> (Accessed 6 October 2020).

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: Current state of research. *International Journal of Internet and Enterprise Management*, 6(4), 279–314. <https://doi.org/10.1504/IJEM.2010.035624>

Archer, N., Fevrier-Thomas, U., Lokker, C., McKibbin, K. A., & Straus, S. E. (2011). Personal health records: A scoping review. *Journal of the American Medical Informatics Association*, 18(4), 515–522. <https://doi.org/10.1136/amiajnl-2011-000105>

Ariens, L. F. M., Schussler-Raymakers, F. M. L., Frima, C., Flinterman, A., Hamminga, E., Arents, B. W. M., Bruijnzeel-Koomen, C. A. F. M., Marjolein, S., de B. W., & Os-Medendorp, H. van. (2017). Barriers and facilitators to ehealth use in daily practice: Perspectives of patients and professionals in dermatology. *Journal of Medical Internet Research*, 19(9), 1–10. <https://doi.org/10.2196/jmir.7512>

Arogundade, O. R. (2023). Network security concepts, dangers, and defence best practical. *Computer Engineering and Intelligent Systems*, 14(2). <https://doi.org/10.7176/CEIS/14-2-03>

Ashford, W. (2019, August 8). *Ransomware: A continued threat to business, report warns*. ComputerWeekly.Com. <https://www.computerweekly.com/news/252468085/Ransomware-a-continued-threat-to-business-report-warns> (Accessed 4 November 2024).

Astakhova, L. V. (2014). The concept of the information-security culture. *Scientific and Technical Information Processing*, 41(1), 22–28.

<https://doi.org/10.3103/S0147688214010067>

ATLAS.ti. (2024). *ATLAS.ti Winders: User Manual, (Version 24)*. ATLAS.ti Scientific Software Development GmbH. <https://atlasti.com/manuals-and-documents?#user-manuals> (Accessed 04 December 2024).

Attride-Stirling, J. (2001). Thematic networks: an analytic tool for qualitative research. *Qualitative Research*, 1(3), 385–405. <https://doi.org/10.1177/146879410100100307>

Badawi, H. (2024). Cybersecurity: Emerging trends and challenges. *Scientific and Practical Cyber Security Journal (SPCSJ)*, 8(3): 92–111. <https://journal.scsa.ge/papers/cybersecurity-emerging-trends-and-challenges/>

Baker, L., Wagner, T., Singer, S., & Bondor, K. (2003). Use of the internet and e-mail for health care information. *Journal of American Medical Association (JAMA)*, 289(18), 2400–2406. <https://doi:10.1001/jama.289.18.2400>

Bakry, A. H., & Bakry, S. H. (2005). Enterprise resource planning: A review and a STOPE view. *International Journal of Network Management*, 15(5), 363–370. <https://doi.org/10.1002/nem.584>

Bakry, S., & Bakry, F. (2001). A strategic view for the development of e-business. *International Journal of Network Management*, 11(2), 103–112. <https://doi.org/10.1002/nem.395>

Bakry, S. H. (2002). E-business development: A strategic view. *Sultan Qaboos University Journal for Science*, 7(1), 11–22. <https://doi.org/10.24200/squjs.vol7iss1pp11-22>

Bakry, S. H. (2004). Development of e-government: a STOPE view. *International Journal of Network Management*, 14(5), 339–350. <https://doi.org/10.1002/nem.529>

Bakry, S. H. (2003). Development of security policies for private networks. *International Journal of Network Management*, 13(3), 203–210. <https://doi.org/10.1002/nem.472>

Barzilay, M. (2013). *A simple definition of cybersecurity*. ISACA Now Blog. <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2016/a-simple-definition-of-cybersecurity> (Accessed 01 September 2020).

Basahel, A. M., Sen, A. A. A., Babou, N. M., & Yamin, M. (2019). A Framework for integration between E-Health systems and new technologies. *International Journal of Human Potentials Management (IJHPM)*, 1(2), 44–45. <http://abmjournal.org/index.php/ijhpm/article/view/19>

Bashshur, R., Shannon, G., Krupinski, E., & Grigsby, J. (2011). The taxonomy of telemedicine. *Telemedicine and E-Health*, 17(6), 484–494. <https://doi.org/10.1089/tmj.2011.0103>

Baylon, C. (2014). Challenges at the intersection of cybersecurity and space security: Country and international institution perspectives. Chatham House, *The Royal Institute of International Affairs*. <https://nsarchive.gwu.edu/sites/default/files/documents/5023659/United-Kingdom-Government-Chatham-House-Research.pdf> (Accessed 31 October 2024).

Beahm, A. (2019, October 4). *DCH Health System still grappling with ransomware attack*. AL. Com Alabama. <https://www.al.com/news/2019/10/dch-health-system-still-grappling-with-ransomware-attack.html> (Accessed 10 October 2022).

Bemmel, J. H., Musen, M. A., & Helder, J. (1997). *Handbook of medical informatics*. Springer; Bohn Stifle Van Loghum.

Benavides-Vaello, S., Strode, A., & Sheeran, B. C. (2013). Using technology in the delivery of mental health and substance abuse treatment in rural communities: A review. *Journal of Behavioural Health Services and Research*, 40, 111–120. <https://doi.org/10.1007/s11414-012-9299-6>

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *Nursing Plus Open*, 2, 8–14. <https://doi.org/10.1016/j.npls.2016.01.001>

Berr, J. (2017, May 16). “WannaCry” ransomware attack losses could reach \$4 billion. CBS News. <https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/> (Accessed 04 August 2020).

Bird, C. M. (2005). How I stopped dreading and learned to love transcription. *Qualitative Inquiry*, 11(2), 226–248. <https://doi.org/10.1177/1077800404273413>

Bird, K. T. (1971). *Teleconsultation: A new information exchange system*. Vol 201. Massachusetts General Hospital, Boston.

Black, A. D., Car, J., Pagliari, C., Anandan, C., Cresswell, K., Bokun, T., McKinstry, B., Procter, R., Majeed, A., & Sheikh, A. (2011). The impact of ehealth on the quality and safety of health care: A systematic overview. *PloS Medicine*, 8(1), 1–16. <https://doi.org/10.1371/journal.pmed.1000387>

Blaya, J. A., Fraser, H. S. F., & Holt, B. (2010). E-Health technologies show promise in developing countries. *Health Affairs*, 29(2), 244–251. <https://doi.org/10.1377/hlthaff.2009.0894>

Boonstra, A., & Broekhuis, M. (2010). Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions. *BMC Health Services Research*, 10, 231. <https://doi.org/10.1186/1472-6963-10-231>

Bounas, K., Georgiadou, A., Katsoulis, M., Mouzakis, S., & Askounis, D. (2020). Towards a cybersecurity culture tool through a holistic, multi-dimensional assessment framework. In *Proceedings of the 13th IADIS International Conference Information Systems, IS 2020*, Sofia, Bulgaria, 135–139. https://doi.org/10.33965/is2020_202006c016

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development*. SAGE Publications.

Branch, L. E. (2018). *Cyber threats and healthcare organizations: A Public health preparedness perspective*. (Doctoral dissertation, West Virginia University). ProQuest Dissertations & Thesis. Accession No. 13893379. <https://researchrepository.wvu.edu/etd/3701>

Brandeis, G. H., Hogan, M., Murphy, M., & Murray, S. (2007). Electronic health record implementation in community nursing homes. *Journal of the American Medical Directors Association*, 8(1), 31–34. <https://doi.org/10.1016/j.jamda.2006.09.013>

- Branley-Bell, D., Coventry, L., & Sillence, E. (2021). Promoting cybersecurity culture change in healthcare. In *Proceeding of the 14th Pervasive Technologies Related to Assistive Environments Conference*, Greece, 544–549. <https://doi.org/10.1145/3453892.3461622>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Brewer, R. (2016). Ransomware attacks: Detection, prevention and cure. *Network Security*, 2016(9), 5–9. [https://doi.org/10.1016/S1353-4858\(16\)30086-1](https://doi.org/10.1016/S1353-4858(16)30086-1)
- Bridges, L. (2008). The changing face of malware. *Network Security*, 2008(1), 17–20. [https://doi.org/10.1016/S1353-4858\(08\)70010-2](https://doi.org/10.1016/S1353-4858(08)70010-2)
- Brookman, J. (2015). Protecting privacy in an era of weakening regulation. *Harvard Law Policy Review*, 9, 355–374. https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/harlpolv9&id=360&men_tab=srchresults
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523. <https://doi.org/10.2307/25750690>
- Burke, W., Stranieri, A., Oseni, T., & Gondal, I. (2024). The need for cybersecurity self-evaluation in healthcare. *BMC Medical Informatics and Decision Making*, 24, 133. <https://doi.org/10.1186/s12911-024-02551-x>
- Burger, S. (2024, January 11). *South African companies vulnerable to cyberthreats owing to affordability challenges*. Engineering News. <https://www.engineeringnews.co.za/article/south-african-companies-vulnerable-to-cyberthreats-owing-to-affordability-challenges-2024-01-11> (Accessed 06 February 2025).
- Bygstad, B., Hanseth, O., & Le, D. T. (2015). From its silos to integrated solutions. A study in E-Health complexity. In *Proceedings of the 23rd European Conference on Information Systems, ECIS 2015*, 0–15. <https://doi.org/10.18151/7217283>

Caballero, A. (2014). Information security essentials for IT managers: Protecting mission-critical systems. In *Computer and Information Security Handbook*, (2nd edition), 1–46. Syngress.

Cameron, J. (2017). *SA companies highly vulnerable to cyber-attacks, warns Africa expert. Where are your weaknesses?* BizNews.com.
<https://www.biznews.com/africa/2017/03/01/cyber-attacks-africa> (Accessed 22 September 2020).

Cameron, K., & Quinn, R. (2006). *Diagnosing and changing organisational culture: Based on the competing values framework* (Revised ed.). Jossey-Bass.

Cardoso, M. G. M. S., Laureano, R. D., & Serrao, C. (2017). Cybersecurity culture in Portuguese organizations: An exploratory analysis. In *Proceeding of the 12th Iberian Conference on Information Systems and Technologies, CISTI 2017*, Lisbon Portugal, 1–5.
<https://doi.org/10.23919/CISTI.2017.7976008>

Casey, T., Fiftal, K., Landfield, K., Miller, J., Morgan, D., & Willis, B. (2015). *The Cybersecurity framework in action: An Intel use case*. Intel Corporation.

Catwell, L., & Sheikh, A. (2009). Evaluating eHealth interventions: The need for continuous systemic evaluation. *PLoS Medicine*, 6(8), 1–6.
<https://doi.org/10.1371/journal.pmed.1000126>

Cavelty, M. D. (2007). *Cybersecurity & threat politics: US efforts to secure the information age Myriam*. Routledge.

Chalil, K. (2020, April 25). *Statistical methods for development research: Correlation*. [Study material]. M.A. Development Studies course (MADVS2005C04), Central University of South Bihar. <https://docslib.org/doc/7718805/the-statistics-tutors-quick-guide-to-commonly-used-statistical-tests?utm>

Chang, H., Choi, J. Y., Shim, J., Kim, M., & Choi, M. (2023). Benefits of information technology in healthcare: artificial intelligence, internet of things, and personal health records. *Healthcare Informatics Research*, 29(4), 323–333.
<https://doi.org/10.4258/hir.2023.29.4.323>

Chapuis, C., Roustit, M., Bal, G., Schwebel, C., Pansu, P., David-Tchouda, S., Foroni, L., Calop, J., Timsit, J. F., Allenet, B., Bosson, J. L., & Bedouch, P. (2010). Automated drug dispensing system reduces medication errors in an intensive care setting. *Critical Care Medicine*, 38(12), 2275–2281. <https://doi.org/10.1097/CCM.0b013e3181f8569b>

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. SAGE Publications.

Charmaz, K. (2014). *Constructing grounded theory* (2nd ed.). SAGE Publications.

Chavula, H. (2013). Telecommunications development and economic growth in Africa. *Information Technology for Development*, 19(1), 5–23. <https://doi.org/10.1080/02681102.2012.694794>

Chen, L. C., & Farkas, D. (2009). An investigation of decision-making and the trade-offs involving computer security risk. In *Proceedings of the 15th Americas Conference on Information Systems, AMCIS 2009*, San Francisco, California. 5205–5212. <https://aisel.aisnet.org/amcis2009/610>

Chen, Y., Ramamurthy, K., & Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, 55(3), 11–19. <https://doi.org/10.1080/08874417.2015.11645767>

Chester, A. (2018, June 18). *Latest big corporate data breach: Why Liberty's clients should be bringing IT to book* | ITWeb. ITWeb. <https://www.itweb.co.za/content/dgp45qaGaYO7X9I8> (Accessed 21 September 2020).

Chiyangwa, T. B., & Mnkandla, E. (2017). Modelling the critical success factors of agile software development projects in South Africa. *SA Journal of Information Management*, 19(1), 1–8. <https://doi.org/10.4102/sajim.v19i1.838>

Chrissis, M.B., Konrad, M., & Shrum, S. (2003). *CMMI: Guidelines for process integration and product improvement*. ISBN 0321154967, 9780321154965, Addison-Wesley.

Christopher, J. D., Bartol, N., & Goff, E. (2014). NIST cybersecurity framework implementation: Energy sector approach. In *Proceedings of the SANS ICS Security Summit*.

Chuma, K. G., & Ngoepe, M. (2022). Security of electronic personal health information in a public hospital in South Africa. *Information Security Journal: A Global Perspective*, 31(2), 179–195, <https://doi.org/10.1080/19393555.2021.1893410>

Chuma, K. G. (2025). Legacy electronic health record systems as culprit behind cybersecurity risks in public healthcare facilities of South Africa. *Global Security: Health, Science and Policy*, 10(1). <https://doi.org/10.1080/23779497.2025.2532556>

CISCO. (2016). *Healthcare security: Improving network defences while serving patients*. <https://www.cisco.com/c/dam/en/us/products/collateral/security/security-benchmark.pdf> (Accessed 7 August 2020).

Ciuperca, E. M., Vevera, V., & Cirnu, C. (2019). Social variables of cybersecurity educational programmes. In *Proceedings of the 15th International Scientific Conference eLearning and Software for Education Bucharest, eLSE 2019*, 190–194. <https://doi.org/10.12753/2066-026X-19-096>

Clark, M. (2019, October 10). *The most devastating healthcare ransomware attacks in 2019*. Etactics. <https://etactics.com/blog/the-most-devastating-healthcare-ransomware-attacks-in-2019> (Accessed 10 June 2023).

Clark, R. M., Panguluri, S., Nelson, T. D., & Wyman, R. P. (2017). Protecting drinking water utilities from cyberthreats. *Journal of American Water Works Association*, 109(2), 50–58. <https://doi.org/10.5942/jawwa.2017.109.0021>

Claunch, D., & McMillan, M. (2013). Determining the right level for your IT security investment: A rural medical center facing threats of data breaches discovered that hospital IT security investments go beyond just dollars and cents. *Healthcare Financial Management*, 67(5), 100–103. <https://link.gale.com/apps/doc/A339635423/AONE?u=anon~be44a22c&sid=googleScholar&xid=a1e8b01c>

Cliff, B. (2012). Using technology to enhance patient-centered care. *Journal of Healthcare Management*, 57(5), 301–303. <https://doi.org/10.1097/00115514-201209000-00003>

Cluley, G. (2024, July 9). *Ransomware attack on blood-testing service puts lives in danger in South Africa*. Bitdefender. <https://www.bitdefender.com/blog/hotforsecurity/ransomware-attack-on-blood-testing-service-puts-lives-in-danger-in-south-africa/> (Accessed 28 October 2024).

Cohen, J. K. (2019, March 8). *Columbia surgical specialists pay \$14K in ransomware attack*. Modern Healthcare. <https://www.modernhealthcare.com/cybersecurity/columbia-surgical-specialists-pay-14k-ransomware-attack/> (Accessed 04 May 2022).

Cohen, L., Manion, L., & Morrison, K. (2007). *Research methods in education* (6th ed.). Routledge.

Coronado, A. J., & Wong, T. L. (2014). Healthcare cybersecurity risk management: Keys to an effective plan. *Biomedical Instrumentation & Technology*, 48(1), 26–30. <https://doi.org/10.2345/0899-8205-48.s1.26>

Corradini, I. (2020). *Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology*. Springer. <http://link.springer.com/10.1007/978-3-030-43999-6>

Cossío-Silva, F., Revilla-Camacho, M., Vega-Vázquez, M., & Palacios-Florencio, B. (2016). Value co-creation and customer loyalty. *Journal of Business Research*, 69(5), 1621–1625. <https://doi.org/10.1016/j.jbusres.2015.10.028>

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, 113, 48–52. <https://doi.org/10.1016/j.maturitas.2018.04.008>

Cox, J. (2016, June 26). *Hacker advertises slew of alleged healthcare organization records*. VICE. https://www.vice.com/en_us/article/9a3dwy/hacker-advertises-slew-of-alleged-healthcare-organization-records (Accessed 25 June 2021).

Creswell, J.W. (2014). *Research design: Qualitative quantitative and mixed methods approaches* (4th ed.). SAGE Publications.

Creswell, J.W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). Thousand Oaks, CA: SAGE Publications.

Creswell, J. W., & Creswell, J. D. (2023). *Research design: qualitative, quantitative, and mixed methods approaches* (6th ed. International). SAGE Publications.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Crock, E. (2016). Access to healthcare services for people living with HIV experiencing homelessness: A literature review. *Australian Journal of Advanced Nursing*, 34(1), 42–51. <https://search.informit.org/doi/abs/10.3316/informit.577005665178276>

Cruzes, D. S., & Dybå, T. (2011). Recommended steps for thematic synthesis in software engineering. In *Proceeding of the International Symposium on Empirical Software Engineering and Measurement (ESEM 2011)*, 275–284. <https://doi.org/10.1109/esem.2011.36>

CSIR, & NDOH. (2014). *South African national health normative standards framework for interoperability in eHealth in South Africa*. (Version 2.0 March 2024; CSIR GWDMS Number: 240075)

Cuenca, J. V. (2017). *Cybersecurity challenges in healthcare industries*. Master's dissertation, Utican College.

Cybersecurity Observatory. (2020). *Major cybersecurity threats in healthcare*. 1st Global Cybersecurity Observatory. <https://cyberstartupobservatory.com/video-infographics/> (Accessed 29 September 2020).

Da Veiga, A. (2019). Achieving a security culture. In Vasileiou, I., & Furnell, S. (Eds). *Cybersecurity education for awareness and compliance*. IGI Global. 72–100. <https://doi.org/10.4018/978-1-5225-7847-5>

Da Veiga, A., Astakhova, V. L., Botha, A., & Herselman, M. (2020). Defining organisational information security culture: Perspectives from academia and industry. *Computers & Security*, 92, 101713. <https://doi.org/10.1016/j.cose.2020.101713>

Da Veiga, A. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. In *Proceedings of the 2016 SAI Computing Conference*, London, UK 1006–1015. <https://doi.org/10.1109/SAI.2016.7556102>

- Da Veiga, A. (2008). *Cultivating and assessing information security culture*. Doctoral dissertation, University of Pretoria.
- Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers and Security*, 29(2), 196–207. <https://doi.org/10.1016/j.cose.2009.09.002>
- Da Veiga, A., & Martins, N. (2015a). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers and Security*, 49, 162–176. <https://doi.org/10.1016/j.cose.2014.12.006>
- Da Veiga, A., & Martins, N. (2015b). Information security culture and information protection culture: A validated assessment instrument. *Computer Law and Security Review*, 31(2), 243–256. <https://doi.org/10.1016/j.clsr.2015.01.005>
- Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers and Security*, 70, 72–94. <https://doi.org/10.1016/j.cose.2017.05.002>
- Dahlberg, L., & Mccaig, C. (2010). Introduction to research and evaluation basics. In *Practical research and evaluation: A start-to-finish guide for practitioners*. SAGE Publications. <https://doi.org/10.4135/9781446268346>
- Dahlstrom, G. A. (2002). *Privacy and confidentiality of patient health information*. Doctoral Dissertation, University of Missouri-Columbia, 1-113.
- Davis, J. (2020, March 9). *Ransomware attacks on healthcare providers rose 350% in Q4 2019*. Health IT Security. <https://healthitsecurity.com/news/ransomware-attacks-on-healthcare-providers-rose-350-in-q4-2019> (Accessed 23 September 2020).
- Davis, J. A., Zakoscielna, K., & Jacobs, L. (2016). Electronic information systems use in residential care facilities: The differential effect of ownership status and chain affiliation. *Journal of Applied Gerontology*, 35(3), 331–348. <https://doi.org/10.1177/0733464814563605>
- Davison, R. M., de Vreede, G. J., & Briggs, R. O. (2005). On peer review standards for the Information Systems literature. *Communications of the Association for Information Systems*, 16, 967–980. <https://doi.org/10.17705/1cais.01649>

Dawadi, S., Shrestha, S., & Giri, R. A. (2021). Mixed-methods research: A discussion on its types, challenges, and criticisms. *Journal of Practical Studies in Education*, 2(2), 25–36.
<https://doi.org/10.46809/jpse.v2i2.20>

De Lange, M., & von Solms, R. (2012). An e-safety educational framework in South Africa. In *Proceedings of the Southern Africa Telecoms and Network Applications Conference (SATNAC)*.
http://www.satnac.org.za/proceedings/2012/papers/3.Internet_Services_End_User_Applications/53.pdf

De Villiers, M. R. (2012). Models for interpretive information systems research, Part 2: Design research, development research, design-science research, and design-based research - A meta-study and examples. In E. M. Mora, O. Gelman, A. Steenkamp, and M. S. Raisinghani & Hershey (Eds.), *Research methodologies, innovations and philosophies in Software Systems Engineering and Information Systems*, IGI Global, 238–255.
<https://doi.org/10.4018/978-1-4666-0179-6.ch012>

De Castro, H. P. (2015). *Government funding for electronic health information and relationship to healthcare data security breaches*. Doctoral dissertation, Capella University.

Dedeke, A. (2017). Cybersecurity framework adoption: Using capability levels for implementation. *IEEE Security & Privacy*, 15(5), 47–54.
<https://doi.org/10.1109/MSP.2017.3681063>

Dedeke, A., & Masterson, K. (2019). Contrasting cybersecurity implementation frameworks (CIF) from three countries. *Information and Computer Security*, 27(3), 373–392.
<https://doi.org/10.1108/ICS-10-2018-0122>

Deloitte. (2012). *Core beliefs and culture: Chairman's survey findings*.
www.deloitte.com/us/about (Accessed 03 March 2021).

Deloitte. (2008). *National e-health and information principal committee: National e-health strategy*. Deloitte Touche Tohmatsu.

Denzin, N. K., & Lincoln, Y. S. (2005). *The discipline and practice of qualitative research*. In *SAGE Handbook of Qualitative Research* (3rd ed.). SAGE Publications.

Department of Health. (2012a). *National eHealth strategy for South Africa 2012/2013 to 2016/2017*. National Department of Health, Republic of South Africa.
https://www.isfteh.org/files/media/southafrica_ehealth_strategy_2012-2016.pdf (Accessed 13 November 2024).

Department of Health. (2012b). *National health act: Regulations relating to categories of hospitals*. Government Gazette, Republic of South Africa.
<https://www.knowledgehub.health.gov.za/elibrary/national-health-act-regulations-relating-categories-hospitals> (Accessed 20 November 2024).

Department of Health. (2012c). *Safety and security audit report on the public health facilities conducted by the ministerial task team on safety and security*. National Department of Health, Republic of South Africa.

Department of Health. (2012d). *The National health care facilities baseline audit national summary report*. National Department of Health, Republic of South Africa.
https://www.hst.org.za/publications/HST%20Publications/NHFA_webready_0.pdf
(Accessed 13 November 2024).

Department of Health. (2017). *National health act, 2003 (Act no 61 of 2003): National health insurance policy: Towards universal health coverage*. Government Gazette, 40955: 627, 30 June 2017. National Health Act, 2003
https://www.gov.za/sites/default/files/gcis_document/201707/40955gon627.pdf (Accessed 17 June 2024).

Derse, R. (2016). *Hackers target hospitals with ransomware*. Relias Media.
<https://www.reliasmedia.com/articles/137468-hackers-target-hospitals-with-ransomware>
(Accessed 05 November 2024).

Desroches, B. C. M., Agarwal, R., Angst, C. M., & Fischer, M. A. (2010). Differences between integrated and stand-alone e-prescribing systems have implications for future use. *Health Affairs*, 29(12), 2268–2277.
<https://www.healthaffairs.org/doi/pdf/10.1377/hlthaff.2010.0557>

Detmer, D., Bloomrosen, M., Raymond, B., & Tang, P. (2008). Integrated personal health records: Transformative tools for consumer-centric care. *BMC Medical Informatics and Decision Making*, 8, 1–14. <https://doi.org/10.1186/1472-6947-8-45>

DeVillis, F. R. (2017). *Scale development: Theory and applications* (4th ed.). SAGE Publications.

Dieleman, J. L., Templin, T., Sadat, N., Reidy, P., Chapin, A., Foreman, K., Haakenstad, A., Evans, T., L Murray, C. J., & Kurowski, C. (2016). National spending on health by source for 184 countries between 2013 and 2040. *Lancet*, 387(10037), 2521–2535. [https://doi.org/10.1016/S0140-6736\(16\)30167-2](https://doi.org/10.1016/S0140-6736(16)30167-2)

Dinev, T., Albano, V., Xu, H., D'Atri, A., & Hart, P. (2016). Individuals' attitudes towards electronic health records: A privacy calculus perspective. In *Advances in Healthcare Informatics and Analytics*, 19–50. Cham: Springer. <https://doi.org/10.1007/978-3-319-23294-2>

Dixon-woods, M., Agarwal, S., Young, B., Jones, D., & Sutton, A. (2004). *Integrative approaches to qualitative and quantitative evidence*. London, UK: Health Development Agency (Vol. 181). Report no 1842792555.

Djuranovic, B. L., Spalevic, Z., & Ilic, A. S. (2025). Protection of patients' data in e-health applications: challenges and abuses. In *Digital Transformation in Healthcare Systems for Patient Care, Wren* (233–252). Springer Nature Switzerland.

Dlamini, & Modise, M. (2012). Cybersecurity awareness initiatives in South Africa: A synergy approach. In *Proceedings of the 7th International Conference on Information Warfare and Security*, 10, 98–107.

Dogac, A. (2012). Interoperability in eHealth systems. In *Proceedings of the VLDB Endowment*, 5(12), 2020–2027. <https://doi.org/10.14778/2367502.2367568>

Du Toit, J. (2015). Research design. In E. A. Silva, P. Healey, N. Harris, and P. Van den Broeck (Eds.). *The Routledge handbook of planning research methods*. New York: Routledge.

Dworkin, S. L. (2012). Sample size policy for qualitative studies using in-depth interviews. *Archives of Sexual Behavior*, 41(6), 1319–1320. <https://doi.org/10.1007/s10508-012-0016-6>

e-Estonia. (2018). *Cybersecurity Report 2018: Investing in the security of information systems to secure digital lifestyle*. E-Estonia. <https://e-estonia.com/cyber-security-report-2018/> (Accessed 15 August 2020).

Edmonds, W., & Kennedy, T. (2017). *An applied guide to research designs quantitative, qualitative, and mixed methods* (2nd ed.). SAGE.

Eizenberg, E., & Jabareen, Y. (2017). Social sustainability: A new conceptual framework. *Sustainability (Switzerland)*, 9(1), 68. <https://doi.org/10.3390/su9010068>

Engemann, K. J., & Henderson, D. (2012). *Business continuity and risk management: Essentials of organizational resilience*. Rothstein Associates Inc.

Erku, D., Khatri, R., Endalamaw, A., Wolka, E., Nigatu, F., Zewdie, A., & Assefa, Y. (2023). Digital health interventions to improve access to and quality of primary health care services: A scoping review. *International Journal of Environmental Research and Public Health*, 20(19). <https://doi.org/10.3390/ijerph20196854>

Esfahani, A. A., Ahmadi, H., Nilashi, M., Alizadeh, M., Bashiri, A., Farajzadeh, M. A., Shahmoradi, L., Nobakht, M., & Rasouli, H. R. (2018). An evaluation model for the implementation of hospital information systems in public hospitals using multi-criteria-decision-making (MCDM) approaches. *International Journal of Engineering and Technology*, 7(1), 1–18. <https://doi.org/10.14419/ijet.v7i1.8404>

Etikan, I., Musa, S. A., & Alkassim, R. S. (2015). Comparison of snowball sampling and sequential sampling technique. *Biometrics & Biostatistics International Journal*, 3(1), 1–2. <https://doi.org/10.15406/bbij.2016.03.00055>

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1. <https://doi.org/10.11648/j.ajtas.20160501.11>

European Commission. (2012). eHealth action plan 2012-2020: Innovative healthcare for the 21st century. In *European Commission: COM (2012) (736)*.

https://health.ec.europa.eu/document/download/39c9a1ee-6afa-4ab9-a472-ddeac925d14f_en?filename=com_2012_736_en.pdf

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679. *Official Journal of the European Union*, 119: 1–88. <https://eur-lex.europa.eu/eli/reg/2016> (Accessed 7 February 2025).

European Union Agency for Network and Information Security (ENISA). (2017). Cybersecurity culture in organisations. In *European Union Agency for Network and Information Security*. <https://doi.org/10.2824/10543>

Evans, J. A. (1999). Electronic medical records system (Patent No. USOO5924074A). In *United States Patent (USOO5924074A)*.

<https://patentimages.storage.googleapis.com/38/55/f0/40f58110804942/US5924074.pdf>

Eysenbach, G. (2001). What is E-Health? *Journal of Medical Internet Research*, 3(2), 1–5. <https://doi.org/10.2196/jmir.3.2.e20>

Farzandipour, M., Sadoughi, F., Ahmadi, M., & Karimi, I. (2010). Security requirements and solutions in electronic health records: Lessons learned from a comparative study. *Journal of Medical Systems*, 34(4), 629–642. <https://doi.org/10.1007/s10916-009-9276-7>

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, 46(3), 541–562. <https://doi.org/10.1016/j.jbi.2012.12.003>

Fink, A. (2003). *How to sample in surveys* (2nd ed.). SAGE Publications. <https://dx.doi.org/10.4135/9781412984478>

Fink, A. (2014). *Conducting research literature reviews: From the internet to paper* (4th ed.). SAGE Publications.

Fink, A. (2017). *How to conduct surveys a step-by-step guide* (6th ed.). SAGE Publications.

Fischer, E. A. (2016). *Cybersecurity issues and challenges: In brief*. Congressional Research Service Report no R43831, Version 18.

<https://crsreports.congress.gov/product/pdf/R/R43831/18> (Accessed 29 August 2019).

Fonseca, T., Ribeiro, C., & Granja, C. (2009). Vital signs in intensive care: Automatic acquisition and consolidation into electronic patient records. *Journal of Medical Systems*, 33(1), 47–57. <https://doi.org/10.1007/s10916-008-9163-7>

Fontaine, P., Ross, S. E., Zink, T., & Schilling, L. M. (2010). Systematic review of health information exchange in primary care practices. *Journal of the American Board of Family Medicine*, 23(5), 655–670. <https://doi.org/10.3122/jabfm.2010.05.090192>

Forte, D., & Power, R. (2007). The ultimate cybersecurity checklist for your workforce. *Computer Fraud and Security*, 2007(9), 14–19. [https://doi.org/10.1016/S1361-3723\(07\)70117-3](https://doi.org/10.1016/S1361-3723(07)70117-3)

Fottler, M. D., Blair, J. D., Whitehead, C. J., Laus, M. D., & Savage, G. T. (1989). Assessing key stakeholders: Who matters to hospitals and why? *Hospital & Health Services Administration*, 34(4), 525.

Francis, T. (2013). Electronic health records: Where we are and where we're going. *Physician Executive*, 39(4), 82–84.

Frayssinet Delgado, M., Esenarro, D., Juárez Regalado, F. F., & Díaz Reátegui, M. (2021). Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. *3C TIC: Cuadernos de Desarrollo Aplicados a Las TIC*, 10(2), 123–141. <https://doi.org/10.17993/3ctic.2021.102.123-141>

Fridlund, B., & Hildingh, C. (2000). Health and qualitative analysis methods. In *Qualitative research, methods in the service of health*, Student Literature, Lund.

Frost & Sullivan, Booze, Allen, H., & (ISC)2. (2014). *The 2013 (ISC) 2 global information security workforce study*. www.frost.com

Furnell, S., & Thomson, K. L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud and Security*, 2009(2), 5–10. [https://doi.org/10.1016/S1361-3723\(09\)70019-3](https://doi.org/10.1016/S1361-3723(09)70019-3)

Furusa, S. S., & Coleman, A. (2018). Factors influencing e-health implementation by medical doctors in public hospitals in Zimbabwe. *South Africa Journal of Information Management*, 20(1), 928. <https://doi.org/10.4102/sajim.v20i1.928>

Gagnon, M. P., Desmartis, M., Labrecque, M., Car, J., Pagliari, C., Pluye, P., Frémont, P., Gagnon, J., Tremblay, N., & Légaré, F. (2012). Systematic review of factors influencing the adoption of information and communication technologies by healthcare professionals. *Journal of Medical Systems*, 36(1), 241–277. <https://doi.org/10.1007/s10916-010-9473-4>

Gagnon, M. P., Nsangou, É. R., Payne-Gagnon, J., Grenier, S., & Sicotte, C. (2014). Barriers and facilitators to implementing electronic prescription: A systematic review of user groups' perceptions. *Journal of the American Medical Informatics Association* 21(3), 535–541. <https://doi.org/10.1136/amiajnl-2013-002203>

Gardner, R. M., Clemmer, T. P., Evans, R. S., & Mark, R. G. (2014). Patient-monitoring Systems. In E.H. Shortliffe, J.J. Cimino (Eds.), *Biomedical Informatics*, (Chap 19). Springer-Verlag London. https://doi.org/10.1007/978-1-4471-4474-8_19

Garren, S. T., & Osborne, K. M. (2021). Robustness of t-test based on skewness and kurtosis. *Journal of Advances in Mathematics and Computer Science*, 36(2), 102–110. <https://doi.org/10.9734/jamcs/2021/v36i230342>

Gatzoulis, L., & Iakovidis, I. (2007). Wearable and portable eHealth systems. *IEEE Engineering in Medicine and Biology Magazine*, 26(5), 51–56. <https://doi.org/10.1109/EMB.2007.901787>

Gcaza, N. (2017). *A national strategy towards cultivating a cybersecurity culture in South Africa*. Doctoral dissertation, Nelson Mandela Metropolitan University.

Gcaza, N., & von Solms, R. (2017a). A strategy for a cybersecurity culture: A South African perspective. *Electronic Journal of Information Systems in Developing Countries*, 80(1), 1–17. <https://doi.org/10.1002/j.1681-4835.2017.tb00590.x>

Gcaza, N., von Solms, R. (2017b). Cybersecurity Culture: An Ill-Defined Problem. In M. Bishop, L. Fitcher, N. Miloslavskaya, & M. Theocharidou (Eds.), *Information Security Education for a Global Digital Society*. WISE 2017. IFIP Advances in Information and Communication Technology, vol 503, 98–109. Springer, Cham. https://doi.org/10.1007/978-3-319-58553-6_9

Gcaza, N., von Solms, R., Grobler, M., & van Vuuren, J. (2017). A general morphological analysis: Delineating a cyber-security culture. *Information and Computer Security*, 25(3), 259–278. <https://doi.org/10.1108/ICS-12-2015-0046>

Gcaza, N., von Solms, R., & Van Vuuren, J. (2015). An ontology for a national cybersecurity culture environment. In *Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015*, Lesvos, Greece, 1–10. <https://www.cscan.org/?page=openaccess>

Gell, G., & Gitter, T. (2008). Hospital information system / electronic health record (HIS / HER) and clinical research. In *Digital Excellence: University Meets Economy*. Springer, Berlin, Heidelberg.

Georgiadou, A., Michalitsi-Psarrou, A., Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Doukas, G., Ntanos, C., Ribeiro, L. L., & Askounis, D. (2021b). Hospitals' cybersecurity culture during the COVID-19 crisis. *Healthcare (Switzerland)*, 9(10), 1–21. <https://doi.org/10.3390/healthcare9101335>

Georgiadou, A., Mouzakis, S., & Askounis, D. (2020a). Towards assessing critical infrastructures' cyber-security culture during the COVID-19 crisis: A tailor-made survey. In *Proceedings of the 14th the International Conference on Networks and Security, NSEC 2020*, Sydney, 71–80. <https://doi.org/10.5121/csit.2020.101806>

Georgiadou, A., Mouzakis, S., & Askounis, D. (2021a). Designing a cyber-security culture assessment survey targeting critical infrastructures during Covid-19 crisis. *International Journal of Network Security & Its Applications*, 13(1), 33–50. <https://doi.org/10.5121/ijnsa.2021.13103>

- Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2020b). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, 62(3), 452–462. <https://doi.org/10.1080/08874417.2020.1845583>
- Ghafur, S., Grass, E., Jennings, N. R., & Darzi, A. (2019). The challenges of cybersecurity in health care: The UK National Health Service as a case study. *The Lancet Digital Health*, 1(1), e10–e12. [https://doi.org/10.1016/S2589-7500\(19\)30005-6](https://doi.org/10.1016/S2589-7500(19)30005-6)
- Gheraouti-Hélie, S. (2009). An inclusive information society needs a global approach of information security. In *Proceedings of the International Conference on Availability, Reliability and Security*, 658–662. <https://doi.org/10.1109/ARES.2009.127>
- Gheraouti-Hélie, S. (2010). A national strategy for an effective cybersecurity approach and culture. In *Proceedings of the 5th, the International Conference on Availability, Reliability, and Security*, ARES 2010, Krakow, Poland, 370–373. <https://doi.org/10.1109/ARES.2010.119>
- Ghosh, A., & Ashok, I. (2017, May 15). *WannaCry: List of major companies and networks hit by ransomware around the globe*. International Business Times. <https://www.ibtimes.co.uk/wannacry-list-major-companies-networks-hit-by-deadly-ransomware-around-globe-1621587> (Accessed 8 July 2020).
- Gillham, B. (2000). *Case study research methods*. Bloomsbury Publishing Plc.
- Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-psarrou, A., Doukas, G., Kontoulis, M., Nikoloudakis, Y., Marin, S., Cabecinha, R., & Ntanos, C. (2022). A cybersecurity culture survey targeting healthcare critical infrastructures. *Healthcare*, 10(2), 327. <https://doi.org/10.3390/healthcare10020327>
- Glandon, G., & Buck, T. (1994). Cost-benefits analysis of medical information systems: A critique. In J. G. Anderson, C. E. Aydin, & S. Jay (Eds.), *Evaluating health care information systems: Methods and applications*. SAGE Publications.
- Glaser, B. G. (2016). Open coding descriptions. *Grounded Theory Review*. 15(2), 108–110. <https://groundedtheoryreview.org/index.php/gtr/article/view/239>

Glaspie, H.W., Karwowski, W. (2018). Human factors in information security culture: A literature review. In Nicholson, D. (Eds.) *Advances in Intelligent Systems and Computing*, vol 593. Springer, Cham. https://doi.org/10.1007/978-3-319-60585-2_25

Godwin III, J. B., Kulpim, A., Rauscher, K. F., & Yaschenko, V. (2014). *Critical terminology foundations. Russia-US Bilateral on Cybersecurity*. (Policy Report 2). EastWest Institute and Information Security Institute, Moscow State University.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report*, 8(4), 597–607. <http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf>

Goldberg, M. A. (1996). Teleradiology and telemedicine. *Radiologic Clinics of North America*, 34(3), 647–665. [https://doi.org/10.1016/S0033-8389\(22\)00496-1](https://doi.org/10.1016/S0033-8389(22)00496-1)

Goldman, D. (2019, June 5). *It's not just quest: LabCorp says it was hacked too*. CNN. <https://edition.cnn.com/2019/06/04/tech/labcorp-hack/index.html> (Accessed 4 November 2024).

Goldstein, D. H., Phelan, R., Wilson, R., Ross-White, A., Vandenberg, E. G., Penning, J. P., & Jaeger, M. (2014). Brief review: Adoption of electronic medical records to enhance acute pain management. *Journal of Anaesthesia*, 61(2), 164–179. <https://doi.org/10.1007/s12630-013-0069-6>

Gomes, R., & Lapão, L. V. (2008). The adoption of IT security standards in a healthcare Environment. *Studies in Health Technology and Informatics*, 136, 765–770. <https://pubmed.ncbi.nlm.nih.gov/18487824/>

Goozner, M. (2014). Protect my privacy but share my data. *Modern Healthcare*, 44(4), 22.

Gough, D. (2007). Weight of evidence: A framework for the appraisal of the quality and relevance of evidence. *Research Papers in Education*, 22(2), 213–228. <https://doi.org/10.1080/02671520701296189>

Gough, D., Oliver, S., & Thomas. 2017. *Introduction to systematic reviews* (2nd ed.). SAGE Publications. London.

Graham, M., & Dutton, W. H. (2019) (Eds.). *Society and the internet: How networks of information and communication are changing our lives* (2nd ed.). Oxford University Press.

- Grigsby, J., Schlenker, R. E., Kaehny, M. M., Shaughnessy, P. W., & Sandberg, E. J. (1995). Analytic framework for evaluation of telemedicine. *Telemedicine Journal*, 1(1), 31–39. <https://doi.org/10.1089/tmj.1.1995.1.31>
- Grossoehme, D. H. (2014). Overview of qualitative research. *Journal of Health Care Chaplaincy*, 20(3), 109–122. <https://doi.org/10.1080/08854726.2014.925660>
- Gundu, T., Maronga, M. I., & Boucher, D. (2019). Industry 4. 0 business perspective: Fostering a cybersecurity culture in a culturally diverse workplace. In *Proceedings of the 4th International Conference on the Internet, Cybersecurity and Information Systems*, Johannesburg, South Africa, 85–94.
- Gupta, D., & Bajramovic, E. (2017). Security culture for nuclear facilities. In *Proceedings of the AIP Conference*, 1799(050014). <https://doi.org/10.1063/1.4972948>
- Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N., & Müller, G. (2011). Aspects of privacy for electronic health records. *International Journal of Medical Informatics*, 80(2), e26–e31. <https://doi.org/10.1016/j.ijmedinf.2010.10.001>
- Hadlington, L. (2018). Employees’ attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology*, 12(1), 49-62. <https://doi.org/10.5281/zenodo.1467909>
- Hair, J., Black, W., Babin, B., & Anderson, R. (2019). *Multivariate data analysis* (8th ed.). Cengage Learning. ISBN 9781473756540
- Halevi, T., Memon, N., Lewis, J., Ponnurangam, K., Arora, A., Dagar, N., Aloul, F., & Chen, J. (2016). Cultural and psychological factors in cyber-security. In *Proceedings of the 18th International Conference on Information Integration and Web-Based Applications and Services, iiWAS 2016*, Singapore, 318–324. <https://doi.org/10.1145/3011141.3011165>
- Hall, R. (2013). Mixed methods: In search of a paradigm. In Le & Lê (Eds.), *Undertaking Research in a changing and challenging world*. Nova Science Publishers Incorporated. https://www.researchgate.net/publication/259045135_Mixed_Methods_In_search_of_a_paradigm (Accessed 25 November 2024).

Hallberg, D., & Salimi, N. (2020). Qualitative and quantitative analysis of definitions of e-health and m-health. *Healthcare Informatics Research*, 26(2), 119–128.

<https://doi.org/10.4258/hir.2020.26.2.119>

Hand, S. (2021, August 21). *R46 million — The cost of a data breach at a South African company*. <https://mybroadband.co.za/news/security/410630-r46-million-the-cost-of-a-data-breach-at-a-south-african-company.html> (Accessed 30 September 2024).

Hanik, B., & Stellefson, M. (2011). E-Health literacy competencies among undergraduate health education students: A preliminary study. *International Electronic Journal of Health Education*, 14, 46–58. <https://eric.ed.gov/?id=EJ946322>

Haque, S. A., Aziz, S. M., & Rahman, M. (2014). Review of cyber-physical system in healthcare. *International Journal of Distributed Sensor Networks*, 10(4), 217415
<https://doi.org/10.1155/2014/217415>

Harries, D., Yellowless, P.M. (2013) Cyberterrorism: Is the U.S. healthcare system safe? *Telemedicine and E-Health* 19(1), 61–66. <https://doi.org/10.1089/tmj.2012.0022>

Hart, C. (2018). *Doing a Literature Review: Releasing the Research Imagination* (2nd ed.). SAGE Publications.

Hassan, N. H., Maarop, N., Ismail, Z., & Abidin, W. Z. (2017). Information security culture in health informatics environment: A qualitative approach. In *Proceedings of the 2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*, Langkawi Island, Malaysia 1–6. <https://doi.org/10.1109/ICRIIS.2017.8002450>

Hassim, A., Heywood, M., & Berger, J. (Eds.). (2007). The private health care sector. In *Health and Democracy: A guide to human rights, health law and policy in post-apartheid South Africa*. Siberlink. 162–199.

Haynes, R. B., Wilczynski, N. L., & the Computerized Clinical Decision Support System (CCDSS) Systematic Review Team. (2010). Effects of computerized clinical decision support systems on practitioner performance and patient outcomes: Methods of a decision-maker-researcher partnership systematic review. *Implementation Science*, 5(1), 1–8.
<https://doi.org/10.1186/1748-5908-5-12>

Häyrynen, K., Saranto, K., & Nykänen, P. (2008). Definition, structure, content, use and impacts of electronic health records: A review of the research literature. *International Journal of Medical Informatics*, 77(5), 291–304.

<https://doi.org/10.1016/j.ijmedinf.2007.09.001>

He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. *Journal of Medical Internet Research*, 23(4), 1–18. <https://doi.org/10.2196/21747>

Health Care Industry Cybersecurity Task Force. (2017). Report on improving cybersecurity in the health care industry.

<https://nsarchive.gwu.edu/sites/default/files/documents/3864731/Health-Care-Industry-Cybersecurity-Task-Force.pdf> (Accessed 6 August 2020).

Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale.

Information Management and Computer Security, 21(4), 266–287.

<https://doi.org/10.1108/IMCS-08-2012-0043>

Henry, G. T. (1990). *Practical sampling*. SAGE Publications.

Hidayati, A. N., Riadi, I., Ramadhani, E., & Amany, S. U. Al. (2021). Development of conceptual framework for cyber fraud investigation. *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, 7(2), 125–135. <https://doi.org/10.26594/REGISTER.V7I2.2263>

HIPAA E-Tool. (2024, January 30). *Concentra is the latest victim of the PJ & A data breach*.

HIPAA E-Tool.. <https://thehipaaetool.com/concentra-is-the-latest-victim-of-the-pja-data-breach/>

Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the mind - intercultural cooperation and its importance for survival* (Revised and expanded 3rd ed.). McGraw-Hill.

Holdsworth, J., & Apeh, E. (2017). An effective immersive cybersecurity awareness learning platform for businesses in the hospitality sector. In *Proceedings of the IEEE 25th International Requirements Engineering Conference Workshops*, REW 2017, 111–117.

<https://doi.org/10.1109/REW.2017.47>

- Holton, J. A. (2010). The coding process and its challenges. *The Grounded Theory Review*, 9(1), 21–40. <https://groundedtheoryreview.org/index.php/gtr/article/view/63?utm>
- Hope, A. (2020). *Credit information of millions of South Africans and businesses leaked in a massive Experian data breach*. CPO Magazine. <https://www.cpomagazine.com/cyber-security/credit-information-of-millions-of-south-africans-and-businesses-leaked-in-a-massive-experian-data-breach/> (Accessed 22 September 2022).
- Horner, V., Rautenbach, P., Mbananga, N., Mashamba, T., & Kwindu, H. (2013). An e-health decision support system for improving compliance of health workers to the maternity care protocols in South Africa. *Applied Clinical Informatics*, 4(1), 25–36. <https://doi.org/10.4338/ACI-2012-10-RA-0044>
- Horwood, C., Luthuli, S., Mapumulo, S., Haskins, L., Jensen, C., Pansegrouw, D., & McKerrow, N. (2023). Challenges of using e-health technologies to support clinical care in rural Africa: A longitudinal mixed methods study exploring primary health care nurses' experiences of using an electronic clinical decision support system (CDSS) in South Africa. *BMC Health Services Research*, 23(1), 30. <https://doi.org/10.1186/s12913-022-09001-2>
- Hotchkiss, D., Aqil, A., Lippeveld, T., & Mukooyo, E. (2010). Evaluation of the performance of routine information system management (PRISM) framework: evidence from Uganda. *BMC Health Services Research*, 10, 188. <https://doi.org/10.1186/1472-6963-10-188>
- Howard, M. D. (1995). Network security (and the internet). *International Journal of Network Management*, 5(6), 296–304. <https://doi.org/10.1002/nem.4560050604>
- Hsiao, J.-L., & Chen, R.-F. (2016). Critical factors influencing physicians' intention to use computerized clinical practice guidelines: An integrative model of activity theory and the technology acceptance model. *BMC Medical Informatics & Decision Making*, 16, 3. <https://doi.org/10.1186/s12911-016-0241-3>
- Huang, K., & Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. In *Proceedings of the Annual Hawaii International Conference on System Sciences*, AHICCC 2019, 6398–6407. <https://doi.org/10.24251/hicss.2019.769>

IBM Security. (2014). *IBM security services 2014 cybersecurity intelligence index*. In IBM global technology services.

https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF?utm_source=chatgpt.com (Accessed 10 July 2020).

IBM Security: Cost of a data breach report (2019). *Computer Fraud & Security*, 2019(8), 4
[https://doi.org/10.1016/s1361-3723\(19\)30081-8](https://doi.org/10.1016/s1361-3723(19)30081-8)

IBM Security: Cost of a Data Breach Report. (2021). *Computer Fraud & Security*, 2021(8), 4. [https://doi.org/10.1016/S1361-3723\(21\)00082-8](https://doi.org/10.1016/S1361-3723(21)00082-8)

IBM Security. (2023). *Cost of a data breach report 2023*. In IBM Corporation.
<https://www.slideshare.net/slideshow/2023-ibm-cost-of-a-data-breach-reportpdf/259470830>
(Accessed 04 November 2024).

IBM Security. (2024). *Cost of a data breach report 2024*. In IBM.
<https://www.ibm.com/security/data-breach/>. (Accessed 27 August 2024).

IDABC. (2004). *European interoperability framework for Pan-European E-Government Services (PEGS)*. European Communities, Luxembourg. ISBN 92-894-8389-X.
<https://op.europa.eu/en/publication-detail/-/publication/a4778634-27fa-43b4-9912-f753c4fd3f> (Accessed 11 June 2020).

Institute of Medicine (2001). Crossing the quality chasm: A new health system for the 21st century. *National Academies Press*, 1-8. <https://doi.org/10.17226/10027>

International Telecommunication Union (ITU). (2008a). *ITU global cybersecurity agenda (GCA), High-Level Experts Group (HLEG) global strategic report*.
https://www.itu.int/osg/csd/cybersecurity/gca/docs/global_strategic_report.pdf (Accessed 08 February 2021).

International Telecommunication Union (ITU). (2008b). Overview of cybersecurity. In *Series X: Data Networks, Open System Communications and Security - Telecommunication Security: Vol. X.1205*. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items/ (Accessed 7 May 2020).

International Telecommunication Union (ITU). (2021). *Guide to developing a national cybersecurity strategy* (Version 2). <https://ncsguide.org/wp-content/uploads/2021/11/2021-Guide-1.pdf> (Accessed 18 June 2022).

Ioannou, M., Stavrou, E., & Bada, M. (2019). Cybersecurity culture in computer security incident response teams: Investigating difficulties in communication and coordination. In *Proceeding of the 2019 International Conference on Cybersecurity and Protection of Digital Services, Cybersecurity 2019*, Oxford, UK, 1–4.
<https://doi.org/10.1109/CyberSecPODS.2019.8885240>

ISACA. (2015). Cybersecurity fundamentals study guide. *Information System Audit and Control Association (ISACA)*. ISBN 978-1-60420-594-7

ISACA & CMMI Institute. (2018). Narrowing the culture gap for better business results. <https://www.isaca.org/-/media/files/isacadp/project/isaca/knowledge-and-insights/info-files/cybersecurity-culture-report.pdf> (Accessed 16 May 2021).

Ismail, N. I., Abdullah, N. H., Shamsudin, A., & Ariffin, N. A. N. (2013). Implementation differences of Hospital Information System (HIS) in Malaysian public hospitals. *International Journal of Social Science and Humanity*, 3(2), 115–120.
<https://doi.org/10.7763/ijssh.2013.v3.208>

ISO/IEC 27032. (2012). *ISO/IEC 27032:2012(en), Information technology: Security techniques, guidelines for cybersecurity*. <https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en>

ISO 27799. (2016). *ISO 27799:2016 - Health informatics: Information security management in health using ISO/IEC 27002*. Geneva, Switzerland: ISO
<https://www.iso.org/standard/62777.html>

ISO/IEC. (2022). *ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection - information security controls*. ISO. <https://www.iso.org/standard/75652.html>

ISO/IEC. (2023). *ISO/IEC 27032:2023: Cybersecurity - guidelines for Internet security* (2nd ed.). <https://www.iso.org/standard/76070.html>

- ITRC. (2019). *2018 End-of-year data breach report*. Identity Theft Resource Center. https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf (Accessed 12 April 2020).
- ITRC. (2020). *2019 End-of-year data breach report*. Identity Theft Resource Center. https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (Accessed 2 May 2020).
- ITRC. (2024). *2023 Data breach report*. Identity Theft Resource Center. https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf (Accessed 28 August 2024).
- Iyawa, G. E., Herselman, M., & Botha, A. (2016). Digital health innovation ecosystems: From systematic literature review to conceptual framework. *Procedia Computer Science*, 100, 244–252. <https://doi.org/10.1016/j.procs.2016.09.149>
- Jääskeläinen, A., & Roitto, J. M. (2015). Designing a model for profiling organizational performance management. *International Journal of Productivity and Performance Management*, 64(1), 5–27. <https://doi.org/10.1108/IJPPM-01-2014-0001>
- Jabareen, Y. (2009). Building a conceptual framework: Philosophy, definitions, and procedure. *International Journal of Qualitative Methods*, 8(4), 49–62. <https://doi.org/10.1177/160940690900800406>
- Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research*, 20(5), e10059. <https://doi.org/10.2196/10059>
- Jansen Van Vuuren, J. C. (2016). *Methodology and model to establish cybersecurity for national security in Africa using South Africa as a case study*. Doctoral dissertation, University of Venda.
- Jennett, P., Scott, R., Affleck, H. L., Hailey, D., Ohinmaa, A., Anderson, C., Thomas, R., Young, B., & Lorenzetti, D. (2004). Policy implications associated with the socioeconomic and health system impact of telehealth: A case study from Canada. *Telemed Journal of Electronic Health*, 10(1), 77–83. <https://doi.org/10.1089/153056204773644616>

- Jha, A., DesRoches, C., Campbell, E., Donelan, K., Rao, S., Ferris, T., Shield, A., Rosenbaum, S., & Blumenthal, D. (2009). Use of electronic health records in U.S. hospitals. *The New England Journal of Medicine*, 360(16), 1628–1638. <https://doi.org/http://dx.doi.org/10.1056/NEJMsa0900592>
- Jiang, J. J., Muhanna, W. A., & Klein, G. (2000). User resistance and strategies for promoting acceptance across system types. *Information and Management*, 37(1), 25-36. [https://doi.org/10.1016/S0378-7206\(99\)00032-4](https://doi.org/10.1016/S0378-7206(99)00032-4)
- Jolliffe, I. T. (2002). *Principal component analysis* (2nd ed.). Springer.
- Juma, K., Nahason, M., Apollo, W., Gregory, W., & Patrick, O. (2012). Current status of e-health in Kenya and emerging global research trends. *International Journal of Information and Communication Technology Research*, 2(1), 50–54.
- Jump, M. (2019). Fighting cyberthreats with technology solutions. *Biomedical Instrumentation and Technology*, 53(1), 38–43. <https://doi.org/10.2345/0899-8205-53.1.38>
- Kadena, E., & Gupi, M. (2021). Human factors in cybersecurity. *Security Science Journal*, 2(2), 51–64. <https://doi.org/10.37458/ssj.2.2.3>
- Kaiser, H. F., & Rice, J. (1974). Little Jiffy, Mark Iv. *Educational and Psychological Measurement*, 34(1), 111–117. <https://doi.org/10.1177/001316447403400115>
- Kart, F., Miao, G., & Moser, L. E. (2007). A distributed e-healthcare system based on the service oriented architecture. In *Proceedings of the IEEE International Conference on Services Computing (SCC 2007)*, Salt Lake City, UT, USA, 652–659, <https://doi.org/10.1109/SCC.2007.2>
- Kaspersky. (2021). *Redefining the human factor in cybersecurity*. Kaspersky Daily. <https://www.kaspersky.com/blog/human-factor-360-report-2023/> (Accessed 4 November 2024).

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering*. EBSE Technical Report EBSE-2007-01, Vol. 2.3. Keele University

https://legacyfileshare.elsevier.com/promis_misc/525444systematicreviewsguide.pdf

(Accessed 3 March 2024).

Khalifehsoltani, S. N., & Gerami, M. R. (2010). E-Health challenges, opportunities and experiences of developing countries. In *Proceedings of the 2010 International Conference on e-Education, e-Business, e-Management and e-Learning*, IC4E 2010, Sanya, China, 264–268.

<https://doi.org/10.1109/IC4E.2010.119>

Khandkar, S. H. (2009). *Open coding*. University of Calgary.

<https://cspages.ucalgary.ca/~saul/wiki/uploads/CPSC681/open-coding.pdf>

Khubone, T., Tlou, B., & Mashamba-Thompson, T. P. (2020). Electronic health information systems to improve disease diagnosis and management at point-of-care in low and middle income countries: A narrative review. *Diagnostics*, 10(5), 327.

<https://doi.org/10.3390/diagnostics10050327>

Kiberu, V. M., Mars, M., & Scott, R. E. (2017). Barriers and opportunities to implementation of sustainable e-health programmes in Uganda: A literature review. *African Journal of Primary Health Care and Family Medicine*, 9(1), 1–10.

<https://doi.org/10.4102/phcfm.v9i1.1277>

Kilsdonk, E., Peute, L. W. P., Knijnenburg, S. L., & Jaspers, M. W. M. (2011). Factors known to influence acceptance of clinical decision support systems. In *User Centred Networked Health Care*, 150–154, IOS Press. <https://doi.org/10.3233/978-1-60750-806-9-150>

Kim, C., Lee, J-S., & Kim, Y-I. (2002). Early-stage evolution of a hospital information system in a middle-income country: A case study of Korea. *International Journal of Healthcare Technology and Management*, 4(6), 514–524.

<https://doi.org/10.1504/IJHTM.2002.002429>

- Kissel, R. (Ed.). (2011). *Glossary of key information security terms. Revision 1 (NISTIR 7298)*, National Institute of Standards and Technology (NIST). U.S Department of Commerce <https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7298r1.pdf> (Accessed 18 August 2021).
- Klimburg, A. (Ed.). (2012). *National cybersecurity framework manual*. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).
- Klonoff, D. C. (2015). Cybersecurity for connected diabetes devices. *Journal of Diabetes Science and Technology*, 9(5), 1143–1147. <https://doi.org/10.1177/1932296815583334>
- Kohlbacher, F. (2006). The use of qualitative content analysis in case study research. *Forum Qualitative Sozialforschung*, 7(1), 1–30. <https://doi.org/10.17169/fqs-7.1.75>
- Kolb, B. (2008). *Marketing research a practical approach*. SAGE Publications.
- Koppel, R., Smith, S., Blythe, J., & Kothari, V. (2015). Workarounds to computer access in healthcare organizations: You want my password or a dead patient? *Studies in Health Technology and Informatics*, 208, 215–220. <https://doi.org/10.3233/978-1-61499-488-6-215>
- Kortjan, N., & von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in South Africa. *South African Computer Journal*, 52(52), 29–41. <https://doi.org/10.18489/sacj.v52i0.201>
- Kotz, D., Gunter, C. A., Kumar, S., & Weiner, J. P. (2016). Privacy and security in mobile health: A research agenda. *Computer*, 49(6), 22–30. <https://doi.org/10.1109/MC.2016.185>
- Kovačić, M., Mutavdžija, M., & Buntak, K. (2022). E-health application, implementation and challenges: A literature review. *Business Systems Research: International Journal of the Society for Advancing Innovation and Research in Economy*, 13(1), 1–18. <https://doi.org/10.2478/bsrj-2022-0001>
- Krippendorff, K. (2004). *Content analysis: An introduction to its methodology*. SAGE Publications.

Krishnamoorthy, S., Dua, A. & Gupta, S. (2023). Role of emerging technologies in future IoT-driven healthcare 4.0 technologies: A survey, current challenges and future directions. *Journal of Ambient Intelligence and Humanized Computing*, 14, 361–407. <https://doi.org/10.1007/s12652-021-03302-w>

Krist, A. H., & Woolf, S. H. (2011). A vision for patient-centered health information systems. *Journal of the American Medical Association (JAMA)*, 305(3), 300–301. <https://doi.org/10.1001/jama.2010.2011>

Krueger. (2015). *Focus groups: A practical guide for applied research* (5th ed.). Thousand Oaks, CA: SAGE.

Krüger, K., Strand, L., Geitung, J.T., Eide, G. E., & Grimsmo, A. (2011). Can electronic tools help improve nursing home quality? *International Scholarly Research Notices (ISRN) Nursing*, 2011(1), 208143. <https://doi.org/10.5402/2011/208142>

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, 25(1), 1–10. <https://doi.org/10.3233/THC-161263>

Ksibi, S., Jaidi, F. & Bouhoula, A. (2023). A comprehensive study of security and cybersecurity risk management within e-health systems: Synthesis, analysis and a novel quantified approach. *Mobile Network Application*, 28, 107–127. <https://doi.org/10.1007/s11036-022-02042-1>

Lakshmann, R. (2020, September 21). *A patient dies after ransomware attack paralyzes German hospital systems*. The Hacker News. <https://thehackernews.com/2020/09/a-patient-dies-after-ransomware-attack.html> (Accessed 28 September 2020).

Lam, M. K., Hines, M., Lowe, R., Nagarajan, S., Keep, M., Penman, M., & Power, E. (2016). Preparedness for eHealth: Health sciences students' knowledge, skills, and confidence. *Journal of Information Technology Education: Research*, 15(2016), 305–334. <https://doi.org/10.28945/3523>

Langford, B., Schoenfeld, G., & Izzo, G. (2002). Norminal grouping sessions vs focus groups. *Qualitative Market Research: An International Journal*, 5(1), 58–70. <https://doi.org/10.1108/13522750210414517>

Lavallée, M., Robillard, P. N., & Mirsalari, R. (2014). Performing systematic literature reviews with novices: An iterative approach. *IEEE Transactions on Education*, 57(3), 175–181. <https://doi.org/10.1109/TE.2013.2292570>

Leavy, P. (2017). *Research design: Quantitative, qualitative, mixed methods, arts-based, and community-based participatory research approaches*. The Guilford press.

Lee, A. (2004). Thinking about social theory and philosophy for information systems. In J. Mingers & L. Willcocks (Eds.), *Social Theory and Philosophy for Information Systems*, 1–26. John Wiley & Sons.

Lee, H. W., Ramayah, T., & Zakaria, N. (2012a). External factors in hospital information system (HIS) adoption model: A case in Malaysia. *Journal of Medical Systems*, 36(4), 2129–2140. <https://doi.org/10.1007/s10916-011-9675-4>

Lee, I., Sokolsky, O., Chen, S., Hatcliff, J., Jee, E., Kim, B., King, A., Mullen-Fortino, M., Park, S., Roederer, A., & Venkatasubramanian, K. (2012b). Challenges and research directions in medical cyber-physical systems. In *Proceedings of the IEEE*, 100(1), 75–90. <https://doi.org/10.1109/JPROC.2011.2165270>

Leenen, L., Aschman, M., Grobler, M., & van Heerden, A. (2018). Facing the culture gap in operationalising cyber within a military context. In *Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018*, Washington, D.C, USA, 387–394. <https://tinyurl.com/ICCWS2018>

Leenen, L., & Van Vuuren, J. (2019). Framework for the cultivation of a military cybersecurity culture. In *Proceedings of the 14th International Conference on Cyber Warfare and Security, ICCWS 2019*, Stellenbosch, South Africa, 212–220.

Letsebe, K. (2017, May 9). *Healthcare information breaches continue to rise*. ITWeb. <https://www.itweb.co.za/content/3mYZR XM9JJ9qOgA8> (Accessed 11 August 2020).

Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science: The International Journal of an Emerging Transdiscipline*, 9, 181–211. <https://doi.org/10.28945/479>

Leyden, J. (2024, March 18). *South African government pension data leak fears spark probe*. DARKREADING Global. <https://www.darkreading.com/cyber-attacks-data-breaches/south-african-government-pension-data-leak-fears-spark-probe> (Accessed 12 September 2024).

Lindner, S. A., Ben Davoren, J., Vollmer, A., Williams, B., & Seth Landefeld, C. (2007). An electronic medical record intervention increased nursing home advance directive orders and documentation. *Journal of the American Geriatrics Society*, 55(7), 1001–1006.
<https://doi.org/10.1111/j.1532-5415.2007.01214.x>

Liska, A. (2021). *Ransomware: Understand. Prevent. Recover*. Recorded Future.
<https://go.recordedfuture.com/hubfs/Ransomware-understand-prevent-recover.pdf> (Accessed 3 July 2025).

Loică, M.-F. (2017). Genesis of cybersecurity culture: An important component of education for a modern society. In *Proceedings of the International Scientific Conference Strategies XXI*, Bucharest, Romania, 387–397.

Luijff, E., Besseling, K., & Graaf, P. De. (2013). Nineteen national cybersecurity strategies. *International Journal of Critical Infrastructures*, 9(1/2), 3–31.
<https://doi.org/10.1504/IJCIS.2013.051608>

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology and Health Care*, 24(1), 1–9.
<https://doi.org/10.3233/THC-151102>

Lundy, O., & Cowling, A. G. (1996). *Strategic human resource management*. Routledge.

Mac Naughton, G., & Hughes, P. (2008). *Doing action research in early childhood studies: a step-by-step guide*. McGraw - Hill International UK Ltd.

Mackenzie, P. (2010). School choice in an international context. *Journal of Research in International Education*, 9(2), 107–123. <https://doi.org/10.1177/1475240910370813>

Madden, T. J., Ellen, P. S., & Ajzen, I. (1992). A Comparison of the theory of planned behavior and the theory of reasoned action. *Personality and Social Psychology Bulletin*, 18(1), 3–9. <https://doi.org/10.1177/0146167292181001>

- Madnick, S. E., & Mangelsdorf, M. E. (2017). What executives get wrong about cybersecurity. *MIT Sloan Management Review*, 58(2), 22–24.
<https://sloanreview.mit.edu/article/what-executives-get-wrong-about-cybersecurity/>
- Mäenpää, H. (2021). *Augmented reality value creation: A conceptual framework for augmented reality social media advergames*. Master's dissertation, Tampere University.
<https://doi.org/10.13140/RG.2.2.15549.59369>
- Mahendru, P. (2024, July 30). *The state of ransomware in healthcare 2024*. Sophos News.
<https://news.sophos.com/en-us/2024/07/30/the-state-of-ransomware-in-healthcare-2024/>
 (Accessed 12 September 2024).
- Mahlaka, R. (2020, August 23). *Experian offers mea culpa after massive data breach blunder*. Daily Maverick. <https://www.dailymaverick.co.za/article/2020-08-23-experian-offers-mea-culpa-after-massive-data-breach-blunder/> (Accessed 21 September 2020).
- Malakhov, K.S. (2023). Insight into the digital health system of Ukraine (ehealth): Trends, definitions, standards, and legislative revisions. *International Journal of Telerehabilitation*. 15(2), e6599. <https://doi.org/10.5195/ijt.2023.6599>.
- Malmedal, B., & Roislien, H. E. (2016). *The Norwegian cybersecurity culture*. Norwegian Centre for Information Security (NorSIS). <https://norsis.no/publikasjoner> (Accessed 28 October 2021).
- Malyuk, A., & Miloslavskaya, N. (2016). Cybersecurity culture as an element of IT professional training. In *Proceedings of the 3rd International Conference on Digital Information Processing, Data Mining, and Wireless Communications, DIPDMWC 2016*, Moscow, Russia, 205–210. <https://doi.org/10.1109/DIPDMWC.2016.7529390>
- Mandava, M., Lubamba, C., Ismail, A., Bagula, A., & Bagula, H. (2016). Cyber-healthcare for public healthcare in the developing world. In *Proceedings of the IEEE Symposium on Computers and Communications, ISCC 2016*, Messina, Italy. 14–19.
<https://doi.org/10.1109/ISCC.2016.7543707>
- Mandl, K. D., & Kohane, I. S. (2008). Tectonic shifts in the health information economy. *New England Journal of Medicine*, 358(16), 1732–1737.
<https://doi.org/10.1056/NEJMs0800220>

Mansfield-Devine, S. (2016). Hospitals become major target for ransomware. *Network Security*, 2016(4), 1–2. [https://doi.org/10.1016/s1353-4858\(16\)30031-9](https://doi.org/10.1016/s1353-4858(16)30031-9)

Marotta, A., & Pearlson, K. (2019). A culture of cybersecurity at Banca popolare di sondrio. In *Proceedings of the 25th Americas Conference on Information Systems*, AMCIS 2019, Cancun, Mexico, 1–10.

Marshall, M. (1996). Sampling for qualitative research. *Family Practice*, 13(6), 522–526. <https://doi.org/10.1093/fampra/13.6.522>

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *The British Medical Journal (BMJ)*, 358, 3179. <https://doi.org/10.1136/bmj.j3179>

Masethe, H., Olugbara, O., Ojo, S., & Adewumi, A. (2013). Integration of health data using enterprise service bus. In *Proceedings of the World Congress on Engineering and Computer Science WCECS 2013 Vol II*, San Francisco, USA, 839–843

Mason, M. (2010). Sample size and saturation in PhD studies using qualitative interviews. *Forum: Qualitative Social Research*, 11(3). <https://doi.org/10.17169/fqs-11.3.1428>

Massaro, M., Dumay, J., & Guthrie, J. (2016). On the shoulders of giants: Undertaking a structured literature review in accounting. *Accounting, Auditing and Accountability Journal*, 29(5), 767–801. <https://doi.org/10.1108/AAAJ-01-2015-1939>

Massoudi, B., Holvast, F., Bockting, C. L. H., Burger, H., & Blanker, M. H. (2019). The effectiveness and cost-effectiveness of e-health interventions for depression and anxiety in primary care: A systematic review and meta-analysis. *Journal of Affective Disorders*, 245, 728–743. <https://doi.org/10.1016/j.jad.2018.11.050>

Mbacop, T. L., De La Cruz, E., Nadella, G. S., Le, H., De La Cruz, A. M., & Oni, O. (2025). Exploring cybersecurity challenges, strategies, and implications in healthcare: A qualitative study. In *Proceedings of the 2025 IEEE Integrated STEM Education Conference (ISEC)*, 1–7. <https://doi.org/10.1109/ISEC64801.2025.11147260>

- McConnell J. (1994). *National training standard for information systems security (INFOSEC) professionals, NSTISS no 4011*. National Security Telecommunications and Information Systems Security committee. <https://www.sait.fsu.edu/resources/NSTISSI-4011.pdf> (Accessed 3 July 2021).
- McGinn, C. A., Grenier, S., Duplantie, J., Shaw, N., Sicotte, C., Mathieu, L., Leduc, Y., Légaré, F., & Gagnon, M. P. (2011). Comparison of user groups' perspectives of barriers and facilitators to implementing electronic health records: A systematic review. *BMC Medicine*, 9, 46. <https://doi.org/10.1186/1741-7015-9-46>
- McLaren, T. S., Head, M. M., Yuan, Y., & Chan, Y. (2011). A multilevel model for measuring fit between a firm's competitive strategies and information systems capabilities. *MIS Quarterly*, 35(4), 909–929. <https://doi.org/10.2307/41409966>
- Mc Loughlin, J. (2024, November 15). *Top industries facing cyber threats*. ITWeb. <https://www.itweb.co.za/article/top-industries-facing-cyber-threats/KA3WwMdZ84XvrydZ> (Accessed 10 May 2025).
- McNiff, J., & Whitehead, J. (2002). *Action research: Principles and practice*. Routledge.
- Mello, J. P. (2017, April 6). *Healthcare security \$65 billion market*. Cybersecurity Ventures. <https://cybersecurityventures.com/healthcare-cybersecurity-report-2017/> (Accessed 10 August 2020).
- Menachemi, N., Burke, D., Diana, M., & Brooks, R. (2005). Characteristics of hospitals that outsource information system functions. *Journal Health Information Management*, 19(1), 63–69. <https://pubmed.ncbi.nlm.nih.gov/15682678/>
- Merilampi, S., & Sirkka, A. (2016) (Eds.). *Introduction to smart ehealth and care technologies*. CRC Press, Taylor & Francis Group. <https://doi.org/10.1201/9781315368818>
- Metalidou, E., Mairangi, C., Trivelle's, P., Eberhagen, N., Skouras, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia - Social and Behavioural Sciences*, 147, 424–428. <https://doi.org/10.1016/j.sbspro.2014.07.133>

- Mihoub, A., Fred, O. B., Chihuahua, O., Derham, A., & Kirchen, M. (2022). Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques. *Computers & Electrical Engineering*, 98, 107716. <https://doi.org/10.1016/j.compeleceng.2022.107716>
- Miles, M., Huberman, A., & Saldana, J. (2019). *Qualitative data analysis. A methods sourcebook* (4th ed.). Sage publications.
- Mills, R. R. (2018). *The current state of insider threat awareness and readiness in corporate cybersecurity - an analysis of definitions, prevention, detection and mitigation*. Master's dissertation, Utica College, ProQuest Dissertations & Theses. 10750085.
- Mitrovic, Z., Thakur, C., & Palhad, S. (2023). Towards building cybersecurity culture in TVET colleges in South Africa. In *Proceedings of the 2023 IST-Africa Conference, IST-Africa 2023*, 1–10. <https://doi.org/10.23919/IST-Africa60249.2023.10187852>
- Mohd Rohani, J., Mohd Yusof, S., & Mohamad, I. (2009). The relationship between statistical process control critical success factors and performance: A structural equation modelling approach. In *Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management, IEEM 2009*, Hong Kong, 1352–1356. <https://doi.org/10.1109/IEEM.2009.5373033>
- Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G., PRISMA Group, P. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *Annals of Internal Medicine*, 151(4), 264–270. <https://doi.org/10.7326/0003-4819-151-4-200908180-00135>
- Moonsamy, A., Ahmed, M. (2023). Developing a comprehensive risk management framework for e-health care delivery. In *Li, Y., Huang, Z., Sharma, M., Chen, L., Zhou, R. (Eds.), Health Information Science*. (Lecture Notes in Computer Science, vol 14305, 113 - 123). Springer. https://doi.org/10.1007/978-981-99-7108-4_9
- Morgan, D. L. (2007). Paradigms lost and pragmatism regained: methodological implications of combining qualitative and quantitative methods. *Journal of Mixed Methods Research*, 1(1), 48–76. <https://doi.org/10.1177/2345678906292462>

Morgan, S. (2020a, September 8). *Healthcare industry to spend \$125 billion on cybersecurity from 2020 to 2025*. Cybersecurity Ventures. <https://cybersecurityventures.com/healthcare-industry-to-spend-125-billion-on-cybersecurity-from-2020-to-2025/> (Accessed 25 January 2022).

Morgan, S. (2020b). *The 2020-2021 healthcare cybersecurity report*. <https://cybersecurityventures.com/wp-content/uploads/2020/09/HG-Healthcare-Cybersecurity-Report-2021.pdf> (Accessed 6 October 2020).

Morse, J. M. (1995). The significance of saturation. *Qualitative Health Research*, 5(2), 147–149. <https://doi.org/10.1177/104973239500500201>

Mostafa, R., Rahman, G. M. A. E., Hasan, G. M., Kabir, A., & Rahman, A. (2010). Proposed deployments to provide e-healthcare in Bangladesh: Urban and rural perspectives. In *Proceedings of the 12th IEEE International Conference on E-Health Networking, Application and Services*, Lyon, France, 361–366. <https://doi.org/10.1109/HEALTH.2010.5556542>

Moxey, A., Robertson, J., Newby, D., Hains, I., Williamson, M., & Pearson, S. A. (2010). Computerized clinical decision support for prescribing: Provision does not guarantee uptake. *Journal of the American Medical Informatics Association*, 17(1), 25–33. <https://doi.org/10.1197/jamia.M3170>

Moyo, A. (2018, July 12). *SA's average data breach costs escalate*. ITWeb. <https://www.itweb.co.za/content/Per037ZgOnXMQb6m/> (Accessed November 2020).

Moyo, A. (2021, September 10). *Justice department battles to contain ransomware attack*. IT Web. <https://www.itweb.co.za/article/justice-department-battles-to-contain-ransomware-attack/DZQ58vVPOB1MzXy2> (Accessed 12 September 2024).

Moyo, A. (2022, March 17). *Breaking: Credit bureau TransUnion hacked*. ITWeb. <https://www.itweb.co.za/content/o1Jr5Mx9BVjqKdWL> (Accessed 12 September 2024).

Moyo, A. (2024, May 24). *Justice department suffers another cyber-attack*. IT Web. <https://www.itweb.co.za/article/justice-department-suffers-another-cyber-attack/rW1xLv5nJkx7Rk6m> (Accessed 12 September 2024).

Mugo, D., & Nzuki, D. (2014). Determinants of electronic health in developing countries. *International Journal of Arts and Commerce*, 3(3), 49–60.

Mungadze, S. (2020, January 9). *Life Healthcare Group hit by cyber attack amid COVID-19*. ITWeb, 19–22. <https://www.itweb.co.za/article/life-Healthcare-group-hit-by-cyber-attack-amid-covid-19/JBwErVnBK4av6Db2/>. (Accessed February 2021).

Munyaradzi, Z. (2018). *A mobile health framework for improving maternity care nurses' work processes*. Doctoral dissertation, University of South Africa.

Munyisia, E. N., Yu, P., & Hailey, D. (2011). Does the introduction of an electronic nursing documentation system in a nursing home reduce time on documentation for the nursing staff? *International Journal of Medical Informatics*, 80(11), 782–792. <https://doi.org/10.1016/j.ijmedinf.2011.08.009>

Murphy, S. (2015). *Healthcare Information Security and Privacy*. McGraw - Hill Education Group.

Mustaca, S. (2014). Are your IT professionals prepared for the challenges to come? *Computer Fraud and Security*, 2014(3), 18–20. [https://doi.org/10.1016/S1361-3723\(14\)70472-5](https://doi.org/10.1016/S1361-3723(14)70472-5)

Mwim, E., & Mtsweni, J. (2022). Systematic review of factors that influence the cybersecurity culture. In *Proceedings of the International Symposium on Human Aspects of Information Security and Assurance*, HAISA 2022, 147–172. https://doi.org/10.1007/978-3-031-12172-2_12

Mzekandaba, S. (2024, February 22). *Data breaches rising at alarming rate, says InfoReg*. ITweb. <https://www.itweb.co.za/article/data-breaches-rising-at-alarming-rate-says-infoereg/wbrpOqg2pXZMDLZn> (Accessed 24 September 2024).

Narad (2024, October 30) *The singHealth data breach: Lessons in compliance and cybersecurity*. Narad. <https://narad.io/blog/the-singhealth-data-breach-lessons-in-compliance-and-cybersecurity/> (Accessed 4 November 2024).

National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity Version 1.0*. NIST Cybersecurity Framework (CSF). Testimony of National Institute of Standards and Technology.

<https://doi.org/10.6028/NIST.CSWP.04162018>

Newman, L. H. (2017, March 2). *Medical devices are the next security nightmare*. WIRED, March 2017. <https://www.wired.com/2017/03/medical-devices-next-security-nightmare/> (Accessed May 2022).

Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A.Z., & Nikpay, S. S. (2022). Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. *JAMA Health Forum*, 3(12), e224873-e224873. <https://doi.org/10.1001/jamahealthforum.2022.4873>

Noble, H., & Heale, R. (2019). Triangulation in research, with examples. *Evidence-Based Nursing*, 22(3), 67–68. <https://doi.org/10.1136/ebnurs-2019-103145>

Norman, C. D., & Skinner, H. A. (2006). eHEALS: The eHealth literacy scale. *Journal of Medical Internet Research*, 8(4), e507. <https://doi.org/10.2196/jmir.8.4.e27>

O'Reilly, K. (2009). Inductive and deductive. In *Key Concepts in Ethnography*. SAGE Publications. 104–109. <https://doi.org/10.4135/9781446268308>

Oates, J. B. (2006). *Researching information systems and computing*. SAGE Publications.

Oates, B. J., Griffiths, M., & McLean, R. (2022). *Researching information systems and computing* (2nd ed.). SAGE Publications.

Ocloo, C. M., Da Veiga, A., & Kroeze, J. (2021). A conceptual information security culture framework for higher learning institutions. In *IFIP Advances in Information and Communication Technology, HAISA 2021*, 613, 63–80. https://doi.org/10.1007/978-3-030-81111-2_6

Offermann, P., Levina, O., Schönherr, M., & Bub, U. (2009). Outline of a design science research process. In *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, DESRIST 2009, 1-11 <https://doi.org/10.1145/1555619.1555629>

Ogden, S. (2021). *Cybersecurity: Creating a cybersecurity culture*. Master's dissertation, California State University - San Bernardino.

Oh, H., Rizo, C., Enkin, M., & Jadad, A. (2005). What is eHealth: A systematic review of published definitions. *World Hospitals and Health Services*, 41(1), 32–40.

<https://doi.org/10.2196/jmir.7.1.e1>

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of Information Systems research. *Sprouts: Working Papers on Information Systems*, 10(26).

Oladipo, J. O., Okoye, C. C., Elufioye, O. A., Falaiye, T., & Nwankwo, E. E. (2024). Human factors in cybersecurity: Navigating the fintech landscape. *International Journal of Science and Research Archive*, 11(1), 1959-1967. <https://doi.org/10.30574/ijjsra.2024.11.1.0258>

Oluoch, T., Santas, X., Kwaro, D., Were, M., Biondich, P., Bailey, C., Abu-Hanna, A., & de Keizer, N. (2012). The effect of electronic medical record-based clinical decision support on HIV care in resource-constrained settings: A systematic review. *International Journal of Medical Informatics*, 81(10), e83–e92. <https://doi.org/10.1016/j.ijmedinf.2012.07.010>

Omran, E., Grandison, T., & Al Sharhan, S. (2015). Leveraging cloud services to spark innovation, privacy and security in Kuwait hospitals. In *Proceedings of the 5th International Conference on Digital Information Processing and Communications, ICDIPC 2015*, Sierre, Switzerland, 65–70. <http://dx.doi.org/10.1787/9789264245471-en>

Organisation for Economic Co-operation and Development (OECD). (2005). *The promotion of a culture of security for information systems and networks in OECD countries*. DSTI / ICCP / REG (2005) 1 / FINAL. OECD
<https://one.oecd.org/document/DSTI/ICCP/REG%282005%291/FINAL/en/pdf> (Accessed 08 January 2021).

Organisation for Economic Co-operation and Development OECD). (2015). *Digital security risk management for economic and social prosperity: OECD recommendation and companion document*. <https://doi.org/DOI>: <http://dx.doi.org/10.1787/9789264245471-en>

Organisation for Economic Co-operation and Development (OECD). (2021). *OECD, Recommendation of the council concerning guidelines for the security of information systems and networks - Towards a culture of security* OECD/LEGAL/0312.

<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0312> (Accessed 10 February 2024).

Osunyomi, B. D., & Grobbelaar, S. S. (2015). Integrating eHealth in HIV/AIDS intervention programmes in South Africa. *SA Journal of Information Management*, 17(1), 1–10.

<https://doi.org/10.4102/sajim.v17i1.623>

Padayachee, K. (2011). Teaching safe and secure usage of ICT: A South African perspective. In *Proceedings of the 2nd International Conference on Society and Information Technologies* (ICSIT 2011), Orlando, USA

Pagliari, C., Sloan, D., Gregor, P., Sullivan, F., Detmer, D., Kahan, J. P., Oortwijn, W., & MacGillivray, S. (2005). What is eHealth (4): A scoping exercise to map the field. *Journal of Medical Internet Research*, 7(1), 1–20. <https://doi.org/10.2196/jmir.7.1.e9>

Pallant, J. (2020). *SPSS survival manual a step by step guide to data analysis using IBM SPSS* (7th ed.). McGraw - Hill Education, Open University Press.

Park, W. S., Seo, S. W., Son, S. S., Lee, M. J., Kim, S. H., Choi, E. M., Bang, J. E., Kim, Y. E., & Kim, O. N. (2010). Analysis of information security management systems at 5 domestic hospitals with more than 500 beds. *Healthcare Informatics Research*, 16(2), 89–99.

<https://doi.org/10.4258/hir.2010.16.2.89>

Passonneau, S., & Coffey, D. (2011). The role of synchronous virtual reference in teaching and learning: A grounded theory analysis of instant messaging transcripts. *College & Research Libraries*, 72(3), 276–295. <https://doi.org/10.5860/crl-102rl>

Pătrascu, P. (2019). Promoting cybersecurity culture through education. In *Proceedings of the 15th International Scientific Conference on eLearning and Software for Education*, 273–279. <https://doi.org/10.12753/2066-026X-19-108>

Patton, M. Q. (1999). Enhancing the quality and credibility of qualitative analysis. *Health Services Research*, 34(5 Pt 2), 1189–1208.

<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1089059/>

Patton, M. Q. (1990). *Qualitative research and evaluation methods* (2nd ed.). SAGE Publications.

Paul, C., & Porche, I. R. (2011). Toward a U.S. army cybersecurity culture. *International Journal of Cyber Warfare and Terrorism*, 1(3), 70–80.
<https://doi.org/10.4018/ijcwt.2011070105>

Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). *A capability maturity model for software* (Version 1.1). (Technical Report CMU/SEI-93-TR-024).
<https://insights.sei.cmu.edu/library/capability-maturity-model-for-software-version-11/>.
(Accessed 5 December 2024).

Paulsen, C., & Byers, R. (2019). *Glossary of Key Information Security Terms*. NIST, Vol. NISTIR 729 (Issue Rev 3). <https://doi.org/10.6028/NIST.IR.7298r3>

Pavlova, E. (2020). Enhancing the organisational culture related to cybersecurity during the university digital transformation. *Journal of Information & Security*, 46(3), 239–249.
<https://doi.org/10.11610/isij.4617>

Pawson, R., Barnes, C., Boaz, A., Grayson, L., & Long, A. (2003). *Types and quality of social care knowledge. Stage two: towards the quality assessment of social care knowledge*. ESRC UK Center for Evidence Based Policy and Practice, Working Paper, 18.

Peffers, K., Rothenberger, M., Tuunanen, T., Vaezi, R. (2012). Design science research evaluation. In Peffers, K., Rothenberger, M., Kuechler, B. (Eds.) *Design science research in Information Systems: Advances in theory and practice*. DESRIST 2012. Lecture Notes in Computer Science, 7286. 398 – 410. Springer, Berlin, Heidelberg.
https://doi.org/10.1007/978-3-642-29863-9_29

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2014). A design science research methodology for Information Systems research. *Journal of Management Information Systems*, 24(3), 45–77. <https://doi.org/10.2753/MIS0742-1222240302>

Perakslis, E. D. (2014). Cybersecurity in health care. *New England Journal of Medicine*, 371(5), 395–397. <https://doi.org/10.1056/NEJMp1404358>

- Perez, H., Neubauer, N., Marshall, S., Philip, S., Miguel-Cruz, A., & Liu, L. (2022). Barriers and benefits of information communication technologies used by health care aides. *Applied Clinical Informatics*, 13(01), 270–286. <https://doi.org/10.1055/s-0042-1743238>
- Perednia, D. A., & Brown, N. A. (1995). Teledermatology: One application of telemedicine. *Bulletin of the Medical Library Association*, 83(1), 42–47.
- Petersen, M. J., Baune, D. A., Huggins, I. G., & LaMarche, D. J. (1996). Telemedicine in Utah: The rural Utah telemedicine pilot project. In *Proceeding of the Technology-Based Re-Engineering Engineering Education: Frontiers in Education, FIE'96 26th Annual Conference*, Salt Lake City, UT, USA. Vol. 2, 986–989. <https://doi.org/10.1109/FIE.1996.573152>
- Petracca, F., Ciani, O., Cucciniello, M., & Tarricone, R. (2020). Harnessing digital health technologies during and after the COVID-19 pandemic: context matters. *Journal of Medical Internet Research*, 22(12), e21815. <https://doi.org/10.2196/21815>
- Petticrew, M., & Roberts, H. (2006). *Systematic reviews in the social sciences: a practical guide*. Blackwell Pub.
- Pfleeger, C. P., Lawrence Pfleeger, S., & Margulies, J. (2015). *Security in Computing* (5th ed.). Pearson Education.
- Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cybersecurity risk. *Computers and Security*, 31(4), 597–611. <https://doi.org/10.1016/j.cose.2011.12.010>
- PharMerica. (2023). *PharMerica notifies individuals of privacy incident*. PharMerica. <https://pharmerica.com/data-privacy-incident/> (Accessed 12 September 2024).
- Phillips, R., & Tanner, B. (2019). Breaking down silos between business continuity and cybersecurity. *Journal of Business Continuity & Emergency Planning*, 12(3), 224–232. <https://doi.org/10.69554/nmcv5299>
- Pickvance, C. G. (2001). Four varieties of comparative analysis. *Journal of Housing and the Built Environment*, 16(1), 7–28. <https://doi.org/10.1023/A:1011533211521>

Pilieci, V. (2016, March 14). *Ottawa Hospital hit with ransomware, information on four computers locked down*. Ottawa Citizen. <https://ottawacitizen.com/news/local-news/ottawa-hospital-hit-with-ransomware-information-on-four-computers-locked-down> (Accessed 8 July 2020).

Pimentel, J. L. (2010). A note on the usage of Likert scaling for research data analysis. *USM R&D Journal*, 18(2), 109-112.

Pimentel, J. L. (2019). Some biases in Likert scaling usage and its correction. *International Journal of Sciences: Basic and Applied Research*, 45(1), 183–191.
<https://www.gssrr.org/index.php/JournalOfBasicAndApplied/article/view/9874>

Police, R. L., Foster, T., & Wong, K. S. (2011). Adoption and use of health information technology in physician practice organisations: Systematic review. *Journal of Innovation in Health Informatics*, 18(4), 245–258. <https://doi.org/10.14236/jhi.v18i4.780>

Polit, D. F., & Beck, C. T. (2008). *Nursing research: Generating and assessing evidence for nursing practice* (8th ed.). Lippincott Wilkins & Wilkins.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology and Work*, 24(2), 371–390. <https://doi.org/10.1007/s10111-021-00683-y>

Ponemon Institute. (2016). Sixth annual benchmark study on privacy and security of healthcare data. *Ponemon Institute LLC*.
<https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf> (Accessed 01 July 2022).

Ponemon Institute. (2017). The rise of ransomware. In *Ponemon Institute LLC*.
<https://www.ponemon.org/local/upload/file/Ransomware%20Report%20Final%201.pdf>
(Accessed 11 July 2024).

Ponemon Institute. (2018). *The 2018 cost of data breach study: Global overview*.
<https://corridorinteractive.com/wp-content/uploads/2019/09/Poneman-Institute-2018-Global-Cost-of-a-Data-Breach-Report.pdf> (Accessed 20 July 2021).

Popescu, C., El-Chaarani, H., El-Abiad, Z., & Gigauri, I. (2022). Implementation of health information systems to improve patient identification. *International Journal of Environmental Research and Public Health*, 19(22), 15236.

<https://doi.org/10.3390/ijerph192215236>

Rachel, G. (2019, March 30). *West Michigan doctor's office hacked, doctors held for ransom*. WWMT West Michigan. <https://wwmt.com/news/local/west-michigan-doctors-office-hacked-doctors-held-for-ransom> (Accessed 9 July 2022).

Ragnedda, M., & Muschert, G. W. (Eds.) (2013). *The digital divide: The Internet and social inequality in international perspective*. <https://doi.org/10.4324/9780203069769>

Rambaree, K. (2018). Abductive thematic network analysis (ATNA) using ATLAS-ti. In *Innovative research methodologies in management: Volume I. Philosophy, measurement and modelling*. https://doi.org/10.1007/978-3-319-64394-6_4

Ramluckan, T., van Niekerk, B., & Martins, I. (2020). A change management perspective to implementing a cybersecurity culture. In *Proceedings of the 20th European Conference on Information Warfare and Security*, ECCWS 2020, 442–448.

Randolph, A. G., Haynes, R. B., Wyatt, J. C., Cook, D. J., & Guyatt, G. H. (1999). Users' guides to the medical literature XVIII. How to use an article evaluating the clinical impact of a computer-based clinical decision support system. *Journal of the American Medical Association (JAMA)*, 282(1), 67–74. <https://doi.org/10.1001/jama.282.1.67>

Reegård, K., Blackett, C., & Katta, V. (2019). The concept of cybersecurity culture. In *Proceeding of the 29th European Safety and Reliability Conference, ESREL 2019*, Hannover, Germany, 4036–4043. <https://doi.org/10.3850/978-981-11-2724-3>

Reid, R., & van Niekerk, J. (2014a). From information security to cybersecurity cultures: In *Proceedings of the Information Security for South Africa, ISSA 2014*, 1–7. <https://doi.org/10.1109/ISSA.2014.6950492>

Reid, R., & van Niekerk, J. (2014b). Towards an education campaign for fostering a societal, cybersecurity culture. In *Proceedings of the 8th International Symposium on Human Aspects of Information Security & Assurance, HAISA 2014*, 174–184.

Rengamani, H., Upadhyaya, S., Rao, H. R., & Kumaraguru, P. (2010). Protecting senior citizens from cybersecurity attacks in the E-Health scenario: An international perspective. In *Proceedings of the 6th Annual Workshop on Cybersecurity and Information Intelligence Research* (CSIIRW 2010). Association for Computing Machinery, NY, USA, Article 82, 1–4 <https://doi.org/10.1145/1852666.1852759>

Republic of Uganda. (2011). *National information security strategy (NISS Final Draft)*. Ministry of Information and Communications Technology, Kampala. <https://www.cert.ug/sites/default/files/2022-05/National%20Information%20Security%20Strategy%202011.pdf> (Accessed 13 November 2024).

Republic of Uganda. (2022). *National Cybersecurity Strategy (2022 – 2026)*. National Information Technology Authority Uganda. <https://www.nita.go.ug/sites/default/files/2024-02/National%20Cybersecurity%20Strategy-UG.pdf> (Accessed 5 December 2024).

Reuters (2020, June 9). *Life Healthcare hit by cyber attack*. SABC News. <https://www.sabcnews.com/sabcnews/life-Healthcare-hit-by-cyber-attack/> (Accessed 22 September 2020).

Riazul Islam, M., Daehan, K., Humaun K. M., Hossain, M., Kyung-Sup, K. (2015). The internet of things for health care: A comprehensive survey. *IEEE Access*, 3, 678–708. <https://doi.org/10.1109/ACCESS.2015.2437951>

Ribeiro, L. G. (2019). *Understanding phishing mitigation strategies in the U.S. Federal Government: A qualitative multiple descriptive case study*. Doctoral dissertation, Capella University.

Richards, L., & Morse, J. M. (2013). *Readme first: A user's guide to qualitative methods* (3rd ed.). SAGE Publications.

Riddell, W. C., & Song, X. (2017). The role of education in technology use and adoption: Evidence from the Canadian workplace and employee survey. *ILR Review*, 70(5), 1219–1253. <https://doi.org/10.1177/0019793916687719>

Rinchi. (2019, January 27). *How to create cybersecurity culture according to an SMS scheduling feature*. TECHINAFRICA. <https://www.techinafrica.com/create-cyber-security-culture-according-professional/> (Accessed 11 June 2021).

Robbins, T. D., Lim Choi Keung, S. N., & Arvanitis, T. N. (2018). E-Health for active ageing: A systematic review. *Maturitas*, 114, 34–40. <https://doi.org/10.1016/j.maturitas.2018.05.008>

Robinson, E. (2008). *E-Health and the Internet: Factors that influence doctors' mediation behaviors with patients*. Master's dissertation, Georgia State University.

Robson, C. (2002). *Real world research* (2nd ed.). Oxford: Blackwell.

Roehl, S. (n.d.). *What is open coding in qualitative research?* ATLAS.Ti. <https://atlasti.com/research-hub/open-coding> (Accessed 3 January 2024).

Rojas-Mendizabal, V. A., Serrano-santoyo, A., Conte-galvan, R., & Gomez-gonzalez, A. (2013). Toward a model for quality of experience and quality of service in e-health ecosystems. *Procedia Technology*, 9, 968–974. <https://doi.org/10.1016/j.protcy.2013.12.108>

Ron, C. (2008). Peer Review. In L. M. Given (Ed.), *The SAGE encyclopaedia of qualitative research methods*. (Vol 1.0). SAGE Publications, Inc. <https://doi.org/10.4135/9781412963909>

Ross, J., Stevenson, F., Lau, R., & Murray, E. (2015). Exploring the challenges of implementing E-Health: A protocol for an update of a systematic review of reviews. *The British Medical Journal (BMJ) Open*, 5(4), 1–5. <https://doi.org/10.1136/bmjopen-2014-006773>

Ross, J., Stevenson, F., Lau, R., & Murray, E. (2016). Factors that influence the implementation of E-Health: A systematic review of systematic reviews (an update). *Implementation Science*, 11(146). <https://doi.org/10.1186/s13012-016-0510-7>

Rout, D. (2015). Developing a common understanding of cybersecurity. *ISACA Journal*, 6, 1–4. <https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/developing-a-common-understanding-of-cybersecurity> (Accessed 06 February 2025).

- Rylander, A. (2012). Pragmatism and design research: An overview. In *Ingår i Designfakultetens serie kunskapssammanställningar*. Royal Institute of Technology, Stockholm, Sweden. https://www.researchgate.net/profile/Anna-Rylander-Eklund/publication/379294969_Pragmatism_and_Design_Research_-_An_Overview/links/6602eafb8be8c8003bb88b8d/Pragmatism-and-Design-Research-An-Overview.pdf (Accessed 22 May 2019).
- Saigushev, N. Y., Vedeneeva, O. A., Melekhova, Y. B., & Tsaran, A. A. (2020). Cooperation of future automated machinery specialists in informational context as a means of communication during vocational training process. *IOP Conference Series: Materials Science and Engineering*, 843(1), 012002. <https://doi.org/10.1088/1757-899X/843/1/012002>
- Salah, D., Paige, R., & Cairns, P. (2014). An evaluation template for expert review of maturity models. In *Product-Focused Software Process Improvement PROFES 2014. Lecture Notes in Computer Science*, 8892, Cham. 318–321. https://doi.org/10.1007/978-3-319-13835-0_31
- Salama, R., Altrjman, C., & Al-Turjman, F. (2024). Healthcare cybersecurity challenges: a look at current and future trends. In *Al-Turjman (Eds.). Computational Intelligence and Blockchain in Complex Systems*. 97–111. <https://doi.org/https://doi.org/10.1016/B978-0-443-13268-1.00003-0>
- Salge, T. O., Kohli, R., & Barrett, M. (2015). Investing in information systems: On the behavioral and institutional search mechanisms underpinning hospitals' IS investment decisions. *MIS Quarterly*, 39(1), 61–89. <https://doi.org/10.25300/misq/2015/39.1.04>
- Saliba, V., Legido-Quigley, H., Hallik, R., Aaviksoo, A., Car, J., & McKee, M. (2012). Telemedicine across borders: A systematic review of factors that hinder or support implementation. *International Journal of Medical Informatics*, 81(12), 793–809. <https://doi.org/10.1016/j.ijmedinf.2012.08.003>
- Saritac, U., Liu, X., & Wang, R. (2022). Assessment of cybersecurity framework in critical infrastructures. In *Proceeding of the IEEE Delhi Section Conference, DELCON 2022*, 1–4. <https://doi.org/10.1109/DELCON54057.2022.9753250>

- Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality and Quantity*, 52(4), 1893–1907. <https://doi.org/10.1007/s11135-017-0574-8>
- Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students* (7th ed.). Harlow, Pearson Education limited.
- Sendelj, R., & Ognjanovic, I. (2022). Cybersecurity challenges in healthcare. *Health Technology and Informatics*, 300, 190–202. <https://doi.org/10.3233/SHTI220951>
- Seng, N. (2023). Cybersecurity incident reporting laws in the Asia Pacific. *International Cybersecurity Law Review*, 4, 325–346. <https://doi.org/10.1365/s43439-023-00088-9>
- Seyedin, H., Moghimi, M., Goharinezhad, S., Azmal, M., & Kalhor, R. (2024). The hospital cost reduction strategies from the managers' point of view: A qualitative study in Iran. *Health Scope*, 13(1), E137620. <https://doi.org/10.5812/healthscope-137620>
- Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition cybersecurity. *Journal of Digital Forensics, Security and Law*, 12(2). <https://doi.org/10.15394/jdfsl.2017.1476>
- Schein, E. (2004). Organizational culture and leadership. In *The Academy of Management Review* (3rd ed.). Jossey-Bass.
- Schein, E. (2009). *The corporate culture survival guide* (2nd ed.). John Wiley and Sons Inc.
- Schein, E. (2010). Organizational culture and leadership. In *EBL* (4th ed.). Jossey-Bass.
- Schlienger, T., & Teufel, S. (2002). Information security culture: The socio-cultural dimension in information security management. In M. A. Ghonaimy, M. T. El-Hadidi, & H. K. Aslan (Eds.), *Security in the information society: vision and perspective*. IFIP TC11 International Conference on Information Security, 191–201. https://doi.org/10.1007/978-0-387-35586-3_15
- Schlienger, T., & Teufel, S. (2003). Information security culture: From analysis to change. *South African Computer Journal*, 2003(31), 46–52. <https://hdl.handle.net/10520/EJC27949>

- Schwartz, J. M. (2016, February 16). *Ransomware hits hospitals*. Bank Info Security. <https://www.bankinfosecurity.com/ransomware-hits-hospitals-a-8872> (Accessed 8 July 2020).
- Scott, J. (2015). Cybersecurity hygiene for the healthcare industry: The basics in healthcare IT, health informatics and cybersecurity for the health sector (Vol. 4). CreateSpace Independent Publishing Platform. ISBN 9781519254597
- Shahri, A. B., Ismail, Z., & Rahim, N. Z. A. (2013). Security culture and security awareness as the basic factors for security effectiveness in health information systems. *Journal Teknologi (Sciences and Engineering)*, 64(2), 7–12. <https://doi.org/10.11113/jt.v64.2212>
- Shenoy, A., & Appel, J. M. (2017). Safeguarding confidentiality in electronic health records. *Cambridge Quarterly of Healthcare Ethics*, 26(2), 337–341. <https://doi.org/10.1017/S0963180116000931>
- Shorten, A., & Smith, J. (2017). Mixed methods research: Expanding the evidence base. *Evidence-Based Nursing*, 20(3), 74–75. <https://doi.org/10.1136/eb-2017-102699>
- Siponen, M., Mahmood, M. A., & Pahlila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2), 217–224. <https://doi.org/10.1016/j.im.2013.08.006>
- Siwicki, B. (2016, May 23). *Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money*. HealthcareITNews. <https://cloudgate.healthcareitnews.com/news/ransomware-attackers-collect-ransom-kansas-hospital-dont-unlock-all-data-then-demand-more> (Accessed 10 August 2023).
- Smart, W. (2018). *Lessons learned review of the WannaCry ransomware cyber attack*. Crown. NHS England. <https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf> (Accessed 8 July 2020).
- Smet, M. (2002). Cost characteristics of hospitals. *Social Science & Medicine*, 55(6), 895–906. [https://doi.org/10.1016/s0277-9536\(01\)00237-4](https://doi.org/10.1016/s0277-9536(01)00237-4)

Snilstveit, B., Oliver, S., & Vojtkova, M. (2012). Narrative approaches to systematic review and synthesis of evidence for international development policy and practice. *Journal of Development Effectiveness*, 4(3), 409–429. <https://doi.org/10.1080/19439342.2012.710641>

Snowdon, A. (2020). *Four areas of digital health that are driving the future of healthcare*. HIMSS. <https://www.himss.org/resources/four-areas-digital-health-are-driving-future-Healthcare>. (Accessed 12 September 2022).

Sonnenberg, C., vom Brocke, J. (2012). Evaluations in the science of the artificial – reconsidering the build-evaluate pattern in design science research. In: Peffers, K., Rothenberger, M., Kuechler, B. (Eds.) *Design science research in Information Systems. Advances in theory and practice*. DESRIST 2012. Lecture Notes in Computer Science, 7286 LNCS, 381-397. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-29863-9_28

Sood, S., Mbarika, V., Jugoo, S., Dookhy, R., Doarn, C. R., Prakash, N., & Merrell, R. C. (2007). What is telemedicine? A collection of 104 peer-reviewed perspectives and theoretical underpinnings. *Telemedicine and E-Health*, 13(5), 573–590. <https://doi.org/10.1089/tmj.2006.0073>

Sousane, R. (2018). *Understanding federal cybersecurity culture: An expert perspective on current and ideal state*. Doctoral dissertation, The George Washington University, ProQuest Dissertations and Theses. 10785377

South Africa (2013). Protection of Personal Information Act No. 4 of 2013. *Government Gazette* no. 37067, https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf (Accessed 22 October 2023).

South Africa. (2017). Cybercrimes and Cybersecurity Bill (B6-2017). *Government Gazette* no. 40487, 1-88, Minister of Justice and Correctional Services. https://www.gov.za/sites/default/files/gcis_document/202012/bill-b6d-2017-cybercrimes-bill.pdf (Accessed 13 November 2024).

South Africa. (2020). Cybercrimes Act 2020 (Act no 19 of 2020). *Government Gazette* no. 44651, 1-127. https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf (Accessed 13 November 2024).

South African Nursing Council. (2022). *Provincial distribution of nursing manpower versus the population of the Republic of South Africa as at 31 December 2022*.
<https://www.sanc.co.za/wp-content/uploads/2023/01/Stats-2022-1-Provincial-Distribution.pdf>
(Accessed 4 November 2024).

Spence, N., Paul III, D., & Coustasse, A. (2017). Ransomware in healthcare facilities: The future is now. In *Proceedings of the Academy of Business Research Conference*, Fall 2017, Atlantic City, NJ, 1–14.
https://mds.marshall.edu/cgi/viewcontent.cgi?article=1185&context=mgmt_faculty
(Accessed 1 September 2020).

Stanley, T. D. (2001). Wheat from chaff: Meta-analysis as quantitative literature review. *Journal of Economic Perspectives*, 15(3), 131–150.
<https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.15.3.131>

State Security Agency. (2015). The National Cybersecurity Policy Framework (NCPF). *Government Gazette* Vol. 609, Issue 39475, 1-30.
http://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf (Accessed 02 June 2020).

Stellefson, M., Hanik, B., Chaney, B., Chaney, D., Tennant, B., & Chavarria, E. A. (2011). eHealth literacy among college students: A systematic review with implications for ehealth education. *Journal of Medical Internet Research*, 13(4), e102.
<https://doi.org/10.2196/jmir.1703>

Storm, D. (2015, June 8). MEDJACK: *Hackers hijacking medical devices to create backdoors in hospital networks*. Computerworld.
<https://www.computerworld.com/article/2932371/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html> (Accessed September 2021).

Storm, D. (2016, June 27). *Hacker selling 655,000 patient records from 3 hacked healthcare organizations*. Computerworld. <https://www.computerworld.com/article/3088907/hacker-selling-655-000-patient-records-from-3-hacked-healthcare-organizations.html> (Accessed 25 June 2020).

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research: grounded theory procedures and techniques*. Sage Publications.

Streiner, D. L. (2003). Starting at the Beginning: An Introduction to coefficient Alpha and internal consistency. *Journal of Personality Assessment*, 80(1), 99–103.

https://doi.org/10.1207/S15327752JPA8001_18

Stroetmann, K. A., Artmann, J., & Stroetmann, V. (2011). Developing national eHealth infrastructures—results and lessons from Europe. In *Proceedings of the AMIA Annual Symposium*, American Medical Informatics Association, Washington DC, 2011, 1347–1354. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3243126/>

Stubley, D. (2013, April 30). *What Is Cybersecurity?* *Security Boulevard*.

<https://securityboulevard.com/2013/04/what-is-cyber-security/?utm> (Accessed 1 September 2023).

Suri, H., & Clarke, D. (2009). Advancements in Research Synthesis Methods: From a Methodologically Inclusive Perspective. *Review of Educational Research*, 79(1), 395–430.

<https://doi.org/10.3102/0034654308326349>

Suter, E., Oelke, N. D., Adair, C. E., & Armitage, G. D. (2009). Ten key principles for successful health systems integration. *Healthcare Quarterly*, 13, 16–23.

<https://doi.org/10.12927/hcq.2009.21092>

Symantec. (2015, April). *Internet Security Threat Report. (Vol. 20)*. Broadcom.

<https://docs.broadcom.com/doc/istr-15-april-volume-20-en> (Accessed 10 May 2019).

Symantec. (2017, April). *Internet Security Threat Report. (Vol. 22)*. Broadcom.

<https://docs.broadcom.com/doc/istr-22-2017-en> (Accessed 10 June 2020).

Symantec. (2018a, March). *Executive Summary: 2018 Internet Security Threat Report. (Vol. 23)*. Broadcom. <https://docs.broadcom.com/doc/istr-23-executive-summary-en> (Accessed 15 April 2020).

Symantec. (2018b, March). *Internet Security Threat Report. (Vol. 23)*. Broadcom.

<https://docs.broadcom.com/doc/istr-23-2018-en> (Accessed 15 April 2020).

Symantec. (2019, February). *Internet Security Threat Report*. (Vol. 24). Broadcom.
<https://docs.broadcom.com/doc/istr-24-2019-en> (Accessed 15 April 2020).

Tahenni, A., Belkhir, A. (2025). Safeguarding Privacy of Sensitive E-Health Data Against AI Predictive Algorithm Threats. In Yang, X.S., Sherratt, S., Dey, N., Joshi, A. (eds) *Proceedings of Tenth International Congress on Information and Communication Technology. ICICT 2025*. Lecture Notes in Networks and Systems, vol 1414. Springer, Singapore.
https://doi.org/10.1007/978-981-96-6432-0_21

Talwar, S., Dhir, A., Islam, N., Kaur, P., & Almusharraf, A. (2023). Resistance of multiple stakeholders to E-Health innovations: integration of fundamental insights and guiding research paths. *Journal of Business Research*, 166, 114135.
<https://doi.org/10.1016/j.jbusres.2023.114135>

Taylor, S. (2019, October 5). *DCH pays hackers*. *Tuscaloosaneews.Com*.
<https://www.tuscaloosaneews.com/news/20191005/dch-pays-hackers-responsible-for-ransomware-attack> (Accessed 7 July 2022).

Terhune C (2015, February 5) *Anthem hack exposes data on 80 million; experts warn of identity theft*. In: Los Angeles Times. <https://www.latimes.com/business/la-fi-anthem-hacked-20150204-story.html> (Accessed 4 November 2024).

Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research Methodology*, 8(45), 1–10.
<https://doi.org/10.1186/1471-2288-8-45>

Thomas, J., Harden, A., & Newman, H. (2012). Synthesis: Combining results systematically and appropriately. In D. Gough, S. Oliver, & J. Thomas (Eds.), *An Introduction to Systematic Review*. Sage Publication.

Thomson, K. L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, 10, 7–11.
[https://doi.org/10.1016/S1361-3723\(06\)70430-4](https://doi.org/10.1016/S1361-3723(06)70430-4)

TrapX Labs. (2015). *Anatomy of an attack MEDJACK (Medical Device Hijack)*. TRAPX SECURITY, 1–39. https://securityledger.com/wp-content/uploads/2015/06/AOA_MEDJACK_LAYOUT_6-0_6-3-2015-1.pdf (Accessed 1 November 2024).

Trim, P., & Upton, D. (2013). *Cybersecurity Culture: Counteracting Cyber Threats through Organizational Learning and Training*. Routledge. <https://doi.org/10.4324/9781315575681>

Triplett, W. J. (2024). Cybersecurity vulnerabilities in healthcare: a threat to patient security. *Cybersecurity and Innovative Technology Journal*, 2(1), 15-25. <https://doi.org/10.53889/citj.v2i1.333>

Troiano, D. (1999). A primer on pharmacy information systems. *Journal of Healthcare Information Management*, 13(3), 41–52.

Tubaishat, A., & Habiballah, L. (2016). eHealth literacy among undergraduate nursing students. *Nurse Education Today*, 42, 47–52. <https://doi.org/10.1016/j.nedt.2016.04.003>

Tulu, B., Chatterjee, S., & Laxminarayan, S. (2005). A taxonomy of telemedicine efforts with respect to applications, infrastructure, delivery tools, type of setting and purpose. In *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, Big Island, HI, USA, 147. <https://doi.org/10.1109/HICSS.2005.56>

Tully, J., Selzer, J., Phillips, J. P., O'Connor, P., & Dameff, C. (2020). Healthcare challenges in the era of cybersecurity. *Health security*, 18(3), 228-231. <https://doi.org/10.1089/hs.2019.0123>

U.S. Department of Energy. (2014, February). *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). Version 1.1*. Department of Energy <http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf> (Accessed 10 September 2024)

U.S. Department of Energy. (2022, June). *Cybersecurity Capability Maturity Model (C2M2). Version 2.1*. Department of Energy <https://energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf> (Accessed 10 September 2024).

U.S. Department of Health and Human Services. (2016). *FACT SHEET: Ransomware and HIPAA*. <http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf> (Accessed 1 July 2020).

U.S. Department of Homeland Security. (2014). *Cybersecurity Capability Maturity Model White Paper*. Homeland Security. <https://www.hsdl.org/c/view?docid=798503> (Accessed 5 December 2024).

U.S. Government Publishing Office. (1996). *Health Insurance Portability and Accountability Act (HIPAA) Act of 1996*, Public Law 104-191. Government Publishing Office <https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf> (Accessed 06 August 2020).

U.S. Government Publishing Office. (2006). *44 U.S. Code. & 3542: Information Security Definitions*. Government Publishing Office <https://www.govinfo.gov/content/pkg/USCODE-2011-title44/html/USCODE-2011-title44-chap35-subchapIII-sec3542.htm> (Accessed 17 August 2020).

U.S. Food and Drug Administration. (2025). *Cybersecurity in Medical Devices: Quality Systems Considerations and Content of Premarket Submissions: Guidance for Industry and Food and Drug Administrative Staff*. <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions> (Accessed 10 July 2025).

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cybersecurity culture: Current practices and future needs. *Computers & Security*, 109, 102387. <https://doi.org/10.1016/j.cose.2021.102387>

Vallas, C. (2019, June 13). *Boardman medical practice hacked, told to pay \$75,000 in bitcoin unlock system to Unlock system*. 21WFMJ. <https://www.wfmj.com/story/40646778/boardman-medical-practice-hacked-told-to-pay-75000-in-bitcoin-to-unlock-system> (Accessed 2 June 2022).

Van 't Wout, C. (2019). Develop and maintain a cybersecurity organisational culture. In *Proceedings of the 14th International Conference on Cyber Warfare and Security, ICCWS 2019*, 457–466.

Van Niekerk, J. F., & von Solms, R. (2010). Information security culture: A management perspective. *Computers and Security*, 29(4), 476–486.
<https://doi.org/10.1016/j.cose.2009.10.005>

Van Niekerk, J., & von Solms, R. (2006). Understanding Information Security Culture: A Conceptual Framework. In *Proceedings of the Information Security South Africa*, ISSA 2006, 1–10. http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/21_Paper.pdf

Van Zadelhoff, M. (2016, September 19). *The Biggest Cybersecurity Threats Are Inside Your Company*. Harvard Business Review. <https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company> (Accessed 4 October 2020).

Vasko, J., & Gardner, C. (2019, February 21). *Insider Threats in Healthcare (Part 7 of 9: Insider Threats Across Industry Sectors)*. Carnegie Mellon University Software Engineering Institute. <https://insights.sei.cmu.edu/insider-threat/2019/02/insider-threats-in-healthcare-part-7-of-9-insider-threats-across-industry-sectors.html> (Accessed 7 June 2023).

Verizon. (2016). *2016 Data Breach Investigations Report*. Verizon business https://www.verizon.com/business/resources/reports/DBIR_2016_Report.pdf? (Accessed 10 May 2020).

Verizon. (2018). *2018 Data Breach Investigations Report: The year of ransomware*. Verizon business https://www.researchgate.net/publication/324455350_2018_Verizon_Data_Breach_Investigations_Report/. (Accessed 10 April 2021).

Verizon. (2022). *2022 Data breach investigation report 4 industries*. Verizon business https://www.researchgate.net/publication/362160949_2022_Data_Breach_Investigations_Report?channel=doi&linkId=62d97becf3acdd5dc20b8ced&showFulltext=true/. (Accessed 10 April 2021).

Verizon. (2024). *2024 Data Breach Investigations Report*. Verizon business <https://www.verizon.com/business/resources/Tad3/reports/2024-dbir-data-breach-investigations-report.pdf> (Accessed 10 March 2025).

- Verma, S., Gautam, R. K., Pandey, S., Mishra, A., & Shukla, S. (2017). Sampling Typology and Techniques. *International Journal for Scientific Research & Development*, 5(9), 2321–0613.
- Von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, 26(1), 2–9. <https://doi.org/10.1108/ICS-04-2017-0025>
- Von Solms, R., & van Niekerk, J. (2013). From information security to cybersecurity. *Computers and Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
- Vilakazi, K., & Adebessin, F. (2023). A systematic literature review on cybersecurity threats to healthcare data and mitigation strategies. In *Proceedings of the Society 5.0 Conference 2023*, vol.93, 240–251. <https://doi.org/10.29007/hf15>
- Wagstaff, J. (2015, June 5). *Medical data, cybercriminals' holy grail, now espionage target*. REUTERS. <https://www.reuters.com/article/cybersecurity-usa-targets/medical-data-cybercriminals-holy-grail-now-espionage-target-idUSL3N0YR30R20150605> (Accessed 8 August 2020).
- Walker, J., Pan, E., Johnston, D., Adler-Milstein, J., Bates, D. W., & Middleton, B. (2005). The value of health care information exchange and interoperability. *Health Affairs (Project Hope)*, 24(Suppl 1) Web, 10–18. <https://doi.org/10.1377/hlthaff.w5.10>
- Waller, M., & Stotler, C. (2018). Telemedicine: a Primer. *Current Allergy and Asthma Reports*, 18(10), 1–9. <https://doi.org/10.1007/s11882-018-0808-4>
- Walls, A., Perkins, E., & Weiss, J. (2013). *Definition: Cybersecurity*. Gartner, 7 July. <https://www.gartner.com/en/documents/2510116> (Accessed 1 September 2024).
- Wamala, F. (2011). *The ITU National Cybersecurity Strategy Guide*. International Telecommunication Union. <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf> Accessed 10 July 2019
- Wang, J., Abid, H., Lee, S., Shu, L., & Xia, F. (2011). A secured health care application architecture for cyber-physical systems. *Control Engineering and Applied Informatics*, 13(3), 101–108.

Wang, J., Zhang, Z., Xu, K., Yin, Y., & Guo, P. (2013). A research on security and privacy issues for patient related data in medical organization system. *International Journal of Security and Its Applications*, 7(4), 287–298.

Weber, J. H & Kuziemsky, C. (2019) Pragmatic Interoperability for eHealth Systems: The Fallback Workflow Patterns, *2019 IEEE/ACM 1st International Workshop on Software Engineering for Healthcare (SEH)*, Montreal, QC, Canada, 2019, pp. 29-36, <https://doi.org/10.1109/SEH.2019.00013>

Wedawatta, G., Ingirige, B., & Amaratunga, D. (2011). Case study as a research strategy: Investigating extreme weather resilience of construction SMEs in the UK. In the *Proceedings of the 7th Annual International Conference of the International Institute for Infrastructure*, 1–9.

Whitman, M. E., & Mattord, H. J. (2012). *Principles of information security* (4th ed.). Cengage Learning, Boston, MA.

Wierzynski, A. J. (2019). *The vulnerabilities of autonomous vehicles*. Master's dissertation, Utica College. ProQuest Dissertations & Theses. 13881137

Wikler, E., Bausch, P., & Cutler, D. (2012). *Paper Cuts: Reducing Health Care Administrative Costs*. www.americanprogress.org/issues/healthcare/reports/2012/06/11/11658/paper-cuts (Accessed 29 October 2024).

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, 88, 101640. <https://doi.org/10.1016/j.cose.2019.101640>

Winter, A., & Haux, R. (1995). A three-level graph-based model for the management of hospital information systems. *Methods of Information in Medicine*, 34(04), 378–396. <https://doi.org/10.1055/s-0038-1634610>

World Health Organization. (2012). *National eHealth Strategy Toolkit Overview*. <https://www.who.int/publications/i/item/national-ehealth-strategy-toolkit/>. (Accessed 20 February 2020).

Wu, F. J., Kao, Y. F., & Tseng, Y. C. (2011). From wireless sensor networks towards cyber physical systems. *Pervasive and Mobile Computing*, 7(4), 397–413.

<https://doi.org/10.1016/j.pmcj.2011.03.003>

Wybourne, M. N., Austin, M. F., & Palmer, C. C. (2009). *National Cybersecurity Research and Development Challenges Related to Economics, Physical Infrastructure and Human Behavior an Industry, Academic and Government Perspective*. Institute for Information Infrastructure Protection (I3P)

Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research*, 39(1), 93–112.

<https://doi.org/10.1177/0739456X17723971>

Yigzaw, K. Y., Olabarriaga, S. D., Michalas, A., Marco-Ruiz, L., Hillen, C., Verginadis, Y., ... & Chomutare, T. (2022). Health data security and privacy: Challenges and solutions for the future. *Roadmap to Successful Digital Health Ecosystems*, 335-362.

<https://doi.org/10.1016/B978-0-12-823413-6.00014-8>

Yin, R. K. (2003). *Case Study Research: Design and Method* (3rd ed.). SAGE Publication.

Yin, R. K. (2014). *Case study research: Design and methods* (5th ed.). SAGE Publication.

Young, M. (2016). *Private vs. Public Healthcare in South Africa*. Honours dissertation, Western Michigan University. http://scholarworks.wmich.edu/honors_theses (Accessed 12 May 2022).

Yüksel, B., Küpçü, A., & Özkasap, Ö. (2017). Research issues for privacy and security of electronic health services. *Future Generation Computer Systems*, 68, 1–13.

<https://doi.org/10.1016/j.future.2016.08.011>

Yusof, M. M., Papazafeiropoulou, A., Paul, R. J., & Stergioulas, L. K. (2008). Investigating evaluation frameworks for health information systems. *International Journal of Medical Informatics*, 77(6), 377–385. <https://doi.org/10.1016/j.ijmedinf.2007.08.004>

Zamora, W. (2019, August 8). *Labs quarterly report finds ransomware's gone rampant against businesses*. Malwarebytes Labs. <https://blog.malwarebytes.com/reports/2019/08/labs-quarterly-report-finds-ransomwares-gone-rampant-against-businesses/> (Accessed 23 September 2020).

Zarei, J., & Sadoughi, F. (2016). Information security risk management for computerized health information systems in hospitals: a case study of Iran. *Risk Management Health Policy*, 9, 75–85. <https://doi.org/10.2147/RMHP.S99908>

Zetter, K. (2016, March 30). *Why Hospitals Are the Perfect Targets for Ransomware*. WIRED. <https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/> (Accessed 1 September 2020).

Zhang, X., Yu, P., Yan, J., & Ton A M Spil, I. (2015). Using diffusion of innovation theory to understand the factors impacting patient acceptance and use of consumer E-Health innovations: A case study in a primary care clinic Healthcare needs and demand. *BMC Health Services Research*, 15, 17. <https://doi.org/10.1186/s12913-015-0726-2>

Zonneveld, M., Patomella, A., Asaba, E., & Guidetti, S. (2020). The use of information and communication technology in healthcare to improve participation in everyday life: A scoping review. *Disability and Rehabilitation*, 42(23), 3416-3423. <https://doi.org/10.1080/09638288.2019.1592246>

APPENDICES

APPENDIX_1: CHAPTER 4

APPENDIX_1A: DEFINITIONS OF THE IDENTIFIED CSC FACTORS



Cybersecurity
culture factors, defini

APPENDIX_2: CHAPTER 5

APPENDIX_2A: ETHICAL CLEARANCE



UNISA-CAES HEALTH RESEARCH ETHICS COMMITTEE

Date: 04/07/2024

Dear Ms Mwim

**Decision: Ethics Approval
Confirmation after Fourth Review
from 01/07/2024 to 30/06/2025**

NHREC Registration # : REC-170616-051
REC Reference # : 2019/CAES_HREC/091
Name : Ms EN Mwim
Student # : 33825610

Researcher(s): Ms EN Mwim
mwimen@unisa.ac.za

Supervisor (s): Dr J Mtsweni
mtswenij@gmail.com; 072-407-4757

Working title of research:

A contextual framework for establishing cybersecurity culture in the public e-Health
Institutions: a case study of South Africa

Qualification: PhD In Information Systems

Thank you for the submission of your yearly progress report and amendment request to the Unisa-CAES Health Research Ethics Committee for the above mentioned research. Ethics approval is confirmed to continue for one year, and may be renewed on a yearly basis subject to submission of a progress report. **Failure to submit the progress report will lead to withdrawal of the ethics clearance until the report has been submitted.**

Due date for next progress report: 30 June 2025

The progress report form can be downloaded from the college ethics webpage:
<https://w2.unisa.ac.za/www.unisa.ac.za/sites/corporate/default/Colleges/Agriculture-%26-Environmental-Sciences/Research/Research-Ethics.html>

APPENDIX_2B: HOSPITAL PERMISSION



MPUMALANGA PROVINCE
REPUBLIC OF SOUTH AFRICA
25 Pekaing School, Carolina, Maseru
Private Bag 708, Carolina, 1185
Tel: 017 843 1472 Fax: 017 843 1473

Libro: Leterphilo

Departement van Gesondheid

Uitvoering: Witsbank

TO : EMILIA N MWIM
LECTURER
SCHOOL OF COMPUTING

FROM : DR O.D ONYUMBE
CLINICAL MANAGER
CAROLINA HOSPITAL

DATE : 06 OCTOBER 2020

SUBJECT : RE: REQUEST TO CONDUCT RESEARCH IN CAROLINA HOSPITAL

The above matter bears reference:

1. We have received your email requesting to conduct research title: "A contextual framework for establishing cybersecurity culture in the public e-health institutions: a case study of South Africa" in Carolina Hospital.
2. Upon consultation with the Chief Executive Officer of the hospital, we hereby grant you permission to conduct the research.
3. For any queries please contact me Dr O.D Onyumba on 017 843 1121 Ext 1022 or 072 206 7359 or email: drokoka@gmail.com

Hope you find the above in order.

Thank You.

Dr O.D Onyumba
Clinical Manager
Carolina Hospital

06.10.2020
Date



MPUMALANGA PROVINCIAL GOVERNMENT



WITBANK HOSPITAL
Private Bag 11280, Maseru, 1200 Maseru, Maseru
Tel: 017 843 1472 Fax: 017 843 1473

Libro: Leterphilo

Departement van Gesondheid

Uitvoering: Witsbank

Enquiries: Ms S.P. Phiso
Tel: 072 321 2098

TO: Ms Emilia Mwin
Lecturer
School of Computing

FROM: Mrs K.A.P. Madonsela
Chief Executive Officer
Witsbank Hospital

DATE: 19/05/2022

RE- REQUEST FOR PERMISSION TO CONDUCT RESEARCH AT WITBANK HOSPITAL.

We are pleased to inform you that we approve your request to conduct research in the institution on A contextual framework for establishing cybersecurity culture in the public e-health institutions

This is a factor that needs to be unveiled for the benefit of a strong cybersecurity culture in the public e-health institutions. Please be advised that you are expected to come back and present your research outcomes to the Facility Management after your study is concluded.

We will support you throughout the execution.

Regards

Mrs K.A.P. Madonsela
CEO Witsbank Hospital

19/05/2022
Date

5 Declaration

Declaration by Applicant:

I Mr/Ms/Dr/Prof/Adv. Emilia Mwin agree to submit/present the result of this study back to the CEO/Institution/District.

Estimated date of feedback: 30-May-23

Comment by CEO/DM/PM:

Supported / Not-Supported

Supported

Signature:

11.12.2020

Date:

Name: Dr O.D Onyumba

CAROLINA HOSPITAL
PRIVATE BAG X708
CAROLINA 1185

2020-12-11

ADMISSION SECTION
TEL 017 843 1122/21 FAX 017 843 1473
SIGNATURE:

A duly signed form can be uploaded on the website by the researcher or emailed to:
JerryS@mpuhealth.gov.za or ThembaM@mpuhealth.gov.za

APPENDIX_2C: MPUMALANGA PROVINCIAL DEPARTMENT OF HEALTH PERMISSION



health
MPUMALANGA PROVINCE
REPUBLIC OF SOUTH AFRICA

Indwe Building, Government Boulevard, Riverside Park, Ext. 2, Mbombela, 1200, Mpumalanga Province
Private Bag X11285, Mbombela, 1200, Mpumalanga Province
Tel l: +27 (13) 766 3429, Fax: +27 (13) 766 3458

Litiko Letemphilo

Departement van Gesondheid

UmNyango WezeMaphilo

Enq: 013 766 3766/3511
Ref: MP_202012_001

Research Approval Letter

Mrs Emilia Mwim
BLOCK C, OFFICE NUMBER 4-13.
University of South Africa College of Science,
Engineering and Technology
ROODEPOORT, 1710

TITLE: APPLICATION FOR RESEARCH APPROVAL: A CONTEXTUAL FRAMEWORK FOR ESTABLISHING CYBERSECURITY CULTURE IN THE PUBLIC E-HEALTH INSTITUTIONS: A CASE STUDY OF SOUTH AFRICA

Dear Mrs Mwim

The Provincial Department of Health Research Committee has approved your research proposal in the latest format you sent.

- Approval Reference Number: MP_202012_001
- Data Collection Period: 10/01/2021 to 20/06/2023.
- Approved Data Collection Facilities:
* Carolina Hospital & Witbank Hospital

Kindly ensure that conditions mentioned below are adhered to, and that the study is conducted with minimal disruption and impact on our staff, and also ensure that you provide us with a soft or hard copy of the report once your research project has been completed.

Conditions:

- Researchers not allowed to make copies or take pictures of medical records.
- Kindly notify the facility manager *BEFORE* you start with data collection to ensure that conditions are conducive in the facility

Kind regards

DR J SIGUDLA
MPUMALANGA PHRC
DATE: 18/07/2022



APPENDIX_3: CHAPTER 6

APPENDIX_3A: THE QUESTIONNAIRE

Introduction

Though E-Health systems present many opportunities to various E-Health institutions, many of these institutions are left vulnerable to cybercrime, threats and trends. Recent research has shown that healthcare institutions struggle to keep up with existing and modern cybersecurity threats, the institutions has become the primary target for healthcare information theft. To tackle the problem of cybercrime and threats in an E-Health institution, there is need to employ coordinated and unified cybersecurity capability.

In response to the above problem, the primary aim of this research is to develop a contextual framework for establishing cybersecurity culture in E-Health institutions. The contextual framework would be evaluated by cybersecurity and/or cybersecurity culture experts.

The questionnaire consists of six sections (sections A-F), All the sections (A – F) are to be answered by all respondents. The six sections are designed to generate answers that will help achieve the aims of this research.

CONSENT TO PARTICIPATE IN THIS STUDY

I, _____ (participant name), confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet.

“A contextual framework for establishing cybersecurity culture in the Public E-Health institutions: a case study of South Africa” (PhD Study)

University of South Africa

College of Science, Engineering and Technology

School of Computing

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be processed into a research report, journal publications and/or conference proceedings, but that my participation will be kept confidential unless otherwise specified.

I agree to participate in this research.

I have received a signed copy of the informed consent agreement.

Participant Name & Surname..... (please print)

Participant Signature..... Date.....

Researcher's Name & Surname...Emilia Mwim..... (please print)

Researcher's signature..... Date.....

Data findings can be released to participants if interested by indicating interest to

Research at the University of South Africa that involves human participants is overseen by the College of Agriculture Science (CAS) Ethics Committee. If you have questions about your rights as a participant or if you have any problems in this regard, write to the chairperson of the Ethics Committee, School of Computing, PO Box 392, Unisa, 0003.© UNISA

	Instructions * Please indicate your response by ticking the appropriate option that best apply to you to each of the questions listed. * Please select only one option unless otherwise indicated.																		
1.	What is your age? <table border="1"><tr><td>1.</td><td>18 - 20 years</td><td></td></tr><tr><td>2.</td><td>21 - 30 years</td><td></td></tr><tr><td>3.</td><td>31 - 40 years</td><td></td></tr><tr><td>4.</td><td>41 - 50 years</td><td></td></tr><tr><td>5.</td><td>51 - 60 years</td><td></td></tr><tr><td>6.</td><td>60 +</td><td></td></tr></table>	1.	18 - 20 years		2.	21 - 30 years		3.	31 - 40 years		4.	41 - 50 years		5.	51 - 60 years		6.	60 +	
1.	18 - 20 years																		
2.	21 - 30 years																		
3.	31 - 40 years																		
4.	41 - 50 years																		
5.	51 - 60 years																		
6.	60 +																		
2.	Your gender: <table border="1"><tr><td>1.</td><td>Male</td><td></td></tr><tr><td>2.</td><td>Female</td><td></td></tr><tr><td>3.</td><td>other</td><td></td></tr></table>	1.	Male		2.	Female		3.	other										
1.	Male																		
2.	Female																		
3.	other																		
3.	Your education level: <table border="1"><tr><td>1.</td><td>Secondary Education</td><td></td></tr><tr><td>2.</td><td>Vocational professional nursing training</td><td></td></tr><tr><td>3.</td><td>Bachelor's degree</td><td></td></tr><tr><td>4.</td><td>Master's MSc degree</td><td></td></tr><tr><td>5.</td><td>Doctoral (PhD) degree</td><td></td></tr><tr><td>6.</td><td>Other: Specify</td><td></td></tr></table>	1.	Secondary Education		2.	Vocational professional nursing training		3.	Bachelor's degree		4.	Master's MSc degree		5.	Doctoral (PhD) degree		6.	Other: Specify	
1.	Secondary Education																		
2.	Vocational professional nursing training																		
3.	Bachelor's degree																		
4.	Master's MSc degree																		
5.	Doctoral (PhD) degree																		
6.	Other: Specify																		
4.	Position or job title: <table border="1"><tr><td>1.</td><td>Doctor</td><td></td></tr><tr><td>2.</td><td>Nurse</td><td></td></tr></table>	1.	Doctor		2.	Nurse													
1.	Doctor																		
2.	Nurse																		

	3.	Auxiliary personnel	
	4.	Lab. Personnel	
	5.	Pharmacist	
	6.	Administrative personnel	
	7.	Other: specify	
5.	Which hospital department or section do you work for? 		
6.	How long have you worked in this hospital?		
	1.	10 + years	
	2.	10 years	
	3.	5 years	
	4.	3 year	
	5.	Less than a year	
7.	Does your work in the hospital involve working on a computer (or any other ICT device) with internet at any time?		
	1. Yes		
	2. No		
	Does your work in the hospital involves access to confidential and sensitive patient data?		
	1. Yes		
	2. No		

Instructions for the completion of Sections B to F

Please note

In the applicable section that follows, please rate your responses to the question statements by selecting, from the agreement rating scale included below, the response that best describes your perception to each of the question statements. Please reflect your true perception on each statement and use the “Neutral” option sparingly - in this way data integrity and the reliability of research results are guaranteed. The agreement legend specifies:

	<i>Agreement legend:</i> 1 = Strongly disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly agree	
	Section B Cybersecurity awareness and competency (preparedness)	

Below are statements on the cybersecurity awareness, training, and knowledge of employee. Please indicate your level of agreement to each of the listed statements.

Agreement legend:

1 = Strongly disagree

2 = Disagree

3 = Neutral

4 = Agree

5 = Strongly agree

		1	2	3	4	5
1. I have been informed or trained on Protection of Personal Information Act (POPIA) to help minimize breaches of private personal data or cybersecurity incidents.						
2. I have been informed about the cybersecurity behavioral practices from the security policy that my hospital expects from every employee.						
3. Employees are continuously made aware of the emerging cybersecurity threats that affect healthcare institutions.						
4. I am fully aware that not keeping to security practices can result in cyber-attack incident which can have both financial and non-financial impact on my hospital						
5. Internal cybersecurity awareness training are constantly provided to employee to teach us what we need to do to protect the hospital computer systems from cyber-attack?						
6. I am confident I could recognize a security attack issue or incident when I see one.						
7. Employees are constantly made aware of the actions to take when they notice an incident of cyber threat like receiving a suspicious email.						
8. I know that my security activities can play a role in sustaining or endangering the security of my hospital critical resources.						
9. My work computer has experienced virus or other security attacks.						

	10. I know what to do when I receive a suspicious email.																																							
	11. I know who to contact when my computer is infected or hacked.																																							
	12. Through training awareness programs, top management make us understand the importance of cybersecurity.																																							
	13. My computer devices in the hospital has virus dictation software installed in them.																																							
	14. Employees are trained on the specific cybersecurity skills and abilities needed to protect the institution from cyber-attacks.																																							
	15. The hospital offers cybersecurity training programs yearly that employees are encouraged and supported to attend to gain the necessary security skills and knowledge that informs their actions on cybersecurity issues at the hospital.																																							
9.	Do you know what these cyber-attacks (Malware, Ransomware, Medical device hijack, spear phishing, social engineering threats, email scam, virus or trojan) are and how to identify them? <table border="1"> <tr> <td>1.</td> <td>Yes - I know what these attacks are and how to identify them</td> <td></td> </tr> <tr> <td>2.</td> <td>No - I do not know what these attacks are and how to identify them</td> <td></td> </tr> <tr> <td>3.</td> <td>Yes - I know what these attacks are but do not know how to identify them</td> <td></td> </tr> <tr> <td>4.</td> <td>I only know what some these attacks are but not how to identify them</td> <td></td> </tr> </table>							1.	Yes - I know what these attacks are and how to identify them		2.	No - I do not know what these attacks are and how to identify them		3.	Yes - I know what these attacks are but do not know how to identify them		4.	I only know what some these attacks are but not how to identify them																						
1.	Yes - I know what these attacks are and how to identify them																																							
2.	No - I do not know what these attacks are and how to identify them																																							
3.	Yes - I know what these attacks are but do not know how to identify them																																							
4.	I only know what some these attacks are but not how to identify them																																							
10.	Which of the following cyber threats do you know and can identify? <table border="1"> <tr> <td>1.</td> <td>Malware</td> <td></td> </tr> <tr> <td>2.</td> <td>Ransomware</td> <td></td> </tr> <tr> <td>3.</td> <td>Medical device hijack</td> <td></td> </tr> <tr> <td>4.</td> <td>Spear phishing</td> <td></td> </tr> <tr> <td>5.</td> <td>Social engineering</td> <td></td> </tr> <tr> <td>6.</td> <td>Email scam</td> <td></td> </tr> <tr> <td>7.</td> <td>Virus or trojan</td> <td></td> </tr> </table> Which of the cyber threats have your experienced or faced? <table border="1"> <tr> <td>1.</td> <td>Malware</td> <td></td> </tr> <tr> <td>2.</td> <td>Ransomware</td> <td></td> </tr> <tr> <td>3.</td> <td>Medical device hijack</td> <td></td> </tr> <tr> <td>4.</td> <td>Spear phishing</td> <td></td> </tr> </table>							1.	Malware		2.	Ransomware		3.	Medical device hijack		4.	Spear phishing		5.	Social engineering		6.	Email scam		7.	Virus or trojan		1.	Malware		2.	Ransomware		3.	Medical device hijack		4.	Spear phishing	
1.	Malware																																							
2.	Ransomware																																							
3.	Medical device hijack																																							
4.	Spear phishing																																							
5.	Social engineering																																							
6.	Email scam																																							
7.	Virus or trojan																																							
1.	Malware																																							
2.	Ransomware																																							
3.	Medical device hijack																																							
4.	Spear phishing																																							
11.																																								

	<table border="1"> <tr> <td>5.</td> <td>Social engineering</td> <td></td> </tr> <tr> <td>6.</td> <td>Email scam</td> <td></td> </tr> <tr> <td>7.</td> <td>Virus or trojan</td> <td></td> </tr> <tr> <td>8</td> <td>Other Please specify</td> <td></td> </tr> </table>	5.	Social engineering		6.	Email scam		7.	Virus or trojan		8	Other Please specify																			
5.	Social engineering																														
6.	Email scam																														
7.	Virus or trojan																														
8	Other Please specify																														
12	Which of the followings applies to the devices you use in the hospital for your work? (you can select multiple options) <table border="1"> <tr> <td>1.</td> <td>Most of them have anti-virus installed on them</td> <td></td> </tr> <tr> <td>2.</td> <td>They have password protection</td> <td></td> </tr> <tr> <td>3.</td> <td>They are accessed by users other than myself</td> <td></td> </tr> <tr> <td>4.</td> <td>I download and stall software on them</td> <td></td> </tr> <tr> <td>5.</td> <td>They are both personal and corporate</td> <td></td> </tr> <tr> <td>6.</td> <td>I have found virus or trojan in them</td> <td></td> </tr> </table>	1.	Most of them have anti-virus installed on them		2.	They have password protection		3.	They are accessed by users other than myself		4.	I download and stall software on them		5.	They are both personal and corporate		6.	I have found virus or trojan in them													
1.	Most of them have anti-virus installed on them																														
2.	They have password protection																														
3.	They are accessed by users other than myself																														
4.	I download and stall software on them																														
5.	They are both personal and corporate																														
6.	I have found virus or trojan in them																														
Section C Employee attitude and behaviors (Responsibility)																															
13.	Please rate the extent of your agreement to each of the following statements that enquire about employee cybersecurity attitudes, practices and behaviors. <i>Agreement legend:</i> 1 = Strongly disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly agree <table border="1"> <thead> <tr> <th></th> <th>1</th> <th>2</th> <th>3</th> <th>4</th> <th>5</th> </tr> </thead> <tbody> <tr> <td>1. Following the security practices, policies and measures of my hospital makes it challenging for me to do my daily business function of caring for patients.</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>2. I am happy to conform with the security practices and guidance of my hospital.</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>3. I make use of many computer systems or ICT devices daily and that makes it problematic for me to maintain security across all the devices.</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>4. I feel that my hospital is well prepared to handle cyber threats at this stage because of the kind of attention it gives to security related issues like incident response among others.</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>		1	2	3	4	5	1. Following the security practices, policies and measures of my hospital makes it challenging for me to do my daily business function of caring for patients.						2. I am happy to conform with the security practices and guidance of my hospital.						3. I make use of many computer systems or ICT devices daily and that makes it problematic for me to maintain security across all the devices.						4. I feel that my hospital is well prepared to handle cyber threats at this stage because of the kind of attention it gives to security related issues like incident response among others.					
	1	2	3	4	5																										
1. Following the security practices, policies and measures of my hospital makes it challenging for me to do my daily business function of caring for patients.																															
2. I am happy to conform with the security practices and guidance of my hospital.																															
3. I make use of many computer systems or ICT devices daily and that makes it problematic for me to maintain security across all the devices.																															
4. I feel that my hospital is well prepared to handle cyber threats at this stage because of the kind of attention it gives to security related issues like incident response among others.																															

	5. I believe that cyber-criminals are more advanced than the people who are supposed to be protecting us.								
	6. I see our (employee) carelessness, negligence and personal intentions as the main challenge of cybersecurity in our hospital.								
	7. The belief, values, attitudes, norms, culture and skills of people in the hospital towards security create serious challenges in achieving cybersecurity.								
	8. My colleagues and I sometimes share tips to help each other with cybersecurity related issues.								
	9. Reporting cyber-attack incident that take place in our hospital to the policy might damage the reputation of the company.								
	10. I report employees or any other party to the relevant authorizes if I notice they are not following the security policies and procedures of the hospital.								
	11. When it is necessary, I give my computer password to a fellow colleague or my manager when you are asked for it.								
	12. My department interact with other departments for more knowledge on cybersecurity issues.								
	13. My colleagues' behavior towards security influences the way I see and behavior towards security.								
	14. Some of my colleagues are very out spoken when it comes to cybersecurity to help create awareness among follow colleagues.								
	15. Employees who are knowledgeable on cybersecurity practices sometimes help other colleagues with their cybersecurity questions.								
	16. Before I open email attachment, I make sure it is from a person I know, and I am expecting the email.								
	17. I sometimes use my own personal devices, such as your mobile phone or USB sticks or CD/DVD discs to store or transfer confidential information.								
	18. I download and install software on the computer devices I use at work.								
	19. I make sure to lock my computer devices when I am not using them or when I leave my office even for a while daily.								
Section D Management cybersecurity practices (Management)									
14.	Please rate the extent of your agreement to each of the following statements that enquire about management cybersecurity practices. <i>Agreement legend:</i> 1 = Strongly disagree 2 = Disagree 3 = Neutral								

4 = Agree 5 = Strongly agree							
			1	2	3	4	5
1. My hospital has a cybersecurity policy.							
2. My hospital has a well-known cybersecurity department, team or external services that champions cybersecurity related issues.							
3. The computer device or other E-Health systems we use in the hospital are old and outdated.							
4. The computer devices we use in the hospital are managed by our institution.							
5. Employees are punished for their failure to comply with the cybersecurity practices set out by the hospital.							
6. It doesn't matter the kind of effort I put, employees are not rewarded for their effort in adhering to cybersecurity practices.							
7. Campaigns are consistently used to update employees on cybersecurity issues.							
8. The institution sometimes conduct cyber threats exercise like phishing email to test employee cybersecurity knowledge and performance.							
9. Our hospital managements often attend cybersecurity related discussions and meetings.							
10. Our top management take part in cybersecurity activities.							
11. Hospital internal communication mediums (like email, posters, and notices) are used to encourage cybersecurity activities among employees.							
12. Security guidelines are made available to employees							
13. The institution uses access control for employees to obtain access to their working environments.							
14. The institution encourages us to follow the right channel to report any weaknesses we notice with the computer devices we use in the hospital.							
15. Employees are encouraged to take action to protect the hospital assets like patients record, healthcare technologies they use and other ICT devices.							
16. The computers used in the hospital only accept password with combinations of letter, number and special characters.							
Section E Healthcare external environment (Environment)							

15.	Please indicate your level of agreement to each of the following listed statements presented on the environmental factors of healthcare cybersecurity. <i>Agreement legend:</i> 1 = Strongly disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly agree <table border="1"> <thead> <tr> <th></th> <th>1</th> <th>2</th> <th>3</th> <th>4</th> <th>5</th> </tr> </thead> <tbody> <tr> <td>1. Healthcare professionals have too many profession (industry) and government related rules, regulations and guidelines to abide by.</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>2. My work focuses mainly on patient care resulting in less attention being paid on maintaining security related practices and activities.</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>3. My hospital is small and not located in busy cities, therefore we do not receive much attention on cybersecurity issues from external institutions.</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>4. Healthcare institutions are subjected to very strict laws, guidelines and regulations on patient and information management.</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>5. The way the institution and its society see cybersecurity influences the way employee behavior towards cybersecurity.</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>6. Our organization needs to take more action on cybersecurity issues in comparison with other hospitals to position itself as one of the hospitals that takes cybersecurity seriously in the country.</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>		1	2	3	4	5	1. Healthcare professionals have too many profession (industry) and government related rules, regulations and guidelines to abide by.						2. My work focuses mainly on patient care resulting in less attention being paid on maintaining security related practices and activities.						3. My hospital is small and not located in busy cities, therefore we do not receive much attention on cybersecurity issues from external institutions.						4. Healthcare institutions are subjected to very strict laws, guidelines and regulations on patient and information management.						5. The way the institution and its society see cybersecurity influences the way employee behavior towards cybersecurity.						6. Our organization needs to take more action on cybersecurity issues in comparison with other hospitals to position itself as one of the hospitals that takes cybersecurity seriously in the country.					
	1	2	3	4	5																																						
1. Healthcare professionals have too many profession (industry) and government related rules, regulations and guidelines to abide by.																																											
2. My work focuses mainly on patient care resulting in less attention being paid on maintaining security related practices and activities.																																											
3. My hospital is small and not located in busy cities, therefore we do not receive much attention on cybersecurity issues from external institutions.																																											
4. Healthcare institutions are subjected to very strict laws, guidelines and regulations on patient and information management.																																											
5. The way the institution and its society see cybersecurity influences the way employee behavior towards cybersecurity.																																											
6. Our organization needs to take more action on cybersecurity issues in comparison with other hospitals to position itself as one of the hospitals that takes cybersecurity seriously in the country.																																											
Section F Technology																																											
15.	Please indicate your level of agreement to each of the following listed statements presented on the technology factors. <i>Agreement legend:</i> 1 = Strongly disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly agree <table border="1"> <thead> <tr> <th></th> <th>1</th> <th>2</th> <th>3</th> <th>4</th> <th>5</th> </tr> </thead> <tbody> <tr> <td>1. It is difficult to keep up with cybersecurity threats as new cyber threats often appears with new emerging technologies creating the need to learn more security controls.</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>2. Government policies on the increasing use of technologies in healthcare institutions are always changing, and this can be a challenge.</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>		1	2	3	4	5	1. It is difficult to keep up with cybersecurity threats as new cyber threats often appears with new emerging technologies creating the need to learn more security controls.						2. Government policies on the increasing use of technologies in healthcare institutions are always changing, and this can be a challenge.																													
	1	2	3	4	5																																						
1. It is difficult to keep up with cybersecurity threats as new cyber threats often appears with new emerging technologies creating the need to learn more security controls.																																											
2. Government policies on the increasing use of technologies in healthcare institutions are always changing, and this can be a challenge.																																											

Thank you for your participation.

APPENDIX 3B - OTHER PARTS OF DEMOGRAPHIC INFORMATION

Department/Section you work at					
		Frequency	Percent	Valid Percent	Cumulative Percent
		5	5.1	5.1	5.1
	Carolina Causality	1	1.0	1.0	6.1
	Carolina Hospital	1	1.0	1.0	7.1
	Carolina hospital	1	1.0	1.0	8.1
	Carolina Hospital	19	19.2	19.2	27.3
	Carolina Hospital information Management	1	1.0	1.0	28.3
	Carolina Hospital OTD	2	2.0	2.0	30.3
	Carolina Hospital Pharmacist	2	2.0	2.0	32.3
	Carolina Hospital Theatre	1	1.0	1.0	33.3
	Carolina Hospital Wellness	1	1.0	1.0	34.3
	Carolina Hospital	3	3.0	3.0	37.4
	Carolina Hospital Pharmacist	1	1.0	1.0	38.4
	Carolina OPD	1	1.0	1.0	39.4
	Emergency Department	2	2.0	2.0	41.4
	Environment Health	1	1.0	1.0	42.4
	Maternity	1	1.0	1.0	43.4
	Maternity	1	1.0	1.0	44.4
	OPD	1	1.0	1.0	45.5
	OPD Clinical associate	1	1.0	1.0	46.5
	PHC	1	1.0	1.0	47.5
	Witbank Admission	2	2.0	2.0	49.5
	Witbank Casualty emergency	2	2.0	2.0	51.5
	Witbank Family Medicine	8	8.1	8.1	59.6

Department/Section you work at					
		Frequency	Percent	Valid Percent	Cumulative Percent
	Witbank Information Unit	1	1.0	1.0	60.6
	Witbank Nursing management	1	1.0	1.0	61.6
	Witbank Occupational Health & Safety	1	1.0	1.0	62.6
	Witbank OPD	3	3.0	3.0	65.7
	Witbank Paediatrics	1	1.0	1.0	66.7
	Witbank Pharmacy department	5	5.1	5.1	71.7
	Witbank Provincial Hospital	27	27.3	27.3	99.0
	Witbank Ward clerk	1	1.0	1.0	100.0
	Total	99	100.0	100.0	

Work involves use of ICT

Work involves use of ICT					
		Frequency	Percent	Valid Percent	Cumulative Percent
	Yes	91	91.9	91.9	91.9
	No	8	8.1	8.1	100.0
	Total	99	100.0	100.0	

Access to confidential data

Access to confidential data					
		Frequency	Percent	Valid Percent	Cumulative Percent
	Yes	95	96.0	96.0	96.0
	No	4	4.0	4.0	100.0
	Total	99	100.0	100.0	

APPENDIX_3C - CRONBACH'S ALPHA RELIABILITY OF THE CONSTRUCT ITEMS

Item-Total Statistics					
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Cronbach's Alpha
Q8 (preparedness)					.900
Q8_1	34.90	110.557	.585	.894	
Q8_2	35.52	111.663	.684	.889	
Q8_3	35.59	113.949	.712	.889	
Q8_4	34.57	113.931	.513	.896	
Q8_5	35.75	114.758	.666	.891	
Q8_6	35.14	112.603	.598	.893	
Q8_7	35.45	112.587	.694	.889	
Q8_8	34.43	113.110	.572	.894	
Q8_9	34.99	120.368	.320	.903	
Q8_10	34.86	115.318	.451	.899	
Q8_11	34.70	109.813	.602	.893	
Q8_12	35.63	114.616	.689	.890	
Q8_13	34.55	116.839	.503	.896	
Q8_14	35.69	113.964	.680	.890	
Q8_15	35.72	116.604	.585	.894	
Q13 (Responsibility)					.627
Q13_1	41.24	50.349	-.081	.659	
Q13_2	41.23	46.935	.159	.624	
Q13_3	41.22	49.664	-.041	.653	

Item-Total Statistics					
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Cronbach's Alpha
Q13_4	42.39	42.017	.485	.575	
Q13_5	42.09	46.532	.137	.629	
Q13_6	41.43	48.248	.069	.635	
Q13_7	41.73	48.037	.057	.640	
Q13_8	42.40	41.692	.494	.572	
Q13_10	42.16	42.994	.470	.581	
Q13_12	42.58	43.614	.475	.583	
Q13_13	42.05	44.069	.442	.588	
Q13_14	42.33	41.286	.581	.563	
Q13_15	42.18	41.314	.536	.566	
Q13_16	41.42	44.308	.243	.612	
Q13_17	41.80	47.000	.084	.640	
Q13_19	41.27	47.670	.065	.640	
Q14 (management)					.816
Q14_1	39.01	70.908	.606	.795	
Q14_2	38.98	70.857	.616	.794	
Q14_3	38.37	77.400	.191	.822	
Q14_4	37.61	78.180	.164	.823	
Q14_5	37.54	93.700	-.602	.861	
Q14_6	38.26	80.379	.050	.830	
Q14_7	39.25	71.640	.641	.794	
Q14_8	39.27	72.343	.640	.795	
Q14_9	39.08	72.851	.574	.798	
Q14_10	38.90	73.745	.510	.802	
Q14_11	38.94	70.282	.610	.794	
Q14_12	38.97	66.928	.803	.780	
Q14_13	38.64	69.724	.549	.797	
Q14_14	38.67	66.776	.711	.784	
Q14_15	38.35	67.782	.600	.792	
Q14_16	37.89	74.039	.335	.813	

Item-Total Statistics					
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Cronbach's Alpha
Q15 (Environment)					.731
Q15_1	16.31	14.299	.585	.659	
Q15_2	16.29	14.719	.562	.667	
Q15_3	16.22	14.481	.469	.694	
Q15_4	16.66	15.248	.509	.683	
Q15_5	16.83	16.103	.303	.743	
Q15_7	16.78	15.685	.401	.712	
Q16 (Technology)					.607
Q16_1	3.16	1.137	.437		
Q16_2	3.51	1.293	.437		

Question 15_1 and Q15_4 are treated as environment and technology

APPENDIX 3D: COMMUNALITIES

Communalities		
	Initial	Extraction
Q8_1	1.000	.736
Q8_2	1.000	.846
Q8_3	1.000	.736
Q8_4	1.000	.767
Q8_5	1.000	.825
Q8_6	1.000	.652
Q8_7	1.000	.745
Q8_8	1.000	.754
Q8_9	1.000	.725

Communalities		
	Initial	Extraction
Q8_10	1.000	.702
Q8_11	1.000	.778
Q8_12	1.000	.771
Q8_13	1.000	.691
Q8_14	1.000	.719
Q8_15	1.000	.742
Q13_1	1.000	.676
Q13_2	1.000	.725
Q13_3	1.000	.689
Q13_4	1.000	.651
Q13_5	1.000	.700
Q13_6	1.000	.766
Q13_7	1.000	.689
Q13_8	1.000	.726
Q13_10	1.000	.700
Q13_12	1.000	.703
Q13_13	1.000	.687
Q13_14	1.000	.742
Q13_15	1.000	.802
Q13_16	1.000	.738
Q13_17	1.000	.664
Q13_19	1.000	.711

Communalities		
	Initial	Extraction
Q14_1	1.000	.827
Q14_2	1.000	.800
Q14_3	1.000	.700
Q14_4	1.000	.706
Q14_5	1.000	.753
Q14_6	1.000	.667
Q14_7	1.000	.759
Q14_8	1.000	.766
Q14_9	1.000	.834
Q14_10	1.000	.809
Q14_11	1.000	.703
Q14_12	1.000	.787
Q14_13	1.000	.723
Q14_14	1.000	.757
Q14_15	1.000	.802
Q14_16	1.000	.733
Q15_1	1.000	.759
Q15_2	1.000	.721
Q15_3	1.000	.744
Q15_4	1.000	.664
Q15_5	1.000	.749
Q15_7	1.000	.708

Communalities		
	Initial	Extraction
Extraction Method: Principal Component Analysis.		

APPENDIX_3E - TOTAL VARIANCE EXPLAINED

Total Variance Explained						
Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	13.933	26.290	26.290	13.933	26.290	26.290
2	4.661	8.795	35.084	4.661	8.795	35.084
3	2.912	5.494	40.578	2.912	5.494	40.578
4	2.436	4.596	45.174	2.436	4.596	45.174
5	2.242	4.230	49.404	2.242	4.230	49.404
6	1.983	3.742	53.147	1.983	3.742	53.147
7	1.738	3.279	56.426	1.738	3.279	56.426
8	1.587	2.994	59.420	1.587	2.994	59.420
9	1.485	2.802	62.222	1.485	2.802	62.222
10	1.344	2.537	64.759	1.344	2.537	64.759
11	1.316	2.483	67.242	1.316	2.483	67.242
12	1.235	2.330	69.571	1.235	2.330	69.571
13	1.122	2.116	71.687	1.122	2.116	71.687
14	1.036	1.955	73.642	1.036	1.955	73.642
15	.952	1.796	75.438			

Total Variance Explained						
Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
16	.910	1.717	77.155			
17	.786	1.483	78.638			
18	.764	1.441	80.079			
19	.741	1.397	81.477			
20	.705	1.330	82.806			
21	.683	1.290	84.096			
22	.664	1.253	85.348			
23	.631	1.190	86.538			
24	.570	1.076	87.614			
25	.532	1.003	88.618			
26	.493	.930	89.547			
27	.464	.875	90.422			
28	.414	.781	91.203			
29	.398	.751	91.955			
30	.366	.691	92.646			
31	.354	.667	93.313			
32	.343	.648	93.961			
33	.319	.602	94.563			
34	.304	.574	95.137			
35	.272	.513	95.650			

Total Variance Explained						
Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
36	.234	.442	96.092			
37	.223	.421	96.512			
38	.207	.390	96.902			
39	.196	.371	97.273			
40	.182	.343	97.616			
41	.170	.320	97.937			
42	.153	.288	98.225			
43	.143	.270	98.495			
44	.124	.234	98.729			
45	.109	.206	98.935			
46	.100	.188	99.123			
47	.091	.172	99.295			
48	.082	.154	99.449			
49	.076	.144	99.593			
50	.071	.135	99.728			
51	.057	.107	99.835			
52	.053	.100	99.935			
53	.034	.065	100.000			
Extraction Method: Principal Component Analysis.						

APPENDIX_3F - DESCRIPTIVE STATISTICS

	Descriptive Statistics					
Constructs		N	Minimum	Maximum	Mean	Std. Deviation
Preparedness (P)	Q8_1	99	1	5	2.76	1.422
	Q8_2	99	1	5	2.15	1.181
	Q8_3	99	1	4	2.07	.992
	Q8_4	98	1	5	3.09	1.317
	Q8_5	99	1	5	1.92	.997
	Q8_6	99	1	5	2.53	1.256
	Q8_7	99	1	5	2.22	1.112
	Q8_8	98	1	5	3.24	1.252
	Q8_9	99	1	5	2.66	1.179
	Q8_10	98	1	5	2.79	1.334
	Q8_11	99	1	5	2.94	1.441
	Q8_12	99	1	4	2.05	.994
	Q8_13	99	1	5	3.11	1.106
	Q8_14	99	1	5	1.99	1.045
	Q8_15	99	1	4	1.96	.999
	Q13_1	99	1	5	3.39	1.159
	Q13_2	99	1	5	3.40	1.059
	Q13_3	99	1	5	3.41	1.169
	Q13_4	99	1	5	2.24	1.126

	Descriptive Statistics					
Constructs		N	Minimum	Maximum	Mean	Std. Deviation
Responsibility (R)	Q13_5	99	1	5	2.55	1.231
	Q13_6	99	1	5	3.20	1.050
	Q13_7	99	1	5	2.91	1.179
	Q13_8	99	1	5	2.23	1.150
	Q13_10	99	1	5	2.47	1.024
	Q13_12	99	1	4	2.06	.935
	Q13_13	99	1	5	2.59	.926
	Q13_14	99	1	5	2.30	1.064
	Q13_15	99	1	5	2.45	1.127
	Q13_16	99	1	5	3.21	1.327
	Q13_17	99	1	5	2.84	1.345
	Q13_19	99	1	5	3.36	1.249
Management (M)	Q14_1	99	1	5	2.17	1.050
	Q14_2	99	1	5	2.20	1.040
	Q14_3	99	1	5	2.81	1.175
	Q14_4	99	1	5	3.58	1.126
	Q14_5	99	1	5	3.65	1.033
	Q14_6	99	1	5	2.92	1.149
	Q14_7	99	1	4	1.93	.940
	Q14_8	99	1	4	1.91	.882
	Q14_9	99	1	4	2.10	.920
	Q14_10	99	1	4	2.28	.926

	Descriptive Statistics					
Constructs		N	Minimum	Maximum	Mean	Std. Deviation
	Q14_11	99	1	5	2.24	1.098
	Q14_12	99	1	5	2.21	1.109
	Q14_13	99	1	5	2.55	1.248
	Q14_14	99	1	5	2.52	1.240
	Q14_15	99	1	5	2.83	1.333
	Q14_16	99	1	5	3.29	1.239
External Environment (EE)	Q15_1	99	1	5	2.49	1.137
	Q15_2	99	1	5	2.47	1.091
	Q15_3	99	1	5	2.40	1.269
	Q15_4	99	1	5	2.84	1.066
	Q15_5	99	1	5	3.01	1.233
	Q15_7	99	1	5	2.96	1.142
Technology (TECH)	Q16_1	99	1	5	2.49	1.137
	Q16_2	99	1	5	2.84	1.066
	Valid N (listwise)	96				

APPENDIX_4: CHAPTER 7

APPENDIX_4A: INTERVIEW QUESTIONS

Interview Schedules

Research Topic: A contextual framework for establishing a cybersecurity culture in the public E-Health institutions: a case study of South Africa

Student: Emilia Mwim

Supervisor: Dr Mtsweni, Jabu and Prof Bester Chimbo

School of Computing

College of Science, Engineering and Technology

University of South Africa

My name is Emilia Mwim, a registered PhD student at Unisa and I am doing research towards a Doctoral degree in the Department of Information Systems at the University of South Africa (Unisa). The research is supervised by Dr. Jabu Mtsweni, an external supervisor, from Council for Scientific and Industrial Research (CSIR) and Professor B. Chimbo an associate Professor in the School of Computing at Unisa. We are inviting you to participate in a study entitled “**A contextual framework for establishing cybersecurity culture in the public E-Health institutions: a case study of South Africa**”.

This study is expected to collect important information that could help the researcher develop a contextual framework that would assist in the establishment of cybersecurity culture in the public E-Health institutions in South Africa.

INSTRUMENT FOR ICT STAFFS

SECTION A AND B:

ETHICAL CONFORMATION, BIOGRAPHICAL AND ICT BACKGROUND INFORMATION

The purpose of these section are to collect biographical information, as well as the setting/description of the hospitals.

	Number	Domain	Interview Question
Section A: Ethical Consideration	1.	Participation	Can you confirm that your participation in this study is voluntary?
	2.	Withdrawal	Are you aware that you are free to withdraw at any time and without giving a reason?
	3.	Rewards	Do you know the study is for the completion of a degree and no benefits will therefore be derived from your participation in the study?
Section B i: Biographical Information	4.	Name and Province	Please confirm that you work for hospital situated in Province?
	5.	Job Title	What is your job title?
	6.	Years	How long have you worked in this hospital?
	7.	Age	Do you fall within the age range of? 20 - 40 years 41 - 60 years
	8.	Education	What education qualification do you have?
Section Bii: ICT Background information	9.	Organisation size	Approximately how many employees works in the hospital?
	10.	ICT Employee	Do you have sufficient capacity in terms of ICT personnel to ensure data availability is maintained?
	11.	System	Which E-Health systems/applications do you support and/or manage in the hospital?

	12.	Training	How many (number) official training courses have you had in the ICT cybersecurity domain during the last 3 years?
	13.	Budget (managers questions)	What is your hospital average yearly budget allocated to ICT?
	14.	Regulation	How familiar are you with the South African National Cybersecurity Policy Framework (NCPF)?
	15.	Regulation	What is your familiarity with Protection of Personal Information Act (POPIA) regulation?
	16.	Cybersecurity team	Does your hospital have existing and dedicated cybersecurity section, team, champion or external party that is formally responsible to handle cybersecurity issues?
	17.	Policy	Does your hospital have cybersecurity policies, procedures and regulations that guide its security practices and activities?
	18	Risk assessment	Does your hospital perform risk assessment to identify and prioritise the cybersecurity threats and organisational vulnerability that affect them?

SECTION C:

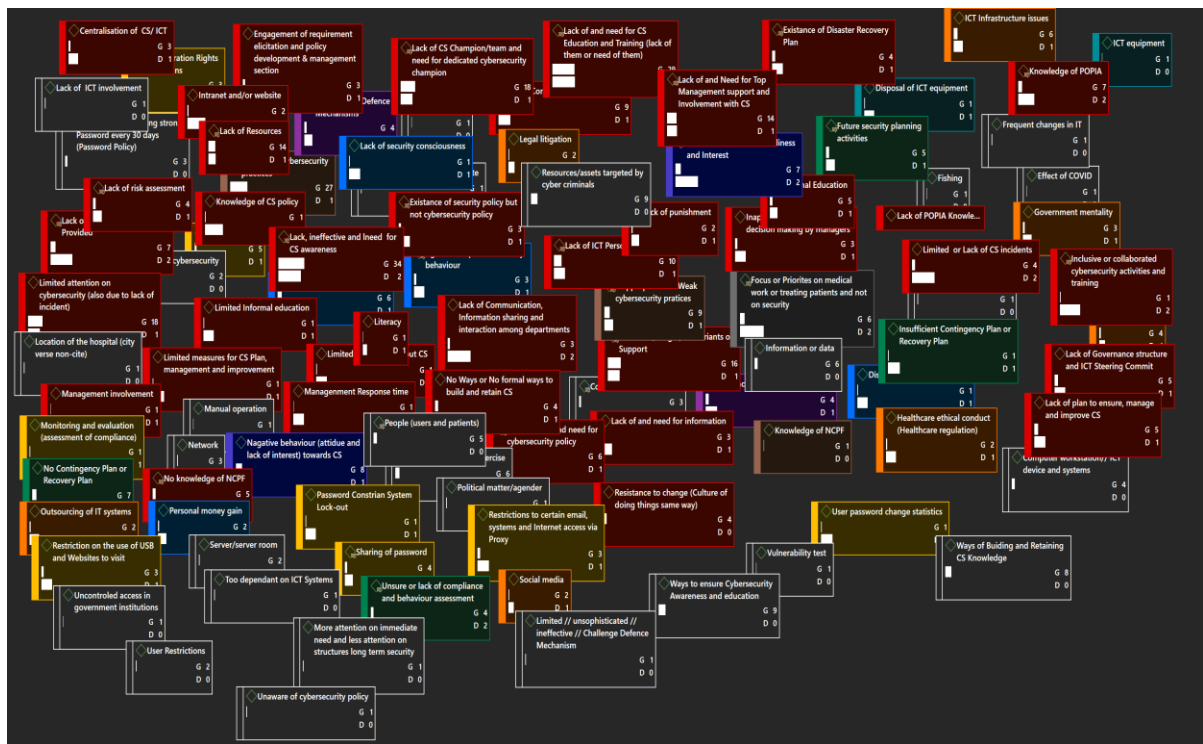
THE INTERVIEW QUESTIONS

The data collected with the questions posed in this section would assist with the understanding the current state of security culture, practices and measures of the institution from the perspectives of ICT staffs. Data collected from this section will also help with understanding the challenges of cybersecurity culture of the hospitals.

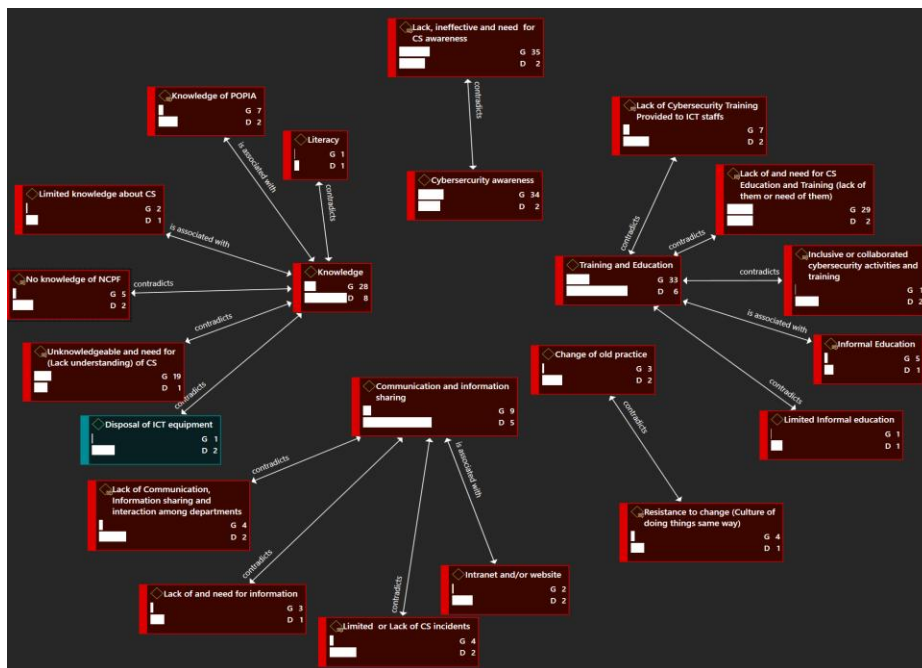
1. In general, how would you describe the culture of your hospital in terms of cybersecurity?
2. What are the critical assets/resources/infrastructures of your hospital that are likely to be target/attacked by cybercriminal?
3. What are the cybersecurity threats and vulnerabilities that present the greatest risk to your hospital?
4. What are the internal organisational factors that influences cybersecurity culture in your hospital?
5. What are the individual factors that influences cybersecurity culture in your hospital?
6. What are the external environmental factors that influences individual behaviour and organisation culture towards cybersecurity in your hospital?
7. What are the management factors that influences cybersecurity culture in your hospital?
8. What cybersecurity plans are in place in your hospital to ensure continuity of business operations?
9. What measures are currently in place to effectively plan, manage, and improve the hospital's cybersecurity?

10. What penetration tests exercise are used to test the overall strength of the hospital defence?
11. What defence mechanisms are used to protect technical assets necessary for the improvement and efficient operation of cybersecurity?
12. What are the practices of your hospital that are used to ensure a secure access to resources cross the organisation?
13. How does the hospital ensure that employees understand the policy and are aware what are expected of them in the policy document (for example their role and responsibilities) to ensure cybersecurity compliance?
14. What are the cybersecurity practices or activities of your hospital that negatively influences employee behaviour?
15. What would you consider as the barriers that prevent or make it difficult from achieving cybersecurity practices set out in your hospital?
16. How does the top management/leadership of your hospital support and get involve in cybersecurity?
17. How does the hospital build and retain cybersecurity knowledge and skills internally among employees?
18. How are cybersecurity compliance and behaviours of employed assessed to ensure that the cybersecurity policies and procedures are adhered to?
19. How do you ensure that the security practices of your hospital align with the business functions of different stakeholder or do not conflict with the business functions of different stakeholders?
20. In your opinion, what do you think the hospital needs to do to encourage more cybersecure behaviour among employee?

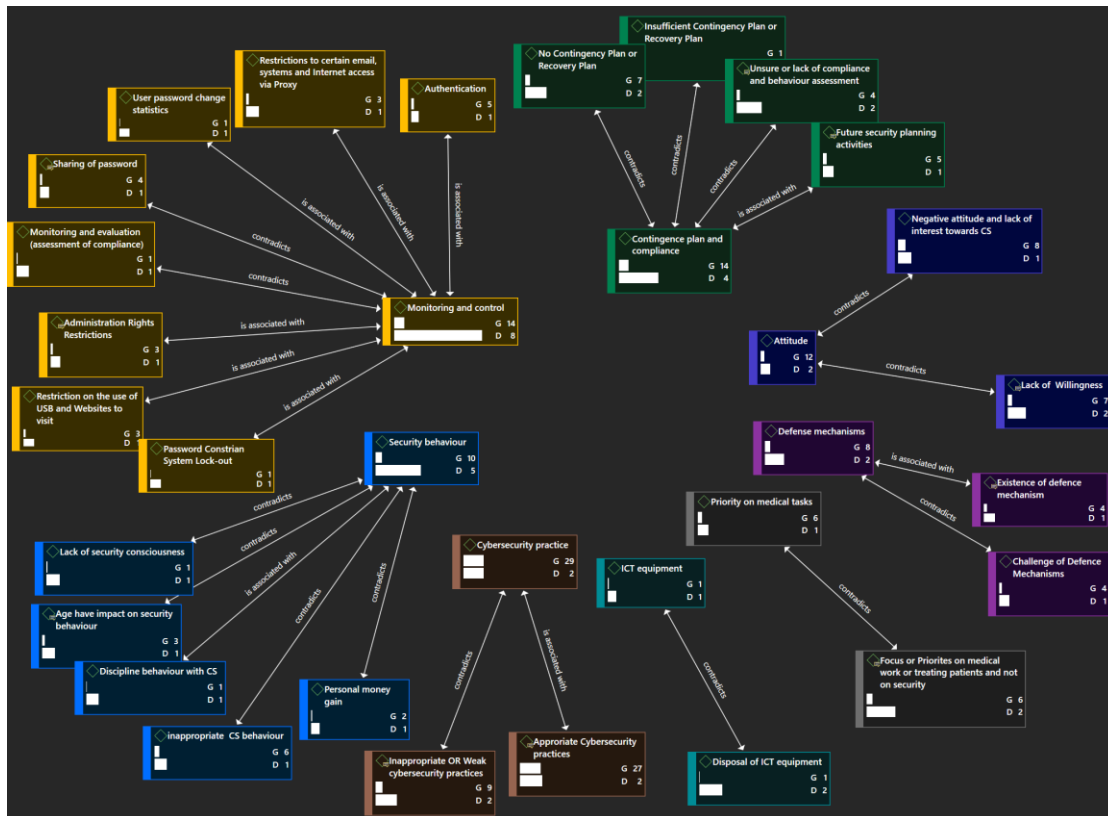
APPENDIX_4B: OPEN CODE



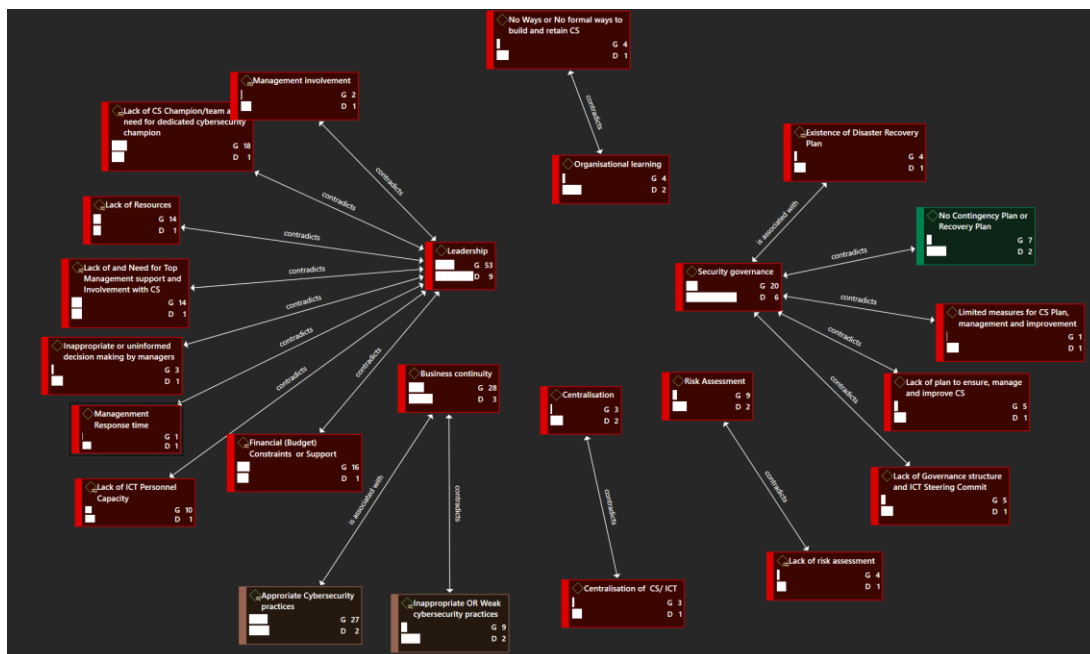
APPENDIX_4C: INITIAL 24 THEMES WITH THEIR ORIGINAL CODES



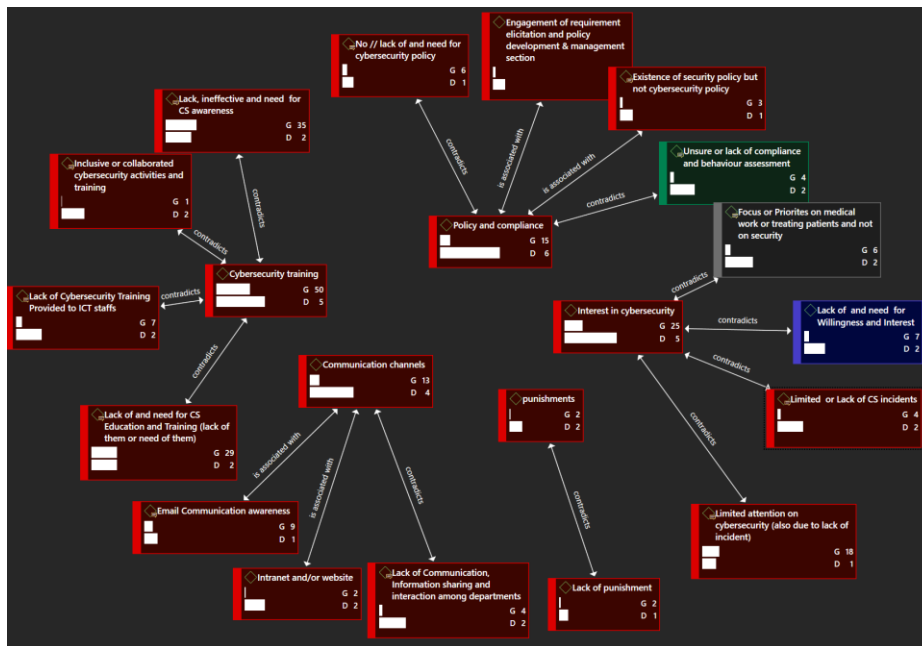
Theme Map 1



Theme map 2



Theme map 3



Theme map 4

Table summary of the 24 initial themes

Initial 24 candidate themes	
Cybersecurity awareness	Leadership
Knowledge	Security governance
Communication and information sharing	Risk assessment
Training and education	Centralisation
Change of old practice	Business continuity
Monitoring and control	Organisational learning
Contingence plan and compliance	Policy and compliance
Attitude	Interest in cybersecurity
Defence mechanism	Discipline
Priority on medical tasks	Communication channels
ICT equipment	Cybersecurity training
Cybersecurity practices	
Security behaviour	

APPENDIX_5: CHAPTER 8

APPENDIX_5A: IOM ELEMENTS AND RELATED ACTIVITIES

IOM elements and related activities

Activity ref no	Activities and actions
Leadership (G-112)	
IOM_L_(1)	(1) Develop (example through keeping records of CS incidents) the interest and attention of top leadership in cybersecurity (CS). For example, through keeping records of the impacts or cost of CS incidents and by making them understand it's significant and need (G-29).
IOM_L_(2)	(2) Provide sufficient and appropriate size resources like ICT staff capacity and other resources for business necessities and to ensure CS (G-24).
IOM_L_(3)	(3) Appoint a cybersecurity culture (CSC) champion or team that will be formally responsible for developing and maintaining cybersecurity culture in the institution and set up cybersecurity culture hub (G-18).
IOM_L_(4)	(4) Include members of top management as part of the cybersecurity culture team to ensure their involvement and support (G-16).
IOM_L_(5)	(5) Have a separate and reasonable sub-budget under ICT for CS-related activities, infrastructures, and ICT personnel as part of top management financial support (G-16).
IOM_L_(6)	(6) Decentralise CS activities by setting up small CS sections in healthcare institutions like hospital and clinics (G-3).
IOM_L_(7)	(7) cybersecurity culture team should assist top management to make sure appropriate cybersecurity related decisions are made (G-3).
IOM_L_(8)	(8) Design proportional and competitive rewards and punishments actions for appropriate and inappropriate CS behaviours that is link to the performance evaluation process (G-2).
IOM_L_(9)	(9) Explain and encourage the top leadership on the importance of quick response time with cybersecurity-related issue and decisions (G-1).
Cybersecurity Governance (G-11)	
IOM_CSG_(1)	(1) Develop a comprehensive but easy-to-follow CS policy with a section that explains what the policy means for employee including their roles and responsibilities concerning CS as well as guidelines for all members of staff to assist with understanding of CS policy (G-7).
IOM_CSG_(2)	(2) Ensure well established security governance structure in the institution like developing and implementing incident response infrastructure to help protect information and the reputation of the institution(G-6).
IOM_CSG_(3)	(3) There should be a well thought out plan on the set-up and management of user restrictions and password management (G-6).
IOM_CSG_(4)	(4) Conduct simulated activities like penetration test and other test excises for an overall assessment of the institution's security defence strength (G-6).
IOM_CSG_(5)	(5) Institution plans in ensuring, managing, and improving CS towards achieving cybersecurity culture should be known by the stakeholders (G-6).

IOM_CSG_ (6)	(6) Monitoring and evaluation of compliance activities by for example: (a) conduct security audits regularly to ensure compliance with industry standards and regulations and manage audit log to keep records, monitor, and manage security event log to assist with recovery plan activities during attack incidents (b) ensure compliance to the activities of other IOM elements like appointment of cybersecurity culture champion, defining of roles and responsibilities of the cybersecurity culture champion, clearly defined and up-to-date cybersecurity policy, and encourage collaboration across departments (c) make staff (particularly new staff) sign a declaration of understanding and compliance for the CS policy of the institution as approve that they have read and understood the policy and will recognise and comply with the institution's CS policy. The declaration should be used in a situation of negligence and non-compliance (G-2).
IOM_CSG_ (7)	(7) Enhance engagement with relevant authorises and parties in the development and management of cybersecurity policy and make sure policy is properly communicated to members of staff (G+3).
IOM_CSG_ (8)	(8) Set up an agreed time (once a year or in two years) when the CS policy is to be re-visited, updated, and communicated to members of the institution. Additionally, make space for ad-hoc updates of CS policy when the need arises (G+4).
IOM_CSG_ (9)	(9) Improve existing CS authentication and restriction activities (G+15).
Business continuity (G-7)	
IOM_BC_ (1)	(1) Ensure continuous CS vulnerability assessment and management activities within the institution (G-9).
IOM_BC_ (2)	(2) Develop, execute, and manage contingency plans (G-6). Examples could include backup, incidents, and disaster response plans.
IOM_BC_ (3)	(3) Conduct risk assessment activities continuously where is lacking to identify possible CS threats, analyse impact on the continuity of operation of the institution, design strategies, execute the strategies, and evaluate the to inform further actions (G-4).
IOM_BC_ (4)	(4) Improve existing risk assessment activities and make it a formal cybersecurity activity of the institution (G+3).
IOM_BC_ (5)	(5) Execute recovery plan during cybersecurity disruptions to ensure continuous operation of essential business functions (G+4). Ensure the recovery plans are tested before execution.
IOM_BC_ (6)	(6) To implement further cybersecurity planning activities set out by the institution (G+5).
Organisational learning (G-3)	
IOM_OL_ (1)	(1) Develop learning and training processes for members of staff at three level individual, department, or group level, and at the system level (G-7)

IOM_OL_ (2)	(2) Establish ways to build and retain CS in the institution by for example: (a) setting up a mentor to guide with CS skills development and training, (b) encourage sharing of CS-related information by creating processes, (c) consult CS experts to assist the cybersecurity culture team with new knowledge, (d) register membership with CS networks for more and the latest information-sharing opportunities (G-4).
Physical security (G+6)	
IOM_PS_ (1)	(1) Implement measures to ensure the protection of data being captured and stored at the institution as well as data being communicated or transferred to prevent data leaks for example using cameras (G+1).
IOM_PS_ (2)	(2) Ensure more protection of server network integrity through network segregation and segmentation (G+2).
IOM_PS_ (3)	(3) improve on the management and protection of physical and remote access to assets like software, hardware, network infrastructure, data, and people (including patients) (G+3).
Communication channels (G+7)	
IOM_CC_ (1)	(1) Reemphasised the channel and network through which CS information and communicate can be generated and circulated which should include channels for reporting detected CS incidents and vulnerabilities (G-4).
IOM_CC_ (2)	(2) Expand on the use of Intranet and/ website as a method of communication (G+2).
IOM_CC_ (3)	(3) Improve on the use of short messages at CS meeting introductions as a channel to promote CS behaviour to support emails communications on CS (G+9).

APPENDIX 5B: PREPAREDNESS AND RESPONSIBILITY ELEMENTS AND RELATED ACTIVITIES

Preparedness and responsibility elements and related activities

Activity ref no	Activities
Cybersecurity competency (G-52)	
P_CSC_ (1)	(1) Assess, create, and document employee's cybersecurity training and education programs, courses, and ensure development of appropriate training and education where it is lacking to safeguard and increase employees' (including ICT staff) cybersecurity abilities (G-36). The assessment should identify levels of employees' cybersecurity education. Subsequently, provision cybersecurity training and education should be prioritized based on employees cybersecurity education.
P_CSC_ (2)	(2) Assess, develop, and grow employees' knowledge and understanding of CS threats in general and threats that particularly attack healthcare institutions (G-20).

P_CSC_ (3)	(3) Identify, define, and ensure employees have knowledge and understanding of national CS policy frameworks including knowledge of their CS policy and related policies (G-5).
P_CSC_ (4)	(4) Create environment to ensure informal CS education among members of staffs where is lacking (G-1).
P_CSC_ (5)	(5) Ensure engagement, involvement, and collaboration in the development of the CS training and education programs (G-1).
P_CSC_ (6)	(6) Ensure institution employee have knowledge of disposal of ICT equipment (G-1).
P_CSC_ (7)	(7) Improve and guild CS informal education and make it acceptable institution practice (G+5).
P_CSC_ (8)	(8) Maintain knowledge of CS related regulations such as Protection Of Personal Information Act (POPIA) (G+7).
Cybersecurity awareness (G-38)	
P_CSA_ (1)	(1) Create and/or increase employee CS awareness on the cognition of: (a) purpose and importance of cybersecurity culture for their institution; (b) CS policies, practices, and procedures of their institution (c) their roles and responsibilities with regards to cybersecurity (d) cyber threats that confront their institutions and various implication of cyber threat incidents (G-34)
P_CSA_ (2)	(2) Increase employees' awareness of their old and new CS practices (G-4).
Communication and information sharing (G-8)	
P_CIS_ (1)	(1) Create a platform that encourage communication, information sharing, and interaction between (G-6).
P_CIS_ (2)	(2) Ensure system of CS incidents record keeping to assist with departmental information sharing (G-4).
P_CIS_ (3)	(3) Improve communication of CS information constantly to the staff using the right channels using intranet and/ website (G+2).
Cybersecurity attitude (G-15)	
R_CSA_ (1)	(1) Motivate for positive mindset towards a culture of CS(G-8).

R_CSA_ (2)	(2) Evaluate and increase staff willingness in the cybersecurity activities of their institution that affect them (G-7).
R_CSA_ (3)	(3) Assesses reasons for resistance to change of old CS attitude and guide against them (G-4).
Cybersecurity behaviour (G+6)	
R_CSB_ (1)	(1) Assess and improve employees' CS behaviour in general (both appropriate and inappropriate) but focus more work on inappropriate ones to correct them (G-6) example of good CS behaviour is to encourage engagement with CS messages, attend CS events, report CS practices of the institution that affect your work.
R_CSB_ (2)	(2) Evaluate the focus or priorities of the institution and its members on CS and initiate change in the right direction (G-6).
R_CSB_ (3)	(3) Identify, define, and simplify the crucial cybersecurity concepts and behaviours according to the CS policy for employees of all ages to easily understand. This should include outlining employees' expected behaviour at the leadership level (G-3).
R_CSB_ (4)	(4) Ensure appropriate behaviour on monetary gain to guide against CS threats (G-2)
R_CSB_ (5)	(5) Evaluate and increase employees' performance and consciousness with the security standards set in the CS policy of their institution (G-1).
R_CSB_ (6)	(6) Continue to examine and maintain employee's cybersecurity actions and activities both official and unofficial that may support defence and protective practices of the institutions (G+24).

APPENDIX_5C: TECHNOLOGY ELEMENTS AND RELATED ACTIVITIES

Technology elements and related activities

Activity ref no	Activities
ICT infrastructure (G-7)	
T_ICTI_ (1)	(1) Map a plan to phase out, improve and/or replace old and outdated IT devices, software, and slow network connections with the latest technology to ensure security (G-3).

T_ICTI_ (2)	(2) Ensure sufficient and appropriate ICT infrastructures and technology that will support cybersecurity practices and activities of the institution (G-2)
T_ICTI_ (3)	(3) Motivate for high ICT budget that makes provision for cybersecurity activities (G-2).
Frequent changes in IT (G-2)	
T_FCIT_ (1)	(1) Plan for software routine updates and maintenance to accommodate constant change to information technology (IT) (G-1).
T_FCIT_ (2)	(2) Motivate for continuous investment in ICT infrastructure to keep up with emerging cyber threats and investment that would encourage more CS awareness and training programs that are up to date with the latest threats due to changing technology (G-1).
Outsourcing of IT systems (G-2).	
T_OITS_ (1)	(1) Check to ensure the outsourced systems meet the standards and outcomes prioritised by the institution (G-1).
T_OITS_ (2)	(2) Conduct assessment and re-assessment occasionally to confirm the cybersecurity requirement of the institution(G-1).

APPENDIX_5D: EENOM ELEMENTS AND RELATED ACTIVITIES

EENOM elements and related activities

Activity ref no	Activities
Legal litigation (G-2)	
EENOM_LL_ (1)	(1) Make sure employees understand the channels of communication and information sharing outside the organisation (G-1).
EENOM_LL_ (2)	(2) educate employee the implication of legal suites on their institution (G-1).
National culture (G-4)	
EENOM_NC_ (1)	Establish and identify the specific national differences or national culture factors that influences (a) technological usage (b) CS values, belief, and ultimately the attitude of employees in the institution (G-4).
Hospital location (G-2)	

EENOM_HL_ (1)	(1) Setup and actively consult external institution to work with for guidance and ideas on the development of CS practices of the institution (G-1).
EENOM_HL_ (2)	(2) Maintain and increase further consultation and consideration of other departments, and sectors for guidance on the improvement of CS practices of their institution (G-1).
Rules and regulation (G+4)	
EENOM_RR_ (1)	(1) Ensure the institution's CS policy complies with the requirements set out by the government laws and regulations. This can help ensure accountability, protection of data, and above all help improve the reputation of the institution (G-5).
EENOM_RR_ (2)	(2) Enhance compliance with healthcare industries and international ethical matters (G+2).
EENOM_RR_ (3)	(3) Continuously check that the CS practices of the institution are in line with other regulations set out like POPIA (G+7).
Reputational damage	
EENOM_RD_ (1)	Create and maintain trust by building: (a) relationship with employee and management to enhance CS compliance (b) confidence in staff CS actions, activities, and intentions (c) open communication of CS incidents and resolution approaches for good reputation of the institution (d) secure access and account management and third-party relationship requirements (G0).

APPENDIX_6: OF CHAPTER 9

APPENDIX_6A: CAPABILITY PROFILE TEMPLATE FOR THE ACTIVITIES OF PREPAREDNESS (P) AND RESPONSIBILITY (R)

Elements	Activities keywords & Groundedness (G)	Present		Intended		Capability gap (CG)	Weight (W)	Priority (W * CG)
		Capability Profile	Maturity	Capability Profile	Maturity			
CS competency	CS training & education [G]	[]	[]	[]	[]	[]	[]	[]
	Knowledge & understanding of CS threats [G]	[]	[]	[]	[]	[]	[]	[]
	Knowledge of national CS policy frameworks [G]	[]	[]	[]	[]	[]	[]	[]
	Informal education [G]	[]	[]	[]	[]	[]	[]	[]
	Collaboration & Engagement CS training [G]	[]	[]	[]	[]	[]	[]	[]
CS awareness	purpose, policy, roles & threats [G]	[]	[]	[]	[]	[]	[]	[]
	Old & new practices [G]	[]	[]	[]	[]	[]	[]	[]
Communication and information sharing	Platform [G]	[]	[]	[]	[]	[]	[]	[]
	CS incident record [G]	[]	[]	[]	[]	[]	[]	[]
	Right channels [G]	[]	[]	[]	[]	[]	[]	[]
CS attitude	Positive attitude [G]	[]	[]	[]	[]	[]	[]	[]
	Staff willingness [G]	[]	[]	[]	[]	[]	[]	[]
	Resistance to change of Old attitudes [G]	[]	[]	[]	[]	[]	[]	[]
CS behaviour	Inappropriate CS behaviours [G]	[]	[]	[]	[]	[]	[]	[]

	CS priorities [G]	[]	[]	[]	[]	[]	[]	[]
	Simplification of CS concept, behaviour & expectations [G]	[]	[]	[]	[]	[]	[]	[]
	Consciousness [G]	[]	[]	[]	[]	[]	[]	[]

**APPENDIX_6B: CAPABILITY PROFILE TEMPLATE FOR THE ACTIVITIES OF TECHNOLOGY
(TECH) ELEMENTS**

Elements	Activities keywords & Groundedness (G)	Present		Intended		Capability gap (CG)	Weight (W)	Priority (W * CG)
		Capability Profile	Maturity	Capability Profile	Maturity			
ICT infrastructures	Legacy system [G]	[]	[]	[]	[]	[]	[]	[]
	Adequate ICT infrastructures [G]	[]	[]	[]	[]	[]	[]	[]
	ICT budget [G]	[]	[]	[]	[]	[]	[]	[]
Frequent changes in IT	Software update & maintenance [G]	[]	[]	[]	[]	[]	[]	[]
	Continuous investment [G]	[]	[]	[]	[]	[]	[]	[]
Outsourcing of IT system	Standards & outcomes [G]	[]	[]	[]	[]	[]	[]	[]
	CS requirement assessments [G]	[]	[]	[]	[]	[]	[]	[]

**APPENDIX_6C: : CAPABILITY PROFILE TEMPLATE FOR THE ACTIVITIES OF EENOM
ELEMENTS**

Elements	Activities keywords & Groundedness [G]	Present		Intended		Capability gap (CG)	Weight (W)	Priority (W * CG)
		Capability Profile	Maturity	Capability Profile	Maturity			
Legal litigation	External communication lines [G]	[]	[]	[]	[]	[]	[]	[]
	Legal implications [G]	[]	[]	[]	[]	[]	[]	[]
National culture	National differences [G]	[]	[]	[]	[]	[]	[]	[]
Hospital location	External connection [G]	[]	[]	[]	[]	[]	[]	[]
	Internal departments [G]	[]	[]	[]	[]	[]	[]	[]
Rules and regulations	Government laws & regulations [G]	[]	[]	[]	[]	[]	[]	[]
	Healthcare industry rules [G]	[]	[]	[]	[]	[]	[]	[]
Reputational damage	Trust [G]	[]	[]	[]	[]	[]	[]	[]

APPENDIX_6D: EXPERT REVIEW QUESTIONS

https://docs.google.com/forms/d/1_P7Y-1LViPFP2nZbD6uqaclbeY1eVeFmO5aqlzAihz0/edit