DEVELOPING A CYBERSECURITY CULTURE FRAMEWORK: A CASE STUDY OF NAMIBIA'S TELECOMMUNICATIONS SECTOR

by

ESTHER NDAPEWA ENDJALA

submitted in accordance with the requirements for
the degree of

MASTER OF SCIENCE

in the subject

COMPUTING

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF. H. ABDULLAH

CO-SUPERVISOR: PROF. M. MUJINGA

AUGUST 2026

DECLARATION

Name: Esther Ndapewa Endjala

Student number: 45163464

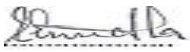
Degree: Master of Science in Computing

I declare that **Developing a Cybersecurity Culture Framework: A Case Study of Namibia's Telecommunications Sector** (title of thesis/dissertation) is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references and that any use of Artificial Intelligence (AI) has been fully disclosed.

I further declare that I submitted the thesis/dissertation to the appropriate originality detection system which is endorsed by Unisa and that it falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

I understand that failure to disclose AI use, plagiarism and/or lack of academic integrity may constitute academic misconduct under Unisa's policies.



13 August 2026

Student Signature

Date

DEDICATION

This work is dedicated to my lovely daughter, Mercia, and my mother, Meme Katrina, for the life lessons they taught me during my studies. My daughter gave me that extra time to work on my studies on weekends throughout this journey. My mother instilled in me the very principles that always help me finish what I have started. Thank you for being my support system when I needed you most.

ACKNOWLEDGEMENTS

I want to thank the **Almighty God** for giving me life, good health and wisdom, which have enabled me to acquire the knowledge necessary to complete my studies.

I am sincerely grateful to my supervisors, Prof. H. Abdullah and Prof. M. Mujinga, for their exceptional guidance, support and encouragement throughout this research journey. Their knowledge and insights have played a vital role in shaping the direction and quality of this work.

I would like to thank my family for their unwavering compassion and support during this thought-provoking journey. Your support and love have been my pillars of strength, keeping me going.

I would like to thank my friends and colleagues who participated in this study and shared their time, insights and experiences. Your contribution is vital to the body of knowledge.

I also would like to express my sincere gratitude to my employer, Mobile Telecommunications Limited, for the study bursary awarded during my studies. The support came at a pivotal moment and greatly enabled the successful pursuit of this qualification.

ABSTRACT

In today's digital environment, where cyber threats are on the rise, organisations face cyber risks that extend beyond technical vulnerabilities. A lack of a cybersecurity culture is often the primary reason why organisational resilience is compromised, as employees' attitudes and behaviours significantly affect the effectiveness of security measures. This study addresses the problem that cybersecurity initiatives in Namibia's telecommunications sector remain largely technical and compliance-driven, while behavioural, organisational and cultural factors that shape secure employee practices are insufficiently understood. Based on these insights, the study seeks to develop a cybersecurity culture framework comprising of six key elements: leadership commitment and support; policy reviews and communication; a Security Education, Training and Awareness (SETA) programme; collaboration and feedback; security champions and ambassadors; and a rewards scheme. A qualitative case study was conducted in a Namibian telecommunications organisation, involving 25 participants purposively selected from across management levels and from IT and non-IT departments. The data were gathered during semi-structured interviews and were analysed thematically. The study's findings reveal key gaps in existing practices, including leaders' passive involvement, inadequate continuous and role-specific training, weak awareness initiatives, and poor reinforcement mechanisms, that impede the development of a proactive security culture. Participants highlighted incentive-based recognition, gamified and tailored training, and security champions as critical enablers of behavioural change. The study contributes to the body of knowledge on organisational cybersecurity by providing context-specific insights to strengthen human-centred defences and by outlining implications for extending this approach to other critical infrastructure sectors that adopt emerging technologies.

KEY WORDS:

Cybersecurity culture, Cybersecurity framework, Cybersecurity governance, Cyber-threats, Employee behaviour, Human-centric security, Human-related cyber risk, Telecommunications sector, Security awareness, Leadership commitment

PUBLICATIONS FROM THIS STUDY

1. Endjala, E., Abdullah, H., & Mujinga, M. 2025. Towards a cybersecurity culture framework: A literature review of awareness and behavioural transformation in telecommunications organisations. In: Yang, XS., 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 1416. Springer, Singapore. https://doi.org/10.1007/978-981-96-6441-2_17

2. Endjala, E., Abdullah, H., Mujinga, M. 2026. Strengthening Cybersecurity Culture for Emerging Technologies: A Case Study of Namibia's Telecommunications Sector. In: Tafuri, B., Kumar, S., Joshi, A. (eds) Machine and Computing Technologies for Sustainable Development. MCT4SD 2025. Lecture Notes in Networks and Systems, vol 1977. Springer, Cham. https://doi.org/10.1007/978-3-032-23716-3_6

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

ABC	Attitudes, Behaviours and Cognitive
CII	Critical Information Infrastructure
CSP	Communications Service Providers
DNS	Domain Name Security
ENISA	European Network and Information Security Agency
ETA	Electronic Transaction Act
GB	Giga Bytes
GSM	Global Systems for Mobile Communications Association
ICT	Information Communication Technology
IS	Information Systems

ISACA	Information Systems Audit and Control Association
IT	Information Technology
ITU	International Telecommunications Union
MICT	Ministry of Information and Communication Technology
NAM-CSIRT	Namibia Cybersecurity Incident Response Team
NIST	National Institute of Standards and Technology
SCT	Social Cognitive Theory (SCT)
TAM	Technology Acceptance Model (TAM)
PPT	People, Process, and Technology
TPB	Theory of Planned Behaviours
PMT	Protection Motivation Theory
SETA	Security Education, Training and Awareness
NTCCF	Namibia Telecommunications Cybersecurity Culture Framework
NIST	National Institute of Standards and Technology
SASE	Secure Access Service Edge
ISO	International Organisation for Standardisation
IEC	International Electrotechnical Commission
GSMA	Global System for Mobile Communications Association
ETSI	European Telecommunications Standards Institute
TIA	Telecommunications Industry Association
SADC	Southern African Development Community

CHAPTER ONE: INTRODUCTION AND BACKGROUND

This chapter provides an introduction and background to the study. Figure 1-1 depicts the layout of this chapter.

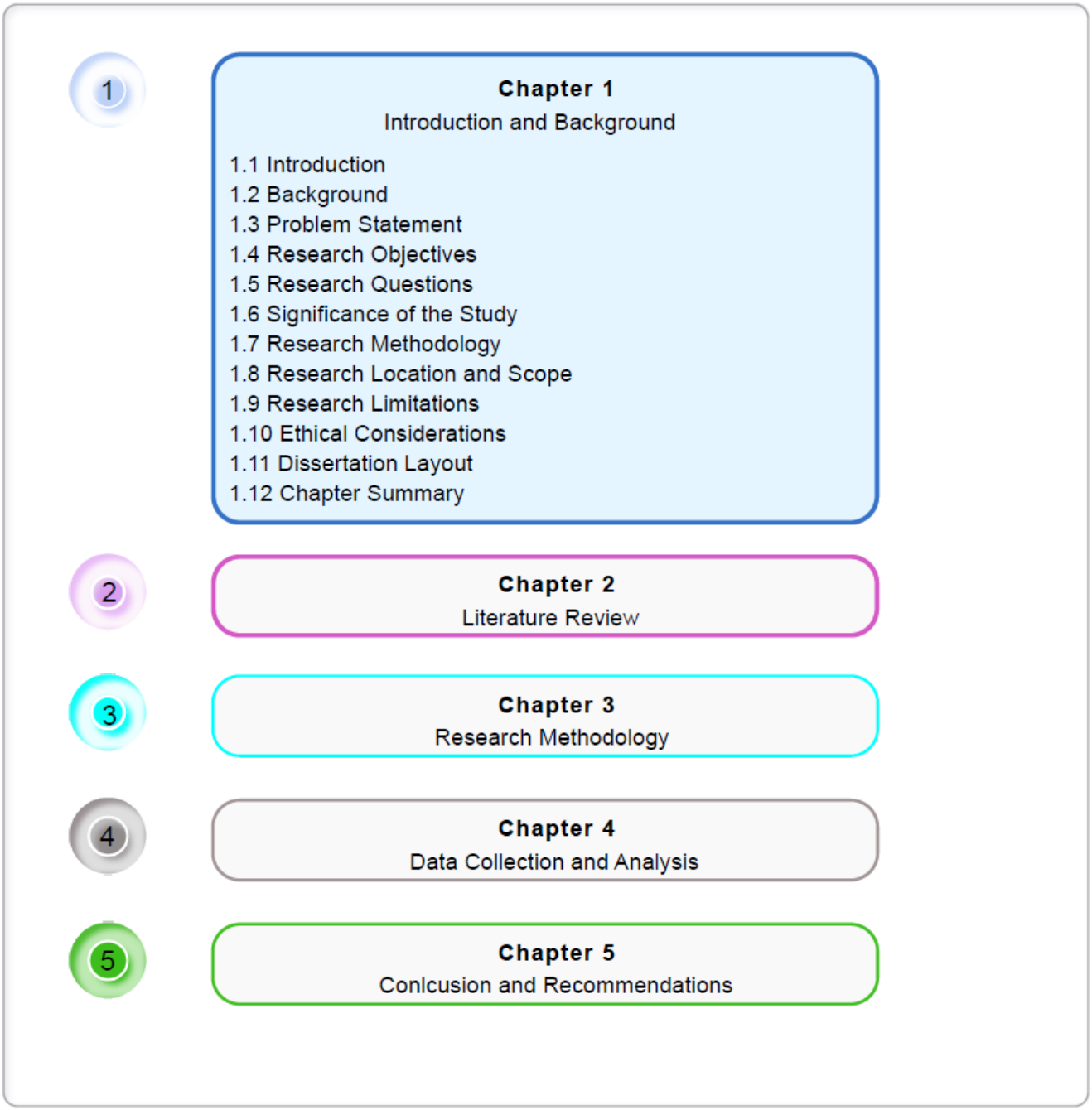


Figure 1-1: Chapter One Layout

1.1 Introduction

Telecommunications organisations play a key role in securing the digital landscape, as they maintain the communications infrastructure that serves millions worldwide, making them prime targets for cybercriminals (Willie, 2023). With the digital transformation progressing rapidly, cybersecurity has emerged as a serious concern for organisations across all industries, as sensitive data and infrastructure are increasingly targeted (Ayyagari & Maru, 2022; Liu, Tian, Li, & Wu, 2024). The growing dependence on digital technologies, which are increasingly exposed to cyber threats such as ransomware, phishing, and data breaches, underlines the need for not only technical defences but also a strong organisational cybersecurity culture (Alavi, Nikou & Kim, 2021).

Cybersecurity culture is more than just rules and technology. It is the responsibility of everyone in the organisation to recognise the importance of cybersecurity and to adhere to security practices every day. An organisation must have a culture that centres on risk awareness, continuous training, enabling policies, and a commitment to best practices to remain safe from cyberattacks (Uchendu, Janczewski & Zhang, 2021). Furthermore, recent studies indicate that building a proactive cybersecurity culture is a multidimensional effort that integrates individual mindsets, leadership commitment, continuous learning, secure behaviour reinforcement and organisational resilience (Uchendu, Nurse, Bada & Furnell, 2021; Delso Vicente et al., 2025; Charalambous, Piki & Stavrou, 2025). Promoting a strong cybersecurity culture in Namibia's telecommunications sector is paramount for safeguarding both the organisation’s data and users' personal information, who rely on these networks. Despite this, most organisations recognise the need to cultivate a cybersecurity culture; however, limited resources, a lack of awareness programmes, and insufficient funding prevent regular training (Baltes & Rees, 2023). The identified limitations in cybersecurity practices expose critical vulnerabilities that must be addressed. Understanding the unique criteria that underpin a long-term, effective cybersecurity culture is crucial to promoting such a culture. This study sought to address existing gaps by developing a comprehensive framework designed to strengthen cybersecurity practices and promote a secure organisational environment. The developed framework aims to transform employees’ attitudes, behaviours, and cognitive skills (ABCs) into a proactive

“human firewall” that would enhance resilience and reduce human-related vulnerabilities within the telecommunications sector.

Additionally, Namibia provides a distinctive context because its telecommunications sector operates as critical national digital infrastructure in a developing economy marked by rapid digitalisation, emerging cybersecurity regulation, limited specialist capacity and increasing dependence on mobile and data services (MICT, 2022; NCSI, 2023). Unlike more mature jurisdictions, Namibia is still strengthening cybersecurity legislation, sector coordination and incident-response maturity, making the telecommunications sector an important setting for examining how cybersecurity culture can be developed under resource, regulatory and capability constraints.

1.2 Background

The telecommunications industry is continually reshaped, becoming a key backbone of global digital interconnection and economic growth. In 2023, there were over 5.6 billion people worldwide, which means around 69% of the total world population, who were mobile service subscribers. This mobile subscriber base was supported by more than 2000 network operators globally (GSMA, 2024). The 5G technology rollout is also playing a significant role in the growth of this vast digital ecosystem, with 1.6 billion 5G connections recorded in 2023 and the number projected to reach 5.5 billion by 2030 (GSMA Intelligence, 2024). In addition, the rapid growth of 5G-enabled Internet of Things (IoT) deployments is projected to substantially increase the number of connected devices within telecommunications networks, thereby expanding the sector’s cyber-attack surface (Ahmed, Sakib, Afrin, Jannat, Taher & Kabir, 2024). While this growth creates significant technological and operational opportunities, it also introduces security, privacy, and scalability risks of the cybersecurity threat surface. Ahmed et al. (2024) caution that interconnected IoT ecosystems can be exploited by malicious actors if organisations fail to implement robust cybersecurity measures, continuous monitoring, and effective governance controls.

Telecommunications companies are prioritising cybersecurity as a key strategic element. The industry has been recognised as one of the most critical operators and maintainers of infrastructure that transmits vast amounts of sensitive data. Security breaches in telecommunications systems may enable malicious actors to exploit the network. It can be noted that from 2022 to 2023, telecommunications companies experienced approximately 77% more cyberattacks (Ogunjinmi, 2025), and the threats have diversified from Distributed Denial of Service (DDoS) attacks and ransomware to Advanced Persistent Threats (APTs). The African telecommunications market is said to be hit the hardest. According to NETSCOUT's threat intelligence data, South Africa and Namibia recorded tens of thousands of cyberattacks targeting wireless carriers in the first half of 2024 alone (Nkosi, 2024).

The rise of digital technology, in turn, has shifted the focus of cybersecurity management from mere technical defences to human factors, thereby incorporating secure behaviours, attitudes, and shared values. Ayyagari and Maru (2022) argue that the integration of cybersecurity culture among employees is a vital human-centred security layer that complements technical controls. However, developing a security culture is challenging in emerging markets such as Namibia, where resource constraints and varying levels of awareness hinder the effective implementation of security measures (Willie, 2023). Technical controls such as firewalls, monitoring tools, access controls and encryption remain essential; however, they cannot fully prevent cyber incidents when employees misunderstand security requirements, bypass controls, fail to report suspicious activity, or lack confidence to respond appropriately (Triplett, 2022; Khadka & Ullah, 2025). Even where additional technical controls are implemented, their effectiveness depends on human interpretation, correct use, timely escalation and organisational reinforcement. Therefore, technical controls must be complemented by a cybersecurity culture that embeds secure behaviour into everyday work practices.

Although the Namibian government introduced the National Cybersecurity Strategy and Awareness Creation Plan in 2023, its implementation has been constrained by pre-existing systemic challenges within the ICT sector as per CRAN Cybersecurity Reports (NAM-CSIRT, 2024). These challenges include shortages of technical expertise and limited organisational

alignment, as identified by Nawa, Chitauro, and Bhunu (2022) prior to the introduction of the strategy. Furthermore, Namibia's ICT sector continues to face challenges originating from the absence of detailed regulatory guidelines and comprehensive strategic cybersecurity frameworks (Waiganjo & Valungameka, 2023). Consequently, many telecommunications service providers continue to take a reactive rather than a proactive approach to cybersecurity, leaving critical information systems vulnerable to attacks and increasing the risk of regulatory non-compliance.

Existing national and sector-related interventions include the National Cybersecurity Strategy and Awareness Raising Plan 2022–2027, the establishment of NAM-CSIRT under CRAN, incident-reporting and response coordination mechanisms, and regulatory encouragement for operators and owners of critical information infrastructure to adopt internationally recognised practices such as encryption, regular security assessments and proactive incident reporting (MICT, 2022; NAM-CSIRT, 2024; The Brief, 2024). However, these interventions remain largely policy, regulatory and incident-response oriented and do not yet provide a sector-specific framework for embedding cybersecurity culture within telecommunications organisations.

Research by Waiganjo, Osakwe & Azeta (2025) confirms that although Namibia's telecommunications sector has grown rapidly, many organisations are ill-equipped to deal with the increasing frequency and complexity of cyber threats. This is compounded by a lack of workforce preparedness and limited cybersecurity training initiatives (Nawa, Chitauro & Bhunu, 2022). Furthermore, Fezzey, Batchelor, Burch, and Reid (2023) claim that the concept of cybersecurity culture in Namibia has not been well developed, and there are a lack of empirical evidence and a fragmented understanding of its possible benefits. The 2023 Deloitte Cybersecurity Survey confirms these results, showing that there are no shared understanding of cybersecurity risks and the strategic value of cybersecurity culture in the Namibian market (Fezzey et al., 2023). Moreover, the lack of effective law enforcement and regulations further complicates the situation, creating significant challenges in establishing a healthy cybersecurity framework (Waiganjo & Valungameka, 2023).

Although human-related vulnerabilities may contribute to cyber risk, they do not automatically indicate a deficient cybersecurity culture. Human error may result from poor system usability, unclear policies, workload pressure, limited training or inadequate communication (Triplett, 2022; Khadka & Ullah, 2025). A cybersecurity culture deficiency exists where organisational norms, leadership practices, reinforcement mechanisms and shared values fail to consistently support secure human behaviour. Liu, Tian, Li and Wu (2024) argue that the absence of consistent legal frameworks and standardised protocols in Namibia undermines the effective management of cyber incidents, leaving organisations with insufficient guidance on how to prevent or respond to cybersecurity threats. Willie (2023) report that even telecommunications service providers with existing cybersecurity policies have experienced recent cyberattacks, underscoring the limitations of policy without practical cultural integration. Despite recent policy-level initiatives, telecommunications organisations in Namibia continue to face significant challenges in embedding cybersecurity awareness and resilience within their operational environments (Waiganjo & Valungameka, 2023). As cyber threats escalate, the absence of regulations and limited organisational readiness underscores the urgent need for a cybersecurity culture framework developed from the ground up. This necessity is particularly critical in the telecommunications sector, where addressing human-related vulnerabilities and fostering proactive security behaviours have become pressing priorities. Without a shared awareness of cyber risks and precise behavioural guidelines for employees, it is inevitable that the continuity of critical infrastructure will be compromised by reactive, disjointed strategies. The present research aimed to bridge this gap by developing a cybersecurity culture framework tailored to the Namibian telecommunications sector. The initiative framework can lead to the adoption of safe habits and fewer cyberattacks, thereby strengthening the organisation and enhancing its resilience through a human-centred strategic approach to managing cyber risks.

Recent cybersecurity incidents in Namibia’s telecommunications sector demonstrate the urgency of the study. In December 2024, Telecom Namibia experienced a ransomware-related data exfiltration incident reportedly involving approximately 626.3GB of data and 492,633 files (The Namibian, 2024; New Era, 2024). Media reports also indicate that Paratus Namibia experienced a separate cybersecurity breach involving approximately 84GB of compromised

data in early 2025 (The Brief, 2025a; The Brief, 2025b). These incidents illustrate that telecommunications operators are exposed to sophisticated threats affecting consumer data, critical infrastructure and public trust.

1.3 Problem Statement

Namibia's telecommunications sector has become increasingly reliant on digital technologies to deliver essential services, exposing it to a growing range of sophisticated cyber threats. Recent cybersecurity incidents affecting Namibian telecommunications operators, including reported data exfiltration and breach incidents involving Telecom Namibia and Paratus Namibia, further demonstrate that the sector faces real and current cyber risks that threaten customer data, operational continuity and public trust. This heightened dependency increases the risk of security breaches, data loss, and operational disruptions, making cybersecurity not only a technical necessity but a strategic imperative for organisational resilience. Although the sector maintains critical infrastructure and processes large volumes of customer data, it remains highly vulnerable to ever-evolving cyber threats that continually expose its overall security posture (Uchendu, 2021). Despite this growing exposure, there is limited evidence of a structured and recognised framework to cultivate a strong cybersecurity culture within the sector. Existing measures tend to prioritise technical controls, while overlooking the critical human factor, which is often the weakest link in cybersecurity resilience (ENISA, 2020). Government initiatives, such as the National Cybersecurity Strategy and Awareness Creation Plan (2023) and the establishment of the National Computer Security Incident Response Team (NAM-CSIRT), represent progress; however, implementation at the organisational level remains limited (Waiganjo et al., 2025). These interventions demonstrate that efforts have been made to strengthen cybersecurity coordination, awareness and incident response in Namibia; however, they remain largely policy and response oriented and do not provide a sector-specific organisational framework for embedding cybersecurity culture within telecommunications organisations. Furthermore, national guidelines such as the Common Minimum Standards of Protective Security Measures (Government of the Republic of Namibia, 1996) were designed for manual-based systems and traditional security controls, limiting their relevance in contemporary digital environments. These legacy guidelines inadequately address the

behavioural and cultural dimensions of cybersecurity, which are essential for fostering proactive cyber risk management. Consequently, their continued use perpetuates reactive security practices and weakens the development of a sustainable cybersecurity culture among telecommunications service providers. While human-related vulnerabilities may contribute to cybersecurity risk, they do not automatically indicate a deficient cybersecurity culture; rather, the problem lies in the limited organisational controls for consistently reinforcing secure behaviour, awareness, accountability and human-centred governance. Therefore, the problem is not merely the absence of technical controls, but the limited integration of technical controls with human-centred governance, awareness, accountability and behavioural reinforcement (Triplett, 2022; Khadka & Ullah, 2025). Without this integration, organisations may continue to invest in security technologies while employees remain insufficiently prepared to recognise, interpret and respond to cyber risks in their daily operations.

1.4 Research Objectives

The main objective of this study was to develop a cybersecurity culture framework that addresses human-related vulnerabilities and strengthen organisational resilience within Namibia's telecommunications sector. This main objective is further divided into the following sub-objectives:

RO1: To identify the key organisational, human, and governance requirements for an effective cybersecurity culture framework within the telecommunications sector.

RO2: To develop the core components and characteristics of an effective cybersecurity culture framework suitable for Namibia's telecommunications sector.

RO3: To refine and present a cybersecurity culture framework for Namibia's telecommunications sector.

In this study, framework development is understood as a staged process in which RO1 identifies the organisational, human and governance requirements, RO2 develops the core components and characteristics of the framework, and RO3 refines and present the framework through empirical insights from the case study organisation.

1.5 Research Questions

The main research question for this study is: How can a cybersecurity culture be improved to address human-related vulnerabilities, strengthen organisational resilience, and enhance cybersecurity awareness within Namibia's telecommunications sector? This main research question is further divided into the following sub-questions:

RQ1: What organisational, human, and governance requirements are necessary for an effective cybersecurity culture framework within the telecommunications sector?

RQ2: What core components and characteristics define an effective cybersecurity culture framework suitable for Namibia's telecommunications sector?

RQ3: How to develop a cybersecurity culture framework for Namibia's telecommunications sector?

In alignment with the research objectives, RQ1 explores the organisational, human and governance requirements that inform the foundation of the framework, while RQ2 examines the core components and characteristics required for an effective cybersecurity culture framework. RQ3 then integrates this literature derived and empirically informed elements to explain how the cybersecurity culture framework is developed for Namibia's telecommunications sector in Chapter Four.

1.6 Significance of the Study

Namibia's telecommunications sector can become more resilient to cyberattacks through a study that focuses on the human dimension of cyber risk factors. Given the sector's role as the primary national digital infrastructure, it is indispensable to raise cybersecurity awareness and establish a strong security culture to protect private data, ensure uninterrupted service, and earn public trust. The study offers a real-world benefit by presenting a well-organised telecommunications business model to guide the establishment and rollout of cybersecurity culture programs. It can help mitigate human-caused vulnerabilities, increase workers' interest in security practices, and facilitate compliance with both the company's rules and national

regulatory frameworks, such as the National Cybersecurity Strategy and the NAM-CSIRT framework.

While Namibia has introduced national cybersecurity interventions such as the National Cybersecurity Strategy and Awareness Raising Plan 2022–2027 and NAM-CSIRT under CRAN, these initiatives primarily strengthen national coordination, incident reporting, awareness raising and response capacity (MICT, 2022; NAM-CSIRT, 2024). The significance of this study lies in extending these policy and regulatory interventions into an organisational-level, sector-specific cybersecurity culture framework that can guide telecommunications organisations in embedding secure behaviour, leadership accountability, training, communication, reporting and behavioural reinforcement into daily operations. The urgency of this intervention is reinforced by recent cyber incidents affecting Namibian telecommunications operators, including large-scale data exfiltration and reported breaches involving sensitive customer and organisational information (The Namibian, 2024; The Brief, 2025b). These incidents demonstrate that cybersecurity culture is not a theoretical concern, but an immediate organisational resilience priority for protecting consumer trust, critical infrastructure continuity and national digital confidence.

Moreover, the results of this study can help policymakers, industry stakeholders, and cybersecurity practitioners understand the context-specific challenges and opportunities in cybersecurity culture across markets. The preliminary framework is a diagram illustrating how to integrate the behavioural, organisational, and strategic elements of cybersecurity to achieve sector-wide resilience. From an academic perspective, the study addresses a gap in the existing literature on cybersecurity culture in the African telecommunications sector. It serves as a source of both theory and practice by deepening understanding of how security awareness, leadership, training, and organisational values coalesce to mitigate cyber threats in high-risk digital sectors.

1.7 Research Methodology

The study used a qualitative single-case study design with an interpretivist orientation as its primary approach and considered the 'research onion' framework of Saunders, Lewis, and Thornhill (2023) as a guide. The research onion framework, which employs a context-sensitive qualitative orientation, is well-suited to examining the cultural aspects of cybersecurity in the real-world context of a telecommunications organisation in Namibia. It enabled the researcher to understand how cybersecurity-related behaviours, values, and practices are embedded in daily organisational life (Hammersley & Atkinson, 2019; Saldaña, 2022). The study does not claim full ethnography because it did not involve long-term immersion or sustained participant observation. The research design comprises layered elements, including research philosophy, approach, methodological choice, strategy, time horizon, and data collection and analysis methods. This framework helps organise research clearly, beginning with philosophical assumptions and progressing through data collection methods. Figure 1-2 illustrates the research onion layers, and each layer is briefly outlined below while discussed in detail in Chapter Three.

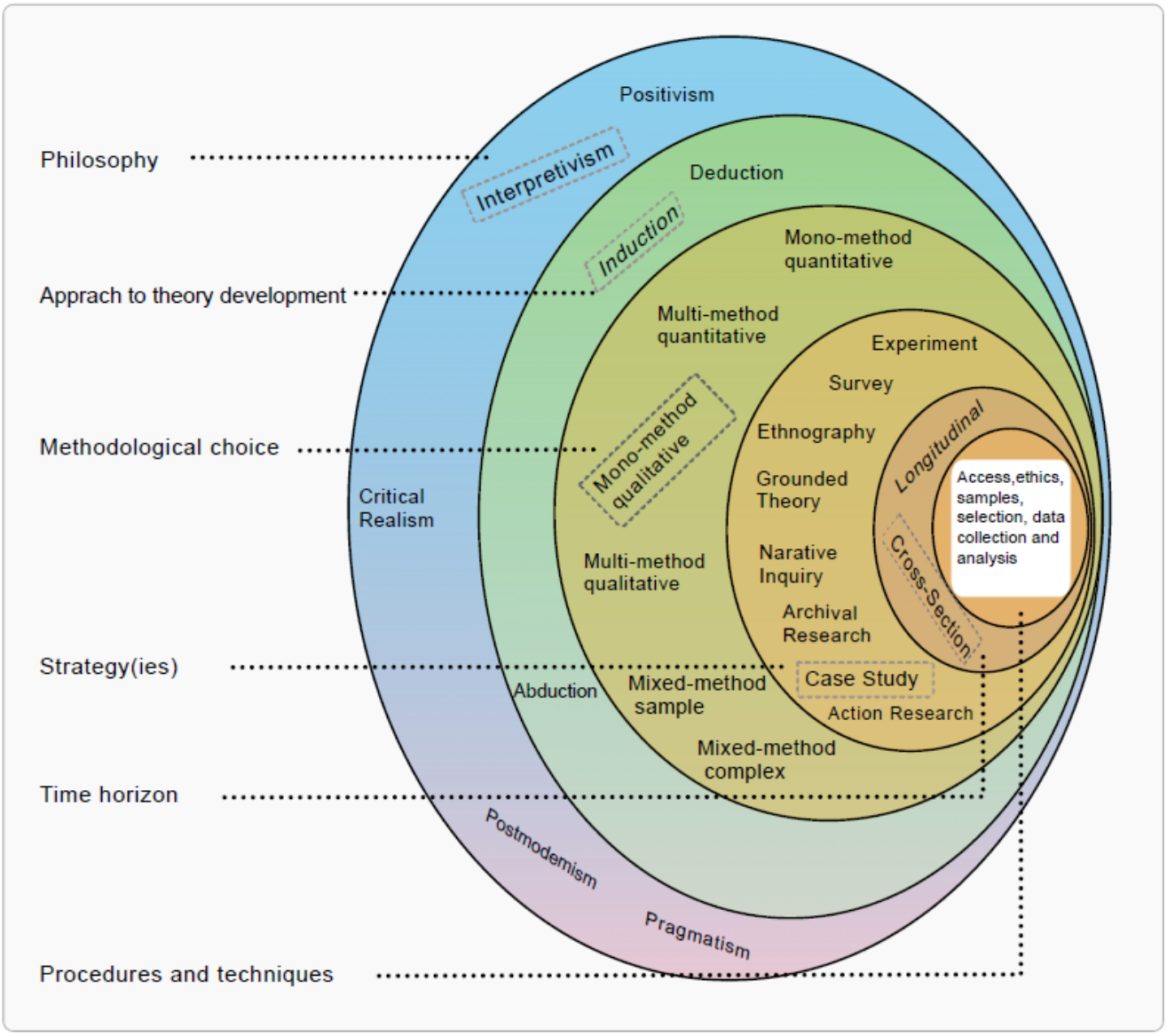


Figure 1-2: Research Onion

Source: Saunders et al., (2023)

1.7.1 Philosophy

This study is grounded in interpretivism, a philosophy that emphasises understanding the subjective meanings individuals assign to their experiences within specific social and organisational contexts (Saunders et al., 2023). Interpretivism is appropriate given the study's objective of exploring perceptions, behaviours, and organisational practices that influence

cybersecurity culture in a real-world setting. Therefore, this position aligns with the study's aim of exploring how employees perceive and engage with workplace cybersecurity culture.

1.7.2 Approach to Theory Development

The study employed an inductive approach whereby the theory is derived from the data rather than leading hypothesis testing. The approach enabled the researcher to construct a conceptual framework based on patterns identified in the empirical data (Saunders et al., 2023). Such a method was suitable and aligned with the study of phenomena that have received little research, for example, cybersecurity culture in Namibia's telecommunications sector.

1.7.3 Methodological Choice

The study adopted a qualitative monomethod approach, relying on a single data collection technique and analysis method (Saunders et al., 2023). In this case, data were gathered using semi-structured interviews with key stakeholders in the telecommunications sector. Qualitative data was used to explore participants' lived experiences and organisational dynamics related to cybersecurity culture. This choice supported the study's interpretivist and context sensitive qualitative orientation. Semi-structured interviews support an in-depth exploration of participants' perceptions, experiences and organisational practices related to cybersecurity culture within the selected telecommunications organisation. However, the study does not claim a full ethnographic design, as it did not involve prolonged immersion, sustained participant observation or long-term field engagement. Instead, the study is positioned as a qualitative single-case study with a context-sensitive qualitative orientation, consistent with interpretivist case study research (Creswell & Poth, 2018; Yin, 2018).

1.7.4 Strategy

A single-case study design was employed, focusing on a single telecommunication organisation in Namibia. Saunders et al. (2023) state that the case study technique allows researchers to explore a phenomenon in its natural setting, particularly when the limits of the phenomenon within its environment are unclear. In this study, a case study was used to gain

an in-depth understanding of the organisational and environmental factors that affect cybersecurity culture. This approach provided detailed, in-depth data on the unique cultural and operational contexts of the chosen organisation (Yin, 2018).

1.7.5 Time Horizon

A cross-sectional time horizon, according to Saunders et al. (2023), is defined as the collection of data at a specific point in time rather than across a longer period. In line with this strategy, this study used a cross-sectional design to examine the level of cybersecurity culture and practices within the chosen telecommunications organisation during the study period.

1.7.6 Procedures and Techniques

This subsection outlines the procedures followed for data collection and the techniques used for data analysis in the study. The data collection procedure involved the use of semi-structured interviews, supported by purposive sampling to identify participants with relevant knowledge and experience in cybersecurity within the telecommunications context. This approach ensured the inclusion of rich information participants across IT staff, non-IT staff and management. The primary analytical technique employed was thematic analysis, which enabled the systematic identification and interpretation of recurring patterns and themes within the interview data. This technique facilitated the organisation of the empirical findings into themes that directly addressed the study's objectives (Saldaña, 2022; Saunders et al., 2023).

The use of semi-structured interviews supports a context sensitive qualitative orientation that guides researchers in exploring the context-specific cultural and behavioural aspects of cybersecurity practice within the organisation. Semi-structured interviews support an in-depth exploration of participants' perceptions and organisational practices, but they do not constitute full ethnography in the absence of prolonged immersion or sustained participant observation. Collectively, these procedures and techniques enabled participants across different organisational roles, to bringing to light real-life practices and contexts in which the whole idea of a cybersecurity culture is a challenge that can be turned into an opportunity by developing a practical, context-specific model of a human-centric cybersecurity resilience framework.

1.8 Research Location and Scope

The current study reviews the telecommunications industry in Namibia, which is undergoing rapid digitalisation and is experiencing limited human-centric cybersecurity interventions, thereby increasing its exposure to cyber threats. This industry is an essential component of the national communication infrastructure and processes large volumes of highly sensitive data, making it a highly attractive target for cyberattacks. The study was conducted within a leading telecommunications organisation in Namibia. This non-probability sampling technique was chosen because the selected organisation possesses specific characteristics. These are large-scale operations, high digital maturity, and centrality to the national telecommunications infrastructure. Such features align well with the study's objectives. Given these features, the case was particularly relevant to the study of the development of a cybersecurity culture framework in industry. By engaging directly with staff involved in both day-to-day operational activities and decision-making, the study gained contextualised insights into the behaviours, values, and practices that constitute cybersecurity culture.

1.9 Research Limitations

Although this study aims to contribute to the understanding and development of a cybersecurity culture framework within Namibia’s telecommunications sector, several limitations must be recognised. Firstly, the study was limited to a single case study within a single major telecommunications organisation, which may limit the generalisability of the findings to other sectors or even other organisations within the same sector.

Secondly, the study relied on qualitative data gathered through semi-structured interviews, which are inherently subjective and may introduce response bias, as participants may provide socially desirable answers rather than reflect actual behaviours and perceptions. Additionally, the cross-sectional approach captured cybersecurity culture at a single point in time, limiting insight into how it may evolve over time or in response to emerging threats. Finally, given the rapidly evolving cybersecurity landscape and technological advancements, the relevance and applicability of the developed framework may be affected by future developments. However, the findings provide context-specific insights that can inform practical interventions and future

research to develop human-centric cybersecurity resilience within the telecommunications sector.

1.10 Ethical Considerations

This study strictly conformed to ethical research standards throughout the study. Ethical approval was obtained from the University of South Africa (UNISA) Research Ethics Committee prior to data collection. The ethical clearance certificate, which authorised the commencement of data collection, is attached as Appendix A. Ethical considerations are essential to protect research participants and to ensure that they are not exposed to any form of harm, whether physical, psychological, or emotional (Bell, Bryman & Harley, 2022). Furthermore, the study obtained formal permission from the organisation's management, with a gatekeeper providing access to the organisation's study environment. This permission was obtained and is documented in Appendix B.

Each participant received a consent form to review and sign, indicating their voluntary agreement to participate. Evidence of signed consent forms is provided in Appendix C, which shows that participants understood their participation and were adequately protected throughout the study. Although complete anonymity may not always be possible in qualitative research, particularly when follow-up interviews are required, the researcher is committed to upholding confidentiality. No identifying information was linked to participants in the final research results, and all personal data collected was anonymised during both the analysis and reporting phases using pseudocode. To protect the collected data, stringent security measures were implemented. All electronic data was encrypted and stored on password-protected systems, while physical documents were kept in secure, access-controlled locations. Adhering to ethical standards throughout the study ensured that participants' rights, dignity, and privacy were protected at every stage.

1.11 Dissertation Layout

This dissertation is structured into five chapters, each addressing a specific aspect of the research process, as outlined below and illustrated in Figure 1-3.

Chapter One provides an overview of the study by presenting the background to the research problem, the problem statement, the main aim and objectives of the study, the research questions and the significance of the research.

Chapter Two outline a critical review of existing literature relevant to cybersecurity culture. It synthesises current theoretical and empirical studies to establish the conceptual foundation for the study and to inform the development of the preliminary cybersecurity culture framework.

Chapter Three provides the research methodology adopted in the study, including the research design, target population and sampling strategy, data collection instruments, data analysis techniques, validity and reliability considerations, ethical issues and limitations of the study.

Chapter Four presents and analyses the empirical findings of the study. The results are interpreted in relation to the research objectives and discussed within the context of the reviewed literature.

Chapter Five concludes the study by summarising the key findings, drawing conclusions aligned with the study objectives and presenting recommendations. Areas for future research are also identified. Figure 1-3 illustrates the overall structure of the dissertation.

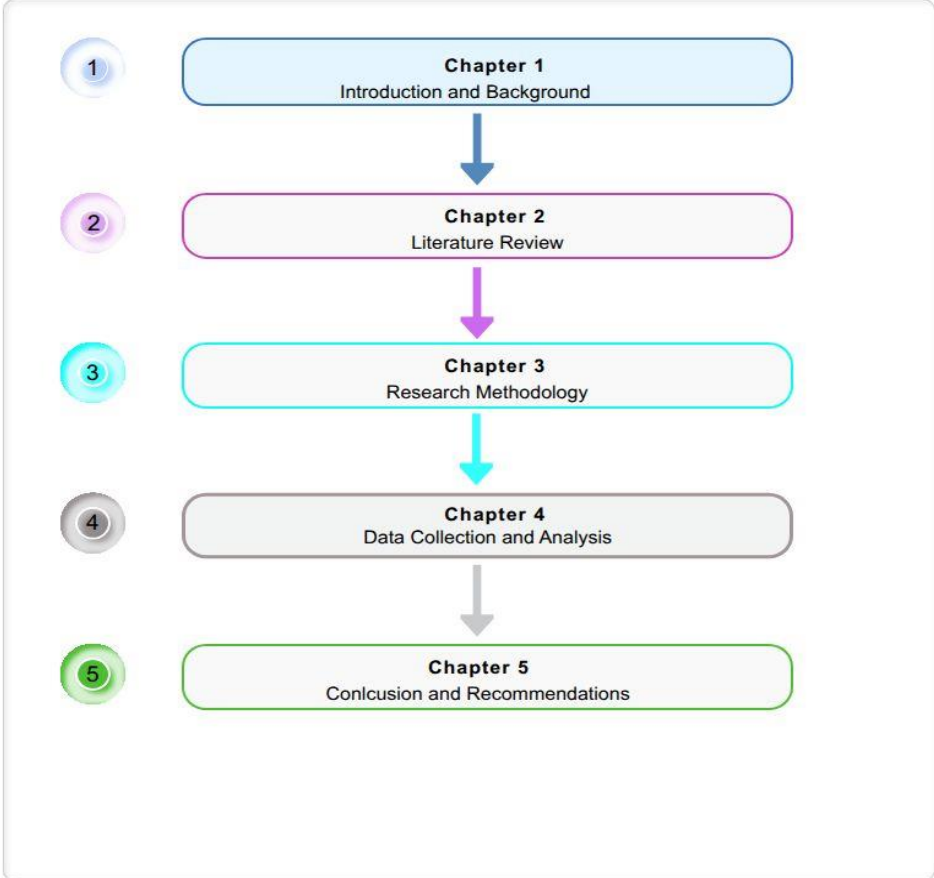


Figure 1-3: Dissertation Chapter's Layout

1.12 Chapter Summary

This chapter provided an overview of the study's overall context, from the problem statement to the research objectives, within Namibia's telecommunications sector. It outlined the evolving threat landscape and the human factors that contribute to cybersecurity vulnerabilities, thereby justifying the need for a contextualised cybersecurity culture framework. The chapter also outlined the study's significance, particularly its potential to strengthen the cybersecurity posture of Namibian telecommunications organisations and to contribute to global efforts to mitigate cyber threats. It further concluded with a rationale for the study's approach and scope. Chapter Two presents a literature review that provides a theoretical foundation for understanding the current state of cybersecurity culture and informs the development of the preliminary framework.

CHAPTER TWO: LITERATURE REVIEW

This chapter provides a comprehensive overview of the literature on cybersecurity culture in the telecommunications sector. Figure 2-1 depicts the layout of this chapter.

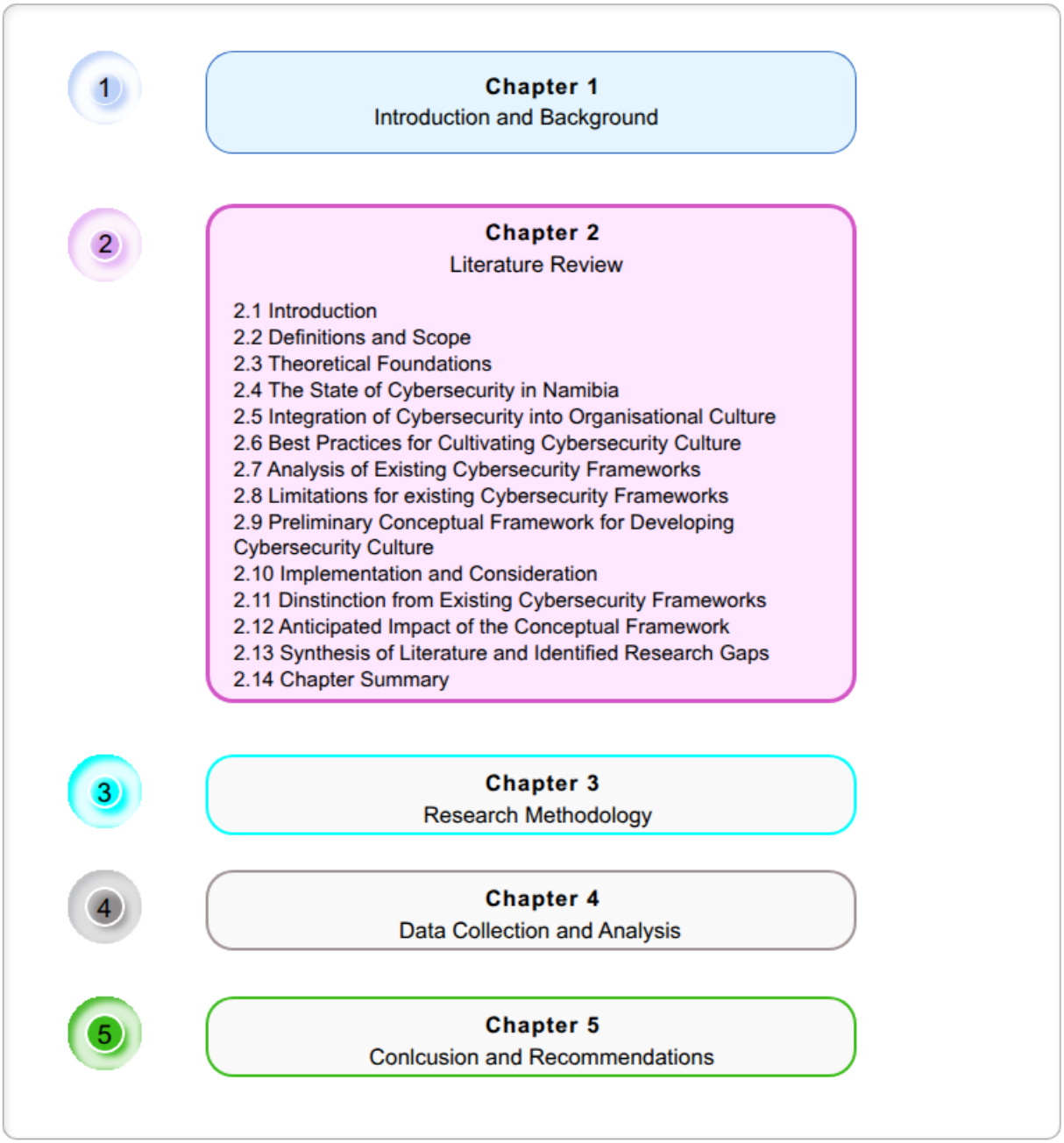


Figure 2-1: Chapter Two Layout

2.1 Introduction

In this chapter, a foundational understanding of the cybersecurity culture is provided by defining the concept and explaining its relevance within organisational settings. It presents a comprehensive review of the current literature to assess how cybersecurity culture is characterised and shaped across different organisational and geographical contexts, with a particular attention to the Namibian telecommunications sector. The chapter also analyses existing international and sector-specific cybersecurity frameworks to determine their strengths, limitations, and relevance for cultivating secure behaviours in the workplace.

In doing so, this chapter addresses the overarching objective of the literature review: to identify conceptual, practical, and contextual gaps in existing studies and frameworks, to translate these gaps into the key components that will inform the development of the preliminary cybersecurity culture framework for this study. These insights lay the groundwork for the empirical investigation presented in Chapter Four and guide the formulation of constructs to be assessed through data collection.

2.2 Definitions and Scope

2.2.1 Cybersecurity

Cybersecurity is an umbrella term that encompasses the processes, technologies, and practices used to protect information assets, computer systems, networks, and services from unauthorised access, malfunction, modification, or destruction (ENISA, 2023). Cybersecurity involves a variety of technical and organisational measures that protect confidential information, maintain its integrity, and ensure its availability. The National Institute of Standards and Technology (NIST, 2022) defines cybersecurity as a set of practices aimed at preventing information systems from being accessed by unauthorised persons, disrupted, stolen, or damaged. Although technical controls are crucial, recent studies emphasise the critical role of the human element in the cybersecurity ecosystem (Alshaikh, 2020). Today, cybersecurity extends beyond installing protective measures; it also requires establishing governance frameworks, implementing risk management methods, and undertaking human-centred activities to enhance an organisation's cyber resilience (Khadka & Ullah, 2025; NIST, 2024).

Employees' behaviour, actions, and awareness levels can significantly impact the organisation's security. Hence, for this research, cybersecurity is treated as a socio-technical field that acknowledges that the effectiveness of security controls depends not only on technology but also on the behaviour, attitudes, and skills of the organisation's members.

2.2.2 Cybersecurity Culture

The term "cybersecurity culture" refers to the shared values, attitudes, behavioural patterns, norms, and beliefs that shape how individuals within an organisation understand, engage with, and prioritise cybersecurity risks and regulations (Uchendu et al., 2021). Incorporating security thinking into daily work processes extends beyond formal compliance. One of the main characteristics of a robust cybersecurity culture is the presence of top management commitment, employee awareness, voluntary incident reporting, and ongoing compliance with security policies and procedures (Alshaikh, 2020). Alshaikh also highlights that a strong, healthy cybersecurity culture is necessary to recover from disruptive events and to mitigate human-related risks. Within the framework of this research, cybersecurity culture is viewed as a combined behavioural and organisational construct that reflects factors such as leadership behaviour, employee training and awareness, communication flows, policy enforcement, and the usability of security technologies. According to recent research, organisational cybersecurity approaches can generally be distinguished between compliance-driven and culture-based approaches. Compliance-driven models tend to focus on adherence to prescribed rules, procedures, standards and policy requirements, often supported by monitoring, audits, sanctions or disciplinary consequences for non-compliance (Hanus & Wu, 2021; ISO/IEC, 2022; NIST, 2024). In contrast, culture-based approaches promote proactive cybersecurity behaviour in, personal accountability, shared responsibility, continuous learning and motivational reinforcement as part of everyday organisational practice (Uchendu et al., 2021; Delso Vicente et al., 2025).

According to ENISA (2021), an established cybersecurity culture facilitates shared accountability among all staff, from senior management to frontline staff. This collaborative strategy enhances an organisation's ability to detect, prevent, and respond effectively to cyber

threats. Telecommunications, as a strategic enabler of digital trust and operational continuity, is also gaining more widespread recognition within the sector (Sadiku, Adekunte & Sadiku, 2024). For this study, cybersecurity culture is defined as the common organisational mindset, norms, and procedures that promote proactive cyber risk management and safe use of technology. These definitions emphasise that cultivating a positive cybersecurity culture requires both organisational structures and mechanisms for individual behavioural change.

These areas of focus align with the study objectives, which are to identify the key factors influencing cybersecurity culture in the Namibian telecommunications sector and to translate these factors into measurable elements to develop a preliminary cybersecurity culture framework. The next chapter examines behavioural and cognitive theories that underpin the development of cybersecurity culture in organisations.

2.3 Theoretical Foundations

This study is informed by four behavioural and organisational theories that offer different perspectives on how individuals and groups engage with cybersecurity practices: Social Cognitive Theory (SCT), Protection Motivation Theory (PMT), the Theory of Planned Behaviour (TPB), and the Technology Acceptance Model (TAM). These theories are not applied in the operational sense of being fully adopted as a measurement framework. Instead, these theories serve as conceptual lenses that guide the interpretation of existing research and help identify behavioural constructs relevant to understanding and shaping cybersecurity culture within an organisational context. The subsections below discuss the relevance and contribution of each theory to the literature informing this study.

2.3.1 Social Cognitive Theory

Social Cognitive Theory (SCT) is based on learning that occurs through observation, modelling, and reinforcement of safe skills. It further posits that human behaviour results from the dynamic interaction between personal factors, environmental influences, and behavioural reinforcement (Uchendu, Nurse, Bada & Furnell, 2021). This triadic reciprocal determinism suggests that in a telecommunication organisation, an employee’s security actions are equally shaped by their

internal beliefs and the external organisational policy environment. Previous studies have used SCT to explain how leadership modelling, organisational norms, and social influence drive employee security practices (Uchendu et al., 2021). SCT emphasises the importance of organisational leadership and policy as critical enablers of safe behaviours, where leaders who demonstrate a commitment to cybersecurity through actions such as active participation in training, promoting best practices, and endorsing organisational security policies that serve as role models influence employees to emulate these behaviours (Willie, 2023). This reciprocal relationship among individuals, their environment, and behaviour reinforcement promotes an organisational culture that supports security awareness and compliance (Delso-Vicente et al., 2025). SCT is therefore valuable for understanding how leadership commitment, peer influence, and organisational expectations contribute to the formation and strengthening of cybersecurity culture within telecommunications organisations.

2.3.2 Protection Motivation Theory

The Protection Motivation Theory (PMT) focuses on how individuals cognitively assess threats and develop protective behaviours based on their perception of risk and coping ability (Alshaikh et al., 2021). PMT has been widely used in the information security sector to examine how the workforce's views on cyber threats, seriousness, susceptibility, and self-confidence influence subsequent security regulations, as well as to consider secure behaviours (Fezzey et al., 2023). Within the organisational environment, PMT is relevant for understanding how employees interpret cyber threats. It primarily informs the literature synthesis rather than the empirical design, ensuring that the threat-based behaviours drive a conceptually acknowledged understanding without dominating the study’s qualitative framework.

2.3.3 Theory of Planned Behaviour

The Theory of Planned Behaviour (TPB) has been widely applied to explain the intentional security behaviour by emphasising attitudes toward the behaviour, subjective norms, and perceived behavioural control (Delso-Vicente et al., 2025). In the telecommunications sector, these factors determine whether an employee’s intention to follow security procedures translates into actual compliance. In organisational cybersecurity studies, TPB helps to explain

why employees choose to comply with or deviate from security protocols based on their beliefs, perceived expectations, and confidence in their ability to act securely (Willie, 2023). When employees intend to comply with cybersecurity policies, favourable attitudes towards cybersecurity, coupled with peer support and adequate training, increase the likelihood that employees will act securely (Fezzey et al., 2023). This theory provides a strong foundation for exploring behavioural intentions and organisational influences that directly relate to cybersecurity culture.

2.3.4 Technology Acceptance Model

The Technology Acceptance Model (TAM) posits that perceived usefulness and ease of use are key determinants of technology acceptance. It is beneficial to understand the adoption of security tools and systems in organisations (Granić & Marangunić, 2024). According to TAM, two key factors, perceived usefulness and perceived ease of use, drive users' attitudes toward using a system, which in turn affect their behavioural intention. Cybersecurity researchers have used TAM to assess why employees adopt or circumvent security tools when these tools are perceived as complex or burdensome (Granić & Marangunić, 2024). Furthermore, explaining the benefits of these solutions, such as increased data protection and a lower chance of breaches, increases perceived usefulness and encourages staff members to incorporate these controls into their existing workflows. Although TAM offers variable insights into the technological dimensions of cybersecurity culture, it is not used to structure the empirical phase of this study to avoid unnecessary theoretical complexity.

These theories provide a robust framework for understanding the psychological and behavioural drivers of a cybersecurity culture. Figure 2-2 illustrates the interconnected theories that progress from the broadest to more specific frameworks, addressing behaviours, technology adoption, and cybersecurity practices, thereby organising them logically to support the study. This sequence begins with Social Cognitive Theory (SCT) as the broad foundation, leading into Protection Motivation Theory (PMT), which narrows the focus to behaviours in response to threats. The Theory of Planned Behaviour (TPB) provides further insights into why

individuals may or may not engage in protective cyber behaviours. Finally, the Technology Acceptance Model (TAM) directly addresses the adoption of cybersecurity technologies.

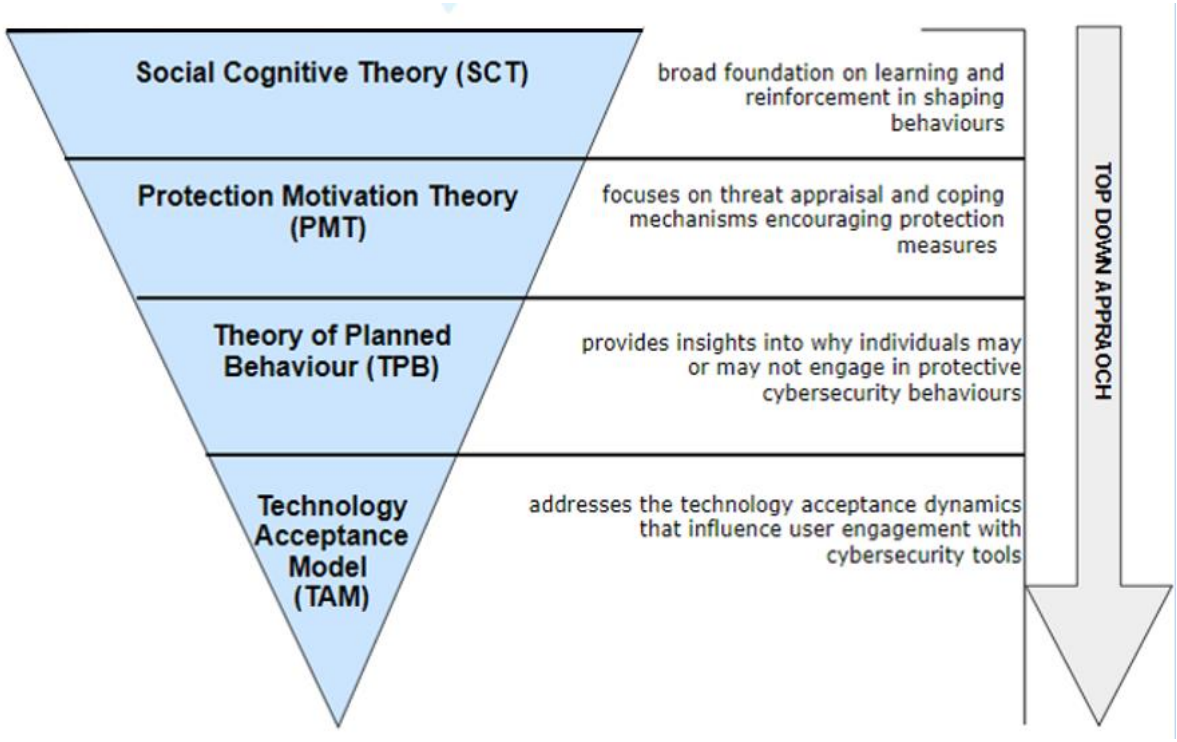


Figure 2-2: Behavioural Theories of Cybersecurity Culture Integration

The figure illustrates the top-down approach, following the sequence of these theories to ensure a logical progression from general principles of human behaviours to specific theories regarding security behaviours and technology acceptance.

2.3.5 Selection of Theoretical Perspectives for this Study

Although this study reviewed SCT, PMT, TPB, and the TAM to frame behavioural and organisational dimensions of cybersecurity culture, only SCT and PMT are considered to inform the development of the interview guide and the subsequent data analysis. These two theories were chosen because they offer strong explanatory power for understanding the behavioural, cognitive, and organisational dynamics relevant to cybersecurity culture within the Namibian telecommunications sector.

SCT provides a foundation for exploring how leadership modelling, organisational learning, communication, and reinforcement mechanisms influence employees' cybersecurity behaviours. While PMT complements SCT by explaining how employees perceive cyber threats and assess their capability to respond, which aligns closely with the study's focus on awareness, perceived vulnerabilities, coping appraisal, and behavioural intentions. Together, these theories provide an integrated analytical lens for interpreting participants' interview data and support the identification of behavioural and cultural factors influencing cybersecurity practices. Hence, guiding both data collection and thematic analysis in this study.

In contrast, while TPB and TAM remain relevant to broader behavioural and technology adoption research, they are not operationalised in the data collection. The TPB conceptually overlaps with constructs already covered by SCT and PMT, and TAM is more applicable to studies evaluating the acceptance of specific technologies rather than to studies of organisational culture. Hence, these theories remain part of the theoretical landscape for contextualising the study but are not applied to data collection. This intentional narrowing of focus ensures that the study remains methodologically consistent, avoids excessive theoretical layering, and maintains a clear connection between the study's conceptual foundation and its qualitative research design. Collectively, these theoretical lenses strengthen the literature synthesis and guide the identification of key constructs that will later inform the development of the provisional cybersecurity culture framework.

The following section identifies and discusses the best practices and strategies reported in the literature that influence cybersecurity culture within organisations.

2.4 The State of Cybersecurity in Namibia

Namibia, like other developing countries, is bringing digital technologies into its public and private sectors. This transformation is making the country's national systems vulnerable to evolving cybersecurity risks. Despite significant progress in building ICT infrastructure and improving digital accessibility, the overall level of cybersecurity maturity in Namibia remains quite low (Waiganjo, Osakwe & Azeta, 2025). The country's poor performance in this respect

is largely attributable to the absence of a comprehensive policy framework, limited public awareness, and weak investment in cybersecurity capabilities (Nawa et al., 2022). Namibia has only a draft electronic transactions and cybercrime bill, which, among other provisions, authorises the government to monitor and/or verify the agencies that require access to sensitive data (Waiganjo & Valungameka, 2023).

Recent research indicates that while Namibia has made notable strides in expanding digital access and infrastructure, the country is not adequately equipped to address cyber threats. The Global Cybersecurity Index identifies severe deficiencies in the legal, technical, and organisational aspects of Namibia's security framework, thereby exposing the country to threats such as ransomware, banking malware, and large-scale data breaches. There are various proactive measures, such as capacity building, awareness creation, and international cooperation, that are highlighted in the National Cybersecurity Strategy and Awareness Creation Plan 2022–2027. Nevertheless, ongoing difficulties in protecting the country’s critical infrastructure indicate a low level of cybersecurity maturity (Waiganjo et al., 2025). It is therefore imperative to address these weaknesses if Namibia is to make significant progress in its cybersecurity sector.

There is no guiding legislation for the current bill due to the absence of comprehensive cybersecurity laws, rapid technological evolution, uncertainties in the legal framework, and jurisdictional issues. Puteho, Gamundani and Nhamu, (2022) argue that inadequate enforcement of existing laws has made Namibia a hub for international cybercrime. According to the Ministry of Information, Communication, and Technology (MICT), Namibia has established a National Computer Security Incident Response Team (CSIRT) called NAM-CSIRT. This entity serves as the country's primary body for managing cybersecurity incidents and responses. NAM-CSIRT operates under the Communications Regulatory Authority of Namibia (CRAN) and is tasked with enhancing the nation's cyber defence capabilities. It serves as the central registry for all national cyber incidents and facilitates the coordination of incident reporting and management across the country. The NAM-CSIRT 2025 report indicates that cyber threats in Namibia have doubled since the last period, with recent

incidents affecting government agencies and telecommunications companies between December 2024 and June 2025, resulting in data losses.

The legal framework, supported by the National Cybersecurity Strategy and Awareness Plan 2022–2027, sets operational guidelines for NAM-CSIRT and its management committee (MICT, 2022). Rising threats in early 2025 highlight that weak cybersecurity practices have exposed Namibian companies to vulnerability (NAM-CSIRT, 2025). Therefore, a practical cybersecurity framework is needed to close the gap between policy and implementation. Furthermore, given that Namibia's telecommunications sector is central to the country’s digital ecosystem and essential to economic and social communication, it is somewhat surprising that there is very little evidence of sector-specific cybersecurity frameworks or strategies in place to ensure cyber resilience. Waiganjo et al. (2025) point out that organisations typically lack cybersecurity teams and rely primarily on basic compliance for security, rather than on a proactive cybersecurity culture. In addition, awareness campaigns and training initiatives are sporadic and often do not reach the entire staff within the organisations, thereby leaving human factors vulnerabilities largely unaddressed. The risk of ineffective cultural involvement is significant, as human error remains the most common cause of cybersecurity breaches worldwide (Hamidi & Singh, 2025).

Furthermore, cybercrime can result in the leakage of information to unauthorised parties and the loss of intellectual property, thereby eroding the organisation's competitive advantage relative to other businesses (Waiganjo & Valungameka, 2023). Given the Namibian government's substantial investments in e-government initiatives, there is a need for commensurate investments in the network security framework. Therefore, cybersecurity best practices must be developed not only for the public but also for telecommunications institutions. Although most cybercrime laws have focused on developed countries, lawmakers in less-developed and developing countries should not ignore the Internet's influence on cybercrime when drafting their laws (Willie, 2023). In addition, law enforcement agencies should implement a range of measures to address cybercrime. In a study on cybersecurity in Namibia's telecommunications sector, Waiganjo et al. (2023) identified a significant gap in the

legal and regulatory framework governing cybersecurity practices. The study identified the need for an innovative cybersecurity culture program that is flexible, tailored to the local context, and capable of addressing the specific challenges of Namibia's telecommunications sector. The conclusions presented here are highly useful for anyone seeking to develop and implement a plan aligned with the needs of the Namibian sector.

The telecommunications sector in Namibia has experienced significant development and transformation in recent years. It is a major contributor to national economic growth and, therefore, has undergone numerous improvements in infrastructure, services, and connectivity. The industry comprises local and international providers delivering telecommunications services, including mobile, fixed-line, internet, and data (GSMA, 2024). Furthermore, Namibia has been actively expanding its telecommunications network in rural areas through universal service obligations and corporate social investment projects. CRAN monitors the telecommunications industry in the country. The authority works to ensure competition on fair terms, protect consumers' interests, and encourage the provision of efficient and affordable telecommunications services (NAM-CSIRT, 2025). Despite increasing demand for digital services and ongoing technological advancements, the sector continues to contribute significantly to Namibia's economy. Facilitating digital inclusion, connectivity, and the country's socio-economic development.

The telecommunications industry is considered part of the national critical infrastructure and is continually exposed to cybersecurity risks, primarily because it handles large volumes of sensitive data and its networks are highly interconnected (Waiganjo & Valungameka, 2023). Establishing a robust cybersecurity culture is vital to protecting confidential customer data, preserving network integrity, and ensuring uninterrupted service. In Namibia, research indicates that telecommunications staff are increasingly aware of cybersecurity issues; however, significant gaps remain in the execution and uniformity of the process (Nawa et al., 2022). Research outlines in greater detail the importance of organisational leadership in creating a cybersecurity culture within the company, through comprehensive and proactive steps that extend beyond mere regulatory compliance (Namibia CSIRT, 2025). Leaders are

urged to prioritise cybersecurity, provide the necessary funding, and develop a corporate culture in which employees are informed about security and held accountable. Taken together, these findings emphasise the need for a joint industry effort to nurture a vibrant and flexible cybersecurity culture.

In summary, the telecommunications sector in Namibia is a key pillar of the country's efforts to achieve economic growth and digital inclusion. Nevertheless, the sector, which is on the front line of delivering infrastructure and services to the public, faces a more complex and advanced cyber threat environment. The lack of sector-specific frameworks underscores the need for context-driven solutions that go beyond technical controls to address human behavioural and organisational-cultural dimensions. Understanding the state of cybersecurity in Namibia sets the stage for analysing factors that influence the organisational cybersecurity culture. The following section discusses the integration of the cybersecurity culture within organisations culture.

2.5 Integration of Cybersecurity into Organisational Culture

Both organisational culture and cybersecurity concern the development and management of staff, as well as the relationship between them. Cybersecurity culture is the organisation's collaboration and response to cybersecurity threats. Thus, it encompasses collective attitudes and approaches to information security (Alshaikh, 2020; da Veiga et al., 2020). Organisational is defined as the set of dominant beliefs, morals, and values that have developed over time to address both internal and external threats (Bandura, 2023). These beliefs are embedded within the organisation to foster a sense of purpose and belonging (MacQueen, 2020). Information security in any organisation is often said to depend on organisational culture. An organisation's culture shapes employees' behaviours (Van Staden & Van Niekerk, 2023). Khadka and Ullah (2025) state that culture aligns personal morals with the organisation's objectives. This aligns with the common belief about organisational culture, as expressed in the phrase “the way we do things around here” (Corradini, 2020).

Studies have shown that cybersecurity culture is rooted in and supports organisational culture. However, it is embedded in an organisation's functioning when cybersecurity principles are demonstrated through leadership, internal communication, and staff learning (Da Veiga et al., 2020; Delso-Vicente et al., 2025). A security culture ensures that cybersecurity is recognised not as a separate IT issue, but as a shared organisational concern. Moreover, a cybersecurity culture encompasses not only formal policies and training but also informal policies that shape how employees communicate with and protect the organisation's technological assets (Uchendu et al., 2021). An active and resilient cybersecurity culture fosters a shared responsibility, helping employees to be more vigilant against emerging threats. As cyber threats and attacks become increasingly advanced and sophisticated, particularly in organisational settings, the importance of building and nurturing a robust cybersecurity culture becomes even more crucial (Abifarin et al., 2023; Charalambous, Piki & Stavrou, 2025).

Integrating cybersecurity into organisational culture supports a more comprehensive security posture. Research organisations with a strong security culture tend to respond more effectively to cyber incidents and demonstrate greater resilience (Da Veiga, Botha & Herselman, 2020). When cybersecurity values are part of the organisation’s DNA, they guide decision-making, encourage the adoption of positive security behaviours, and contribute to effective risk management over time. Different countries and sectors may have distinct cybersecurity cultures, but the core concepts of shared responsibility, trust, and proactive behaviours remain the same across contexts (Uchendu et al., 2021). Consequently, aligning cybersecurity culture with organisational culture is key to developing more precise and effective interventions. The overlap area is depicted in Figure 2-3, which shows how cybersecurity principles, practices, and attitudes intersect with the overall organisational culture. The illustration shows how cybersecurity becomes an integral part of the organisation, guiding decision-making, actions, and interactions at all levels.

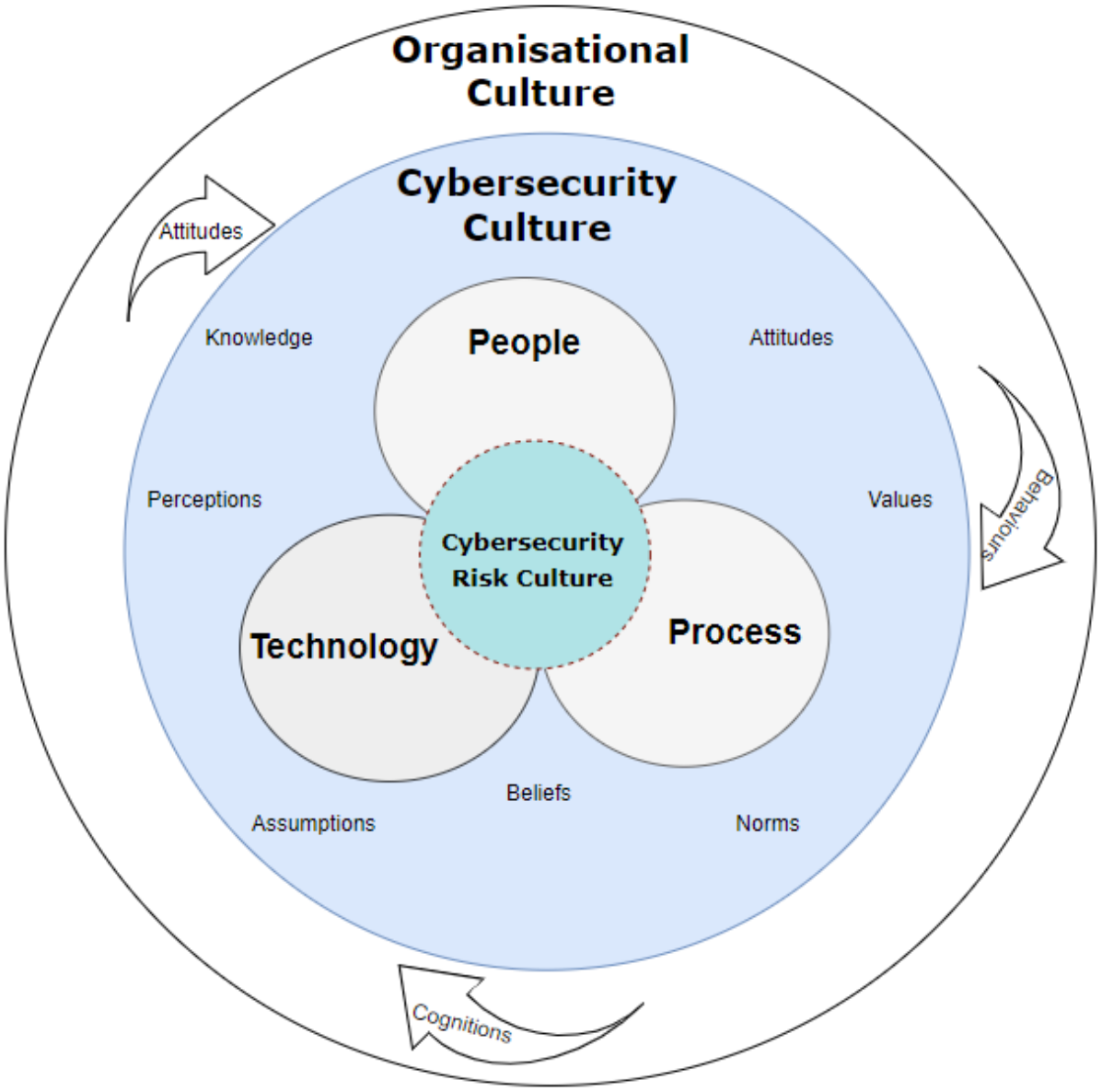


Figure 2-3: Integration of Cybersecurity into Organisational Culture

Figure 2-3 illustrates the organisation's cultural core. Having laid this groundwork, the next section reviews Namibia’s cybersecurity landscape, examining the nation's readiness and real-world challenges that hinder the establishment of a cybersecurity culture in organisations.

2.6 Best Practices for Cultivating Cybersecurity Culture

Building a strong cybersecurity culture is a complex task that involves various aspects such as leadership commitment, employee engagement, effective communication, appropriate technological support, and continuous organisational learning (Alshaikh, 2020; Cram, Proudfoot & D'Arcy, 2020; Granić & Marangunić, 2024; Alberto-Tomas, Diaz-Marcos, Aguado-Tevar & de Blanes-Sebastián, 2025). While the international literature continues to focus on human and organisational factors as core elements for enhancing cyber resilience, significant contradictions and gaps remain, particularly in developing economies and rapidly digitised sectors such as telecommunications. The inconsistencies in how different industries and countries plan, implement, and assess these practices are a reality. Here, the authors synthesise the latest findings and highlight gaps in the literature, particularly in the African telecommunications environment. They also identify underexplored areas that have led to the development of a context-specific cybersecurity culture framework for Namibia's telecommunications sector.

2.6.1 Leadership Commitment and Governance

Top management engagement is a recurring theme in the study and a key enabler of cybersecurity culture development. Indeed, senior management support is widely regarded as one of the most powerful indicators of cybersecurity project success (Alshaikh, 2022; ISO/IEC, 2022). Leaders who not only talk about but also lead by example, allocate necessary budgets, and integrate security as a key factor in all their strategic decisions help their staff understand and practice security, thereby making it second nature (Hamidi & Singh, 2025). It is also through the way leaders demonstrate cybersecurity as a collective organisational commitment that they exert their strongest influence, rather than merely as a set of technical rules to be followed (Corradini, 2020).

Moreover, the literature indicates that visible and effective leadership is not limited to issuing orders; it also involves actively engaging in cybersecurity initiatives, fostering support for policy enforcement and accountability, and ensuring security is internalised as a shared organisational value. This type of visible engagement, such as endorsing awareness initiatives,

supporting policy enforcement, and participating in governance activities, demonstrates organisational commitment and thereby increases the congruence between cybersecurity objectives and business priorities (Maynar, McGill, & Wang, 2022; Tejay & Winkfield, 2025). From a governance perspective, senior leadership is crucial to ensure that cybersecurity is integrated into the organisation's overall governance framework rather than kept as a separate area within IT departments (Uchendu, et al., 2021; Haney, Cunningham, & Furman, 2023).

The agreement on the role of leadership is very strong. However, the gap between theory and sustained practice in organisations remains significant. Numerous studies have shown that leadership's role in cybersecurity is often recognised rhetorically, but in practice it is constrained by competing priorities, limited knowledge, and resource shortages, particularly in developing countries (Timcke, Gaffley & Rens, 2023). International and African case-based evidence illustrates that while leadership-driven governance structures can elevate cybersecurity visibility, long-term cultural change depends on consistent leadership behaviour rather than symbolic endorsement alone (Mataruse, 2020; Alshaikh, 2020; Lemieux, 2025).

Leadership commitment and governance appear to be mutually dependent factors that influence the level of cybersecurity prioritisation and the actual cybersecurity practices within organisations. However, real-world evidence on how leadership behaviours foster long-term cybersecurity culture, particularly in African telecommunications companies, remains scarce. This underexplored area underscores the need for context-sensitive research and supports the inclusion of leadership dynamics as a core component of the preliminary development of a cybersecurity culture framework.

2.6.2 Training, Awareness, and Continuous Learning

Training, awareness, and continuous learning are widely recognised as central instruments for strengthening cybersecurity culture by addressing human-related vulnerabilities. According to the literature, well-rounded Security Education, Training and Awareness (SETA) programmes enhance employees' capacity to identify cyber threats, adhere to security policies, and use safer work methods (Uchendu, Nurse, Bada, & Furnell, 2021; Delso-Vicente et al., 2025). Since employees are regarded as the weakest link in the cybersecurity ecosystem, continuous

learning is the organisation's first line of defence when appropriate knowledge, skills, and behaviours are provided to employees (Alshaikh, 2021; CISA, 2022). Instead of viewing cybersecurity training as a one-time compliance exercise, modern research highlights the need for continuous learning that co-evolves with and responds to new threats and changes within the established organisation. Therefore, the best practice is to implement structured, role-specific, and ongoing SETA initiatives that support awareness within daily organisational routines.

Although there is near-unanimous agreement on the necessity of large-scale training, academic work clearly reveals ongoing constraints in deploying and creating awareness campaigns. Insecure communication and the burden of working investigations remain impersonal, highly specialised, and disconnected from employees' real-world daily work, thereby undermining long-term behavioural change (Cram et al., 2020). Additionally, research indicates that workers who receive job-focused training, are more realistic about the situation, and are supported by practical examples and repeated communication, are better able to regulate their behaviour (Uchendu et al., 2021). However, empirical research examining the sustained impact of such tailored approaches remains limited, particularly outside high-income organisational contexts.

Moreover, although technical controls still play a major role, companies are increasingly recognising that resilience is not only a matter of technology but also of the human dimension. In other words, resilience depends on individuals being aware of security, being cautious, and maintaining the right attitude. (Khadka & Ullah, 2025). Even-minded SETAs adopt strategies to achieve long-term behavioural change, rather than short-lived training or one-off awareness campaigns. They are using a holistic strategy that combines education, simulations, and scenario-based learning to help security-minded behaviours become second nature. Techniques such as phishing simulations, gamified modules, and case study-driven exercises have proven effective in building long-term awareness and resilience (Zhang et al., 2022; Alsharnouby, Al-Dubai & Wills, 2024;). In particular, the use of blended learning methods,

including e-learning, instructor-led sessions, and hands-on workshops, consistently improves retention and promotes the consistent practice of secure habits.

The effectiveness of training and awareness initiatives is also shaped by organisational constraints, including limited financial resources, shortages of skilled cybersecurity professionals, and competing operational priorities. These issues are particularly pronounced in developing economies, where companies struggle to sustain ongoing learning programs over time (Timcke, Gaffley & Rens, 2023). Here, workforce training may be sporadic, underfunded, or limited to meeting regulatory requirements rather than changing workers' mindsets. This tension between the recognised importance of continuous learning and the practical realities of resource-constrained environments represents a significant gap in the literature.

Similarly, recent studies shed further light on the need to conceptually trace cybersecurity awareness within the organisational learning ecosystem. At the same time, Alberto-Tomas, at le., 2025) suggest that methods such as micro-learning, simulations, and peer-based learning can help integrate awareness into operations without reducing operational efficiency. However, studies examining how these methods perform in sectors with extensive interactions and high operational speed, such as telecommunications, particularly in Namibia, remain scarce. Consequently, there is a lack of empirical evidence on the optimal design of continuous learning strategies to reinforce a cybersecurity culture in the aforementioned environments. The above-mentioned gaps in the literature indicate the need for modernised curricula, sector partnerships, and practical learning that equip the workforce to be both cyber-aware and highly adaptable.

In balance, although training and awareness are generally considered the most important aspects of a cybersecurity culture, the existing body of work indicates that telecommunications organisations with tight budgets struggle to understand how continuous, context-specific learning can be sustained. These gaps highlight the need for empirical research on training practices that can achieve a balance among the three elements: effectiveness, feasibility, and

behavioural impact, and thus provide a basis for developing a cybersecurity culture framework for the Namibian telecommunications sector.

2.6.3 Policies, Procedures and Organisational Alignment

Organisational policies, procedures, and governance structures provide the foundation for articulating and operationalising cybersecurity expectations within organisations. The literature consistently positions well-defined cybersecurity policies as essential instruments for guiding employee behaviour, defining roles and responsibilities, and supporting compliance with regulatory and organisational requirements (ISO/IEC, 2022). Well-articulated cybersecurity policies serve as a reference point for informed decision-making and promote consistent application of security protocols (Waiganjo, Osakwe & Azeta, 2024). When effectively designed and communicated, policies help shape norms and reinforce cybersecurity as an integral component of organisational culture rather than a purely technical obligation.

However, research also highlights a recurring disconnect between policy formulation and implementation. Although many organisations maintain comprehensive cybersecurity policies, their effectiveness is often undermined by limited employee awareness, inconsistent enforcement, or misalignment with operational realities (Hanus & Wu, 2021). Employees may perceive policies as abstract, overly complex, or detached from daily work processes, which weakens their influence on actual behaviour. This gap between formal governance structures and lived organisational practice remains a persistent challenge across sectors. According to Alshaikh et al. (2021), formal cybersecurity policies significantly enhance policy compliance and accountability when supported by effective dissemination strategies and role-based awareness initiatives. This suggests that the procedural aspect of cybersecurity culture must go beyond documentation and be translated into tangible practices embedded within operational workflows.

Governance mechanisms play a critical role in addressing this disconnect by embedding cybersecurity within broader organisational oversight structures. Studies emphasise that enterprise-wide governance arrangements, such as risk management committees, audit structures, and cybersecurity steering groups, can help elevate cybersecurity to a strategic

concern and ensure accountability beyond the IT function (Uchendu, et al., 2021; Haney et al., 2023). Such mechanisms facilitate coordination across departments and promote consistent policy interpretation and enforcement. Nevertheless, empirical evidence suggests that governance structures are often unevenly implemented, with limited clarity regarding roles, escalation pathways, and decision-making authority. Governance issues in developing countries are often exacerbated by institutional weaknesses, complex regulations, and low levels of cybersecurity maturity (Timcke, Gaffley & Rens, 2023). Even if international standards and frameworks indicate how to shape policy and governance, without much help from the literature, it is hard to see how deeply these documents are reflected in the operations of African telecommunications companies. On the one hand, current research largely overlooks factors such as organisational culture, regulatory environments, and resource availability, which ultimately determine governance effectiveness.

In general, the study notes that coherent policies and strong governance structures are key to building a cybersecurity culture; however, their role in producing consistent behavioural patterns remains unclear. There is little empirical research on telco organisations in African contexts, underscoring the need for governance frameworks that are not only aligned with standards but also account for local organisational realities. It is essential to overcome these barriers to develop a cybersecurity culture framework that integrates policy, governance, and behavioural aspects within the Namibian telecommunications sector. A culture that embraces continuous policy improvement, transparent reporting, and organisational participation significantly improves cybersecurity readiness and resilience.

2.6.4 Communication, Collaboration and Organisational Engagement

Effective communication and cross-functional collaboration are widely recognised as central enablers of a strong cybersecurity culture. The literature consistently demonstrates that cybersecurity awareness initiatives are more effective when supported by clear, consistent, and bidirectional communication channels that engage employees across organisational levels (Kritzinger, Da Veiga & van Staden, 2023; Delso-Vicente et al., 2025). A communication process that moves beyond one-way policy dissemination and instead encourages dialogue,

feedback, and shared understanding helps embed cybersecurity into everyday organisational practices. Collaborative approaches also help deepen a company's cybersecurity culture by making security everyone's responsibility rather than the sole responsibility of a highly specialised technical department. Research shows that when IT, risk management, human resources, and business units work together, they can coordinate their activities more effectively, respond to incidents more efficiently, and share accountability for achieving effective cybersecurity outcomes (Maynard, McGill & Wang, 2022). Such collaboration is particularly important in complex organisational environments, where fragmented communication structures can lead to inconsistent security practices and diminished situational awareness. This culture of openness reinforces trust and facilitates timely incident reporting, enabling organisations to act pre-emptively rather than reactively.

Despite this consensus, the literature reveals persistent challenges in translating communication and collaboration into sustained behavioural change. Many organisations continue to rely on compliance-driven messaging that emphasises rules and penalties, which may inadvertently foster resistance or disengagement among employees (Uchendu, et al., 2021). In contrast, participatory communication strategies, such as interactive workshops, security champions, and peer-led discussions, have been shown to improve employee engagement and strengthen social norms regarding secure behaviour. However, these approaches remain under-scrutinised in empirical studies, particularly within resource-constrained environments. Organisational involvement is also influenced by the degree to which employees feel included and empowered in cybersecurity initiatives. Research indicates that organisational trust and learning are enhanced when employees are given the freedom to report incidents, share concerns, and participate in security improvement efforts without fear of blame. However, only a few studies have examined in detail how such inclusive engagement frameworks operate in telecommunications companies, particularly in African regions where communication may be hampered by hierarchical structures and regulatory pressures. Communication, collaboration, and organisational engagement are crucial yet not equally well-understood facets of cybersecurity culture. Although the literature supports the importance of participation and collaboration, it provides little evidence on how to sustain these practices over

time in telecommunications environments. Closing the gap by defining a cybersecurity culture framework that integrates communication and engagement strategies aligned with the operational realities of Namibia's telecommunications sector would be a significant step toward furthering this development. Communication and collaboration are not only enablers of technical compliance but also critical drivers of cultural transformation in cybersecurity.

2.6.5 Technology, Usability, and Human-Technology Interaction

Technology plays a fundamental role in enabling organisational cybersecurity; however, the effectiveness of technical controls is closely mediated by human technology interaction. The literature consistently shows that even well-designed cybersecurity technologies can be undermined when systems are perceived as complex, intrusive, or misaligned with users' workflows (Uchendu, et al., 2021; Granić & Marangunić, 2024). As such, usability has emerged as a critical determinant of whether employees adopt, correctly use, or bypass security technologies in practice. Tools such as firewalls, endpoint detection systems, intrusion prevention mechanisms, and Identity and Access Management (IAM) solutions serve as both protective barriers and facilitators of secure user behaviours. However, when these tools are perceived as intrusive, overly complex, or incompatible with business processes, they can inadvertently encourage insecure workarounds and reduce user compliance (van Schaik, Jeske, Onibokun, Coventry & Jansen, 2020).

Studies grounded in human-centred security emphasise that security mechanisms perceived as easy to use and clearly beneficial are more likely to be accepted and integrated into routine work practices (Granić & Marangunić, 2024). When authentication systems, access controls, or monitoring tools are poorly designed, employees may resort to insecure workarounds, thereby weakening organisational security despite formal policy compliance (Delso-Vicente et al., 2025). The trade-off between security measures and operational efficiency is a salient example of technical robustness that must be balanced against user experience. Moreover, the study found that cybersecurity technologies enhance culture formation only when adequate user education and contextualised guidance are provided. Employees who understand the purpose and value of security tools are more likely to perceive them as enablers rather than

obstacles (Willie, 2023). In addition, organisations that deploy security technologies without adequate communication or training risk reinforcing negative attitudes toward cybersecurity, thereby eroding trust and engagement over time.

Therefore, usable security is not just a technical consideration; it is a cultural factor that shapes employees' willingness to adopt secure behaviours. Research on usable security indicates that the design and usability of cybersecurity tools significantly influence user behaviour and organisational compliance with security protocols. Systems that fail to consider user capabilities and context often lead to frustration, errors, and non-compliance, whereas improved usability can enhance secure behaviour and alignment with organisational security objectives (Di Nocera, Tempestini & Orsini, 2023). Additionally, the availability of robust infrastructure and state-of-the-art security tools signals the organisation's commitment to cybersecurity, which strengthens employee trust in organisational systems and policies. According to Mali (2024), organisations that invest in advanced technological defences, such as multifactor authentication and threat intelligence platforms, demonstrate improved protection of digital assets and a reduced risk of unauthorised access, thereby supporting proactive risk management and enhancing security resilience. These tools not only protect digital assets but also enable real-time detection and response, which are essential for fostering a culture of vigilance and resilience.

Despite these insights, the literature reveals significant gaps in empirical research on usability and human–technology interaction within telecommunications environments, particularly in developing economies. Much of the existing research is conducted in highly resourced settings, where technological maturity and user support structures differ markedly from those found in African telecommunications organisations (Timcke, Gaffley & Rens, 2023). As a result, limited attention has been paid to how contextual constraints, such as legacy systems, limited technical support, and high operational pressures, shape employees' interactions with cybersecurity technologies.

Collectively, technology alone is not sufficient to cultivate a resilient cybersecurity culture. Users' interaction with security technologies, influenced by usability, communication, and

organisational support, is a key determinant of users' secure behaviour. The lack of emphasis on human-technology interaction in African telecommunications contexts underscores the need for a context-sensitive framework that considers not only the behavioural and organisational dimensions but also the design of technology. This study addresses the gap by using usability and human–technology interaction as primary factors in developing a cybersecurity culture framework for Namibia's telecommunications sector.

Similarly, if a tool is poorly designed or overly complex, it may cause frustration and noncompliance. Developing a culture of cybersecurity entails moving in two directions simultaneously. On the one hand, you should continue upgrading your security technology; on the other hand, you should focus on usability, integration, and employee enablement.

2.6.6 Rewards, Incentives and Behavioural Reinforcement

The use of rewards, incentives, and social and behavioural reinforcement mechanisms is complementary; however, these tools are not always fully employed in developing a lasting cybersecurity culture. According to the literature, policies, training, and technology are the foundational controls, whereas reinforcement mechanisms are the key to continuous, secure behaviour (Alshaikh, 2020; Delso-Vicente et al., 2025). If there is no reinforcement, cybersecurity projects can easily be seen as just compliance-driven tasks rather than deeply rooted organisational values. Behavioural science indicates that positive reinforcement, such as recognition, feedback, and incentives, can strengthen desired behaviours by increasing their perceived value and social acceptance (Zhang et al., 2022). Reward systems in the context of organisational cybersecurity have been shown to promote employee engagement, increase accountability, and make the adoption of security measures routine (Corradini & Corradini, 2020). Crucially, the beneficial effects of the reward system are not entirely dependent on money; non-monetary recognitions, peer commendations, and career-oriented incentives have also been identified as factors in long-lasting behavioural change (Ogbanufe & Ge, 2023).

However, the studies reveal ongoing disputes over how cybersecurity incentive programs should be conceptualised and implemented. Faulty reward control can lead to mere token compliance or even to risky behaviours, for example, hiding incidents to shield performance

metrics (Tejay & Winkfield, 2025). Moreover, over-monitoring that accompanies these incentives also raises ethical and privacy concerns, which can erode trust and employee commitment if not managed openly (Ogbanufe & Ge, 2023). These contradictions point to the need for well-adjusted positive reinforcement measures that encourage learning and accountability and do not rely on fear or surveillance. Empirical data on rewards and incentives for cybersecurity remain quite sparse, particularly in the telecommunications sector and in African organisational contexts. Our studies are mostly conceptual or focused on wealthy environments; thus, little is known about how incentives function in situations of limited resources, varying workforce skill levels, and changing regulatory frameworks (Chang & Coppel, 2020). In addition, the question of how reward mechanisms interact with leadership behaviour, organisational norms, and informal peer influence to shape the core of cybersecurity culture remains largely unexplored.

In brief, rewards and behavioural reinforcement mechanisms together constitute a vital yet under-investigated aspect of cybersecurity culture. If they align with the organisation's core values, governance structures, and human-centred security practices, behavioural reinforcement can transform cybersecurity from an enforced mandate into a collective responsibility. The limited empirical exploration of these controls in African telecommunications environments reinforces the need for a context-specific framework that integrates behavioural reinforcement alongside leadership, training, governance, communication, and technology considerations. This study addressed this gap by positioning rewards and incentives as enabling components within the cybersecurity culture framework for Namibia’s telecommunications sector.

In general, the literature coverage of several core themes, such as leadership that aligns culture, training that sustains behavioural changes, policy structures and expectations, communication that fosters engagement, and usable technology that supports secure work practices, is limited. However, important gaps persist and are widely recognised as foundational to shaping cybersecurity culture. Unlike the sector-specific frameworks presented in later sections, these gaps collectively justify developing a tailored cybersecurity culture

framework grounded in overarching principles applicable across organisational sizes. The next section, therefore, critically reviews existing cybersecurity frameworks to determine the extent to which they address behavioural, organisational, and contextual factors relevant to this study.

2.7 Analysis of Existing Cybersecurity Frameworks

Building on the previous section, this part examines well-known cybersecurity frameworks to develop a conceptual framework that fosters a cybersecurity culture in organisations. The discussion highlights how the frameworks provide a structured approach that aligns with the best practices and strategies outlined earlier. Cybersecurity frameworks serve as a practical way for organisations to integrate secure practices into their operations and governance structures. Various frameworks at the international, regional, and national levels have been established to guide the sector in enhancing its cyber resilience in response to evolving sector needs. The review of these frameworks herein focuses on their relevance to the telecommunications sector, highlighting the main advantages, shortcomings, and gaps in fostering a cybersecurity culture. The results of this evaluation serve as the foundation for drafting a framework aligned with the telecommunications sector's needs and realities.

2.7.1 International Cybersecurity Frameworks

The National Institute of Standards and Technology (NIST) published the NIST Cybersecurity Framework (CSF) version 2.0, which provides comprehensive guidelines for managing and mitigating cybersecurity risks. While not an official global standard, it is widely recognised and adopted by organisations worldwide for its flexible and practical approach to enhancing cyber resilience across sectors. It provides a risk-based approach to managing cybersecurity through six core functions: Governance, Identification, Protection, Detection, Response, and Recovery (NIST, 2024). The NIST CSF is adaptable and scalable, making it attractive to sectors such as telecommunications. Although it is highly effective at outlining the next steps in cybersecurity capability development, the NIST CSF places limited emphasis on organisational cultural factors such as employee behaviour, leadership accountability, and inter-team collaboration (Alshaikh, 2020).

ISO/IEC 27001 is another widely used standard produced by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC). It provides a comprehensive framework for implementing an Information Security Management System (ISMS), including the risk assessments, security controls, and continuous improvement processes (ISO/IEC, 2022). Its emphasis on formal documentation and compliance mechanisms has made it popular among large organisations. However, critics argue that it may not adequately foster cybersecurity culture or employee engagement at all organisational levels (Alshaikh, 2020). In addition, the Centre for Internet Security (CIS) Controls offers practical, prioritised cybersecurity practices for mitigating threats. However, the controls are predominantly technical and do not explicitly address human-centric and organisational-cultural factors that are critical to long-term cybersecurity resilience (CIS, 2021).

2.7.2 Telecommunications Sector-Specific Frameworks

Frameworks specifically developed for the telecommunications sector provide valuable sectoral insights. The Global System for Mobile Communications Association (GSMA) is a global association representing mobile network operators and provides industry guidance through its Security Accreditation Scheme (SAS) and Mobile Telecommunications Security framework (GSMA, 2021). The framework focuses on protecting mobile networks and subscribers' data and generally prioritises operational standards over cultural change. The European Telecommunications Standards Institute (ETSI) and the Telecommunications Industry Association (TIA) provide frameworks and standards to enhance network security and incident management (ETSI, 2020). The cybersecurity standards of ETSI, which also address the security of the Internet of Things (IoT), aim to identify component-specific threats within the telecommunications ecosystem. The TIA has released ICT lifecycle management standards, which focus on supply chain security and network resilience. Although the industry-specific technical requirements are present in the standard, it does little to close the gap in guiding organisations on how to cultivate secure habits and a cohesive, awareness-based culture of cybersecurity. Standards rarely integrate leadership commitment, changes in behaviour, or organisational culture into their implementation frameworks (ETSI, 2020). Hence, these

frameworks collectively acknowledge the need for stronger cybersecurity postures in telecommunications, as they often treat human factors as secondary considerations.

2.7.3 Regional Cybersecurity Frameworks

The African Union (AU) Convention on Cybersecurity and Personal Data Protection, commonly referred to as the Malabo Convention, is a comprehensive legal instrument designed to enhance data protection and cybersecurity governance across African countries. One of the key objectives of the Convention is to establish a unified legal framework for the protection of personal data, the security of electronic transactions, and cybersecurity across all sectors, including telecommunications (African Union, 2019). However, scholarly analyses indicate that the implementation of the Malabo Convention varies significantly across African Countries and remains largely focused on legislative and regulatory adoption rather than operational guidance for organisations. Studies highlight challenges such as limited institutional capacity, uneven legal harmonisation, and a lack of practical implementation guidelines to translate the Convention's principles into organisational cybersecurity practices (Bouke, Abdullah, Alshatebi, Atigh & Cengiz, 2023). The Southern African Development Community (SADC) is a regional intergovernmental organisation in Southern Africa that encourages member states to cooperate in order to harmonise cyber laws and data protection, strengthen national cybersecurity capabilities, and combat cybercrime and human trafficking (SADC, 2022). Nevertheless, like the Malabo Convention, SADC's programmes are generally ambitious and frequently encounter difficulties in the enforcement and realisation of cybersecurity measures. This is even more true at the local level, particularly with respect to capacity building, regional coordination, and addressing common threats such as cyber warfare. As a result, there is a gap in translating these initiatives into a comprehensive organisational cybersecurity framework. This is attributed to the absence of an actionable telecommunications-specific framework.

2.7.4 National Policy Context and Regulatory Environment

The Namibian regulatory landscape remains fragmented, and enforcement actions remain limited. The country lacks a cybersecurity law that requires all sectors to comply with minimum

security standards. Despite existing laws addressing data protection and cybercrime, Namibia still lacks a comprehensive, binding set of regulations to establish standard cybersecurity rules (Waiganjo & Valungameka, 2023). The lack of regulations leads to the ongoing implementation of cybersecurity measures at different scales, resulting in employees with varying degrees of awareness and the company being more reactive than proactive in handling cybersecurity incidents.

Existing interventions include the National Cybersecurity Strategy and Awareness Raising Plan 2022–2027, the establishment of NAM-CSIRT under CRAN, incident-reporting and response coordination mechanisms and regulatory encouragement for operators and owners of critical information infrastructure to adopt internationally recognised practices such as encryption, regular security assessments and proactive incident reporting (MICT, 2022; NAM-CSIRT, 2024; The Brief, 2024). However, these interventions remain largely policy, regulatory and incident-response oriented. They do not yet provide a sector-specific framework for embedding cybersecurity culture within telecommunications organisations.

Recognising these challenges, the Namibian government has taken significant steps to strengthen national cybersecurity preparedness. CRAN formally launched the NAM-CSIRT on 14 April 2025, following its establishment by a government policy decision on 23 November 2023. Establishing the Namibia Cyber Incident Response Team (NAM-CSIRT) and implementing the Namibia National Cybersecurity Policy Framework (NNCPF) are significant milestones in the development of a national cybersecurity ecosystem (NAM-CSIRT, 2022). Such steps are intended to strengthen homeland security against cyberattacks through more efficient collaboration, enabling immediate responses to incidents and raising the public-sector security level. Nevertheless, the rollout of these policies is only beginning, and there remain issues with their enforcement, infrastructure, and resource allocation (Munyama & Botha, 2023).

Furthermore, the implementation of NNCPF remains in its early stages, and there is currently no sector-specific cybersecurity framework for Namibia's telecommunications sector. The absence of a mature legal framework and stable regulatory environment also contributes to

uneven cybersecurity practices and limited organisational readiness (Amutenya & Botha, 2019). Namibia currently lacks a dedicated regulatory or implementation framework tailored to the telecommunications sector's unique threats and needs. Furthermore, the slow operationalisation of the NNCPF and a lack of enforcement mechanisms further hinder the establishment of mature cybersecurity practices (Amutenya & Botha, 2019). The following section outlines the limitations of existing cybersecurity frameworks and provides recommendations for improvement.

2.8 Limitations for Existing Cybersecurity Frameworks

Currently, existing frameworks are effective not only in identifying methods for controlling technical cyber risks but also in establishing governance structures and complying with regulatory requirements. However, there are still some restrictions. It is necessary to understand these limitations to recognise the gaps that render them inefficient in developing a cybersecurity culture within an organisation. Among the widely accepted and used standards and frameworks across industries are ISO/IEC 27001, the NIST Cybersecurity Framework, and industry-specific cybersecurity maturity frameworks. They deliver risk-handling mechanisms in a well-structured manner, including the implementation of controls and incident response. Nevertheless, the literature increasingly acknowledges that these frameworks have significant limitations when viewed from the perspectives of organisational culture and human behaviour (Alshaikh, 2020; Alberto-Tomas, Diaz-Marcos, Aguado-Tevar & de Blanes-Sebastián, 2025).

A major drawback of existing cybersecurity frameworks is that they barely touch on human and behavioural aspects. Most of these frameworks, with few exceptions, place a strong emphasis on organisational policies, controls, and processes. At the same time, it is usually assumed that employees will behave rationally and compliantly once formal mechanisms are established. This assumption has been questioned extensively in behavioural cybersecurity research, which reveals that compliance is not necessarily a precursor to deep-rooted secure behaviours and internalised security values (Uchendu, et al., 2021; Delso-Vicente et al., 2025). Hence, frameworks that focus primarily on technical controls and neglect behavioural drivers may achieve only procedural compliance, without fostering a cyber-resilient culture.

Another obstacle comes from the behavioural and social aspects that have not yet been completely integrated. While some frameworks acknowledge the presence of human factors, these components are rarely treated as the core of design; instead, they are treated as add-ons. A review of the playbook reveals that leadership behaviour, social norms, peer influence, and reinforcement mechanisms, among others, have a determining impact on the cybersecurity culture. However, frameworks rarely operationalise these elements (Corradini, 2020; Alberto-Tomas, et al, 2025). The conceptual deficiency hampers the frameworks' ability to demonstrate how security practices are understood, negotiated, and implemented within an organisation's departments.

Moreover, many current frameworks are generic and one-size-fits-all, which limits their applicability across organisational and sectoral contexts. One may say that telecommunications companies operate in dangerous, intricate, and interdependent environments characterised by complex infrastructures, regulatory challenges, and unceasing service requirements. On the other hand, most cybersecurity framework studies are sector-specific and do not provide substantial support to the telecommunications sector in understanding how contextual factors influence the development of cybersecurity culture (Chang & Coppel, 2020). This issue is particularly pronounced in developing economies, which are significantly affected by cybersecurity challenges stemming from legacy systems, skill shortages, and resource constraints.

The literature also highlights limitations, including a lack of contextual relevance and geographic bias. Many highly cited cybersecurity frameworks and empirical studies are developed and tested in high-income countries and rarely undergo empirical testing in African organisational settings (Haney, et al., 2023). Thus, current frameworks might not really account for the institutional and governance aspects of African telecommunications organisations. This insensitivity to context casts doubts on whether such frameworks are transferable and effective in the Namibian telecommunications sector, given that organisational cultures, regulatory environments, and workforce capabilities may differ substantially from those assumed in the dominant frameworks.

In addition, the static nature of many framework designs presents further challenges. Cybersecurity culture is dynamic and evolves in response to technological change, emerging threats, and organisational transformation. However, several frameworks remain anchored in periodic compliance assessments and maturity snapshots, offering limited insight into how culture can be continuously reinforced and adapted over time (MacQueen, 2020; Alberto-Tomas, et al., 2025). This temporal limitation limits their usefulness for guiding long-term behavioural change and cultural sustainability.

Finally, the literature reveals a limited empirical link between framework components and measurable cultural outcomes. While many frameworks propose comprehensive sets of controls or domains, few studies empirically examine how these elements interact to influence employees' attitudes, perceptions, and behaviours over time, particularly in telecommunications environments (Uchendu, et al., 2021). This gap limits organisations' ability to assess which components are most influential in shaping cybersecurity culture and which require contextual adaptation.

Collectively, although existing cybersecurity frameworks provide important structural foundations, they exhibit significant limitations in addressing the behavioural, cultural, and contextual dimensions of cybersecurity. Namibia's telecommunications environment is a clear example of where these limitations are particularly significant, as there is a lack of empirical evidence, and the realities of the organisations differ from the assumptions of the dominant frameworks. The missing elements identified in this study suggest the need for a context-specific cybersecurity culture framework grounded in behavioural science that incorporates leadership, awareness, governance, communication, technology usability, and reinforcement methods. Addressing these limitations provides the conceptual rationale for the framework developed in Section 2.9.

Table 2-1 synthesises the key thematic dimensions identified in the literature and highlights the limitations of existing cybersecurity frameworks in addressing cultural and behavioural factors.

Table 2-1: Literature Gaps

Thematic Dimension from Literature	**Emphasis on Existing Cybersecurity Frameworks**	**Identified Limitations and Gaps in the Literature**	**Implications for Framework Development**
Leadership and Governance	Leadership is acknowledged in policy and governance standards (e.g., ISO/IEC 27001), often at a strategic level	Leadership commitment is frequently referenced but weakly operationalised in relation to everyday employee behaviour; limited empirical evidence from African telecommunications contexts	Indicates the need to position leadership commitment as a core cultural driver influencing norms, accountability and behavioural framework ling
Training, Awareness, and Continuous Learning	Emphasis on awareness programmes and periodic training initiatives	Awareness is often equated with behaviour change; limited evaluation of long-term behavioural impact and sustainability of training interventions	Highlights the need for continuous, role-based learning mechanisms embedded within organisational culture
Policies, Procedures, and Governance Structures	Strong focus on formal policies, procedures, and compliance mechanisms	Over-reliance on formal controls; limited attention to how policies are interpreted, enacted, and reinforced in daily work practices	Suggests integrating governance structures with behavioural and cultural reinforcement mechanisms
Communication, Collaboration, and Engagement	Communication is often treated as one-way dissemination of policies and guidelines	Limited exploration of informal communication, peer influence, and cross-functional collaboration in shaping cybersecurity culture	Supports the inclusion of participatory and collaborative elements within a cybersecurity culture framework
Technology, Usability, and Human–	Technical controls and security tools are central to most frameworks	Usability and user experience are under-explored; security tools may	Indicates the importance of integrating usability and human-centred design

Technology Interaction		be bypassed if perceived as obstructive; limited telecom-specific empirical studies	considerations into cybersecurity culture
Rewards, Incentives and Behavioural Reinforcement	Rarely incorporated explicitly into cybersecurity frameworks	Reinforcement mechanisms are under-theorised; ethical and motivational tensions surrounding incentives remain under-studied	Justifies the inclusion of reinforcement mechanisms as enablers of sustained secure behaviour
Contextual and Sectoral Sensitivity	Frameworks are largely generic and global in orientation	Limited contextual adaptation for telecommunications environments and African organisational settings	Reinforces the need for a context-specific cybersecurity culture framework tailored to Namibia's telecommunications sector

The table illustrates underexplored areas and contextual gaps, primarily in telecommunications and organisational environments in Namibia, which together justify the design of the preliminary conceptual cybersecurity culture framework. The identified shortcomings underscore the need for a local, relevant, behaviourally driven cybersecurity culture framework for the Namibian telecommunications sector. Next, the components of the preliminary conceptual framework are presented.

2.9 Preliminary Conceptual Framework for Developing Cybersecurity Culture

The preliminary conceptual framework presented in this section is developed from the literature synthesis undertaken through RO1 and RO2. RO1 identifies the organisational, human and governance requirements that form the foundation of the framework, while RO2 defines the core components and characteristics required for an effective cybersecurity culture framework. Together, these objectives provide the literature-informed building blocks from which the

preliminary conceptual framework is constructed before it is examined and contextualised through the empirical findings in Chapter Four. The Chapter Two represents a preliminary conceptual framework developed from the literature reviewed in this chapter, including behavioural theories, cybersecurity culture studies and existing cybersecurity frameworks. It is not the final framework of the study. Rather, it serves as a literature-informed analytical lens that guides the empirical investigation by identifying the initial components, constructs and relationships to be explored during data collection and analysis. This approach is consistent with qualitative case study logic, where existing theory and literature may inform the initial conceptual framing while empirical evidence is later used to confirm, adapt or extend the framework within its real-world context (Triplett, 2022; Khadka & Ullah, 2025; Fallatah, Furnell & Wagner, 2026).

The preceding sections of this chapter have shown that existing cybersecurity frameworks are very helpful in managing technical issues and supporting regulatory compliance. However, these frameworks have several shortcomings in addressing the behavioural, cultural, and contextual aspects of cybersecurity. The literature consistently points out that these challenges are persistent and include difficulties in operationalising leadership commitment, sustaining training and awareness initiatives, interpreting and enacting policies, fostering communication and collaboration, the usability of security technologies, and reinforcing secure behaviours. These drawbacks are particularly pronounced in telecommunications environments and remain largely unexplored in African organisational contexts.

Considering these deficiencies, the development of a preliminary conceptual framework to improve the cybersecurity culture of Namibia's telecommunications sector. The preliminary framework is not offered as a final solution. Instead, it is a theoretical framework that incorporates fundamental ideas from the literature and applies them to real-world settings in telecommunications organisations. From the organisational and behavioural perspectives, the framework synthesises findings from previously published studies. These findings explain the key factors influencing the emergence and the sustainability of cybersecurity beliefs, practices, and behaviours in organisations.

The preliminary conceptual framework positions cybersecurity culture as a multifaceted construct that emerges from the integration of organisational, behavioural, and technological factors. It integrates key components such as leadership commitment and governance; training and continuous learning; policy and procedural alignment; communication and collaboration technology usability, human-technological interaction, and behavioural reinforcement mechanisms as interconnected elements. These components are treated as interconnected rather than independent elements. They reflect both well-established and less extensively explored themes in the cybersecurity literature. Importantly, the framework does not present these components as fixed outcomes. Instead, they serve as a guiding construct that informs and directs the empirical investigation.

Most importantly, the framework recognises that cyber security culture is subject to change and development. Instead of treating culture as a fixed characteristic, the framework views it as a continuous process in which changes in the external environment, including threats, internal priorities, and employee engagement, shape it. Recent research supports the implementation of adaptive, context-sensitive approaches to cybersecurity culture, particularly in highly risky and rapidly changing sectors such as telecommunications. Building on previous research and directly addressing the identified shortcomings, the study provides a solid framework for the qualitative examination offered in the following chapters. The conceptual framework not only informs the preparation of the interview guide instruments but also provides a perspective for analysing the empirical findings, while leaving room for local variations in Namibia's telecoms sector.

This section proposes a conceptual framework for enhancing cybersecurity culture in the telecommunications sector. The framework synthesises key organisational, behavioural, and technological components identified in the literature. Figure 2-4 presents the preliminary cybersecurity culture framework and illustrates the relationships among its core components. These components provide a coherent foundation for the preliminary framework, linking theoretical insights and empirical findings to practical measures of organisational values.

Instead of depicting a linear or causal framework, the framework adopts an integrative structure that reflects the dynamic and interdependent nature of cybersecurity culture development.

Figure 2-4: Preliminary Conceptual Cybersecurity Culture Framework

At the foundation of the framework is leadership commitment and governance, which provide strategic direction, accountability, and organisational legitimacy for cybersecurity initiatives. Leadership influences how cybersecurity priorities are communicated, resourced, and embedded within organisational structures, thereby shaping the conditions under which secure behaviours can emerge and be sustained.

Surrounding this foundation are five interconnected enabling components: training, awareness, and continuous learning; policies, procedures, and organisational alignment; communication, collaboration, and organisational engagement; technology usability and human–technology interaction; and rewards, incentives, and behavioural reinforcement. These components are

positioned as mutually reinforcing rather than hierarchical, highlighting that cybersecurity culture is shaped through continuous interaction between formal controls, social processes, and individual behaviours.

The framework places cybersecurity culture at the centre as an emergent outcome of these interactions. Culture is conceptualised as the shared values, beliefs, and practices that influence how cybersecurity is perceived and enacted across the organisation. The two-way relationships indicated in the framework suggest that cybersecurity culture is both a determinant of and a consequence of organisational practices, employee experiences, and technological environments over time.

Importantly, the framework recognises the context-specific nature of the Namibian telecommunications sector. It acknowledges changes outside the organisation, such as regulatory requirements, sectoral risks, and organisational constraints, as factors that shape and interact with the framework's internal components. This contextual framework emphasises the framework’s adaptability and relevance of the framework in challenging operational environments that are highly risky, resource-constrained, and rapidly changing.

The following section describes and justifies the framework's elements and demonstrates the synergistic role of these components in developing an efficient cybersecurity culture within the organisation. It presents the key components identified as essential for the preliminary cybersecurity culture framework. The preliminary conceptual framework for improving cybersecurity culture in the Namibian telecommunications sector comprises interlinked components and synthesises the theories presented in this chapter. The components herein refer to three main dimensions of the organisation, namely behavioural, technological, and organisational, which together determine the extent to which cybersecurity values, norms, and practices are incorporated in an organisation. The components are not intended to be individual entities but rather units that continuously blend, thereby affecting workers' perspectives, willingness, and conduct regarding cybersecurity. The components illustrated in Figure 2-4 are discussed in detail in the subsections that follow.

2.9.1 Leadership Commitment and Governance

Leadership commitment and governance constitute the framework's foundational components. Previous studies have agreed that leadership behaviour, strategic prioritisation, and governance structures determine organisational norms. Therefore, leadership behaviour, strategic prioritisation, and governance structures also shape employees' perceptions of cybersecurity within an organisation (Alshaikh, 2020; Alberto-Tomas, et al,. 2025). In the framework, leaders' support is understood as their active and visible, continuous participation in cybersecurity management, including governance, accountability, and decision-making. Governance mechanisms constitute the structural environment through which the organisation's cybersecurity expectations are not only spoken but also are controlled, and their observance is ensured throughout the organisation.

2.9.2 Training, Awareness, and Continuous Learning

Training, awareness, and continuous learning represent a behavioural enablement component that supports the development of cybersecurity knowledge and skills. Studies suggest that merely identifying the problems is not sufficient to produce lasting changes in behaviour. Therefore, continuous, role-specific learning methods must keep pace with evolving threats (Chang & Coppel, 2020). This element of the framework depicts learning as a continuous process through which employees understand their security responsibilities and cybersecurity risks in the telecommunications environment.

In line with recognised best practice, the framework advocates implementing structured, role-specific, and continuous Security Education, Training, and Awareness (SETA) initiatives. These initiatives are designed not only to increase awareness but also to embed cybersecurity knowledge and practices into employees' daily routines. Training is more effective by customising SETA programmes to the specific duties and challenges of various roles within the organisation. Furthermore, the emphasis on ongoing education ensures that staff remain up to date with evolving threats and organisational policies, making cybersecurity a consistent and integral part of everyday organisational life.

2.9.3 Policies, Procedures and Organisational Alignment

Policies and procedures form an essential organisational component that translates strategic cybersecurity objectives into operational expectations. Existing frameworks emphasise formal controls; however, the literature reveals that their effectiveness depends on how policies are interpreted and enacted in daily work practices (Delso-Vicente et al., 2025). In the preliminary framework, policies and procedures are conceptualised not merely as compliance instruments but as mechanisms that must be aligned with organisational culture, workflows, and behavioural reinforcement to promote secure conduct.

2.9.4 Communication, Collaboration and Organisational Engagement

Efficient communication and collaboration are fundamental to the social dimension of cybersecurity culture. The existing literature emphasises the importance of two-way communication, peer review, and interdepartmental collaboration for the development of shared cybersecurity values and norms (Corradini & Corradini, 2020; Wang et al., 2022). This element of the framework reflects the formal and informal channels of communication through which cybersecurity messages are delivered, supported, and become familiar across the organisation’s boundaries.

2.9.5 Technology, Usability, and Human Technology Interaction

Technology usability and human technology interaction represent the interface between technical controls and human behaviour. Research demonstrates that employees are more likely to adopt and correctly use cybersecurity technologies when systems are perceived as usable and supportive of work tasks (Granić & Marangunić, 2024). The concept acknowledges that the effectiveness of technology largely depends on user experience, system design, and the extent to which security tools align with operational realities in telecommunications organisations.

2.9.6 Rewards, Incentives and Behavioural Reinforcement

Behavioural reinforcement mechanisms are among the main instruments of the framework that help ensure its durability. According to the literature, recognition, rewards, and incentives are

elements of implementing secure behaviours that become normalised and sustained when they are aligned with organisational values (Ogbanufe & Ge, 2023; Delso-Vicente et al., 2025). In the framework, this component reflects how reinforcement mechanisms contribute to the achievement of long-term behavioural consistency that is not dependent solely on punitive or compliance-driven methods.

Together, these components interact to produce cybersecurity culture as an emergent organisational property rather than a discrete or standalone intervention. Cybersecurity culture is thus understood as the shared values, beliefs, and practices that shape how employees perceive, prioritise, and enact cybersecurity in their everyday work. The preliminary framework conceptualises culture as dynamic and continually evolving, shaped through sustained interactions among leadership, organisational structures, behavioural processes, and technological systems. As depicted in Figure 2-4, the framework integrates insights from the literature while simultaneously guiding the empirical inquiry developed in the subsequent chapters. Rather than offering a definitive solution or a predictive outcome, the framework provides an analytical lens through which the key elements and relationships that constitute cybersecurity culture can be systematically identified and examined in the context of the present research. For clarity, the Chapter Two framework represents the preliminary conceptual framework developed from literature and existing frameworks. The framework presented later in Chapter Four represents the empirically informed framework developed after analysing participants' insights. The progression from Chapter Two to Chapter Four shows how literature-derived components were examined, confirmed, adapted or extended using empirical evidence from the Namibian telecommunications case study.

2.10 Implementation Considerations

The preliminary conceptual framework is intended to guide the empirical exploration of cybersecurity culture rather than to prescribe specific organisational interventions. Therefore, the understanding of the framework's implementation should be analytical and methodological, guiding the study's research and interpretation of cybersecurity culture. This method ensures

a logical connection between the literature review presented in Chapter Two and the qualitative research design discussed in Chapter Three.

From a data-driven perspective, the preliminary framework plays a key role in designing research tools by identifying central themes for the study of cybersecurity culture. The elements of the framework serve as conceptual guides that inform the development of interview questions and the structuring of data analysis, thereby facilitating the researcher's exploration of how leadership, organisational practices, behavioural processes, and technological factors interrelate in the telecommunications setting. Significantly, the framework does not specify predetermined variables or measurement levels, thereby allowing participants' viewpoints and the study context to emerge naturally.

The framework also supports interpretive analysis by providing a structured lens through which empirical data can be examined and compared. The framework achieves this by structuring insights from interrelated components, which, in turn, helps identify patterns, conflicts, and connections in the data without implicitly indicating causal direction or outcome. This interpretive flexibility is particularly important in qualitative research, where understanding meaning, perception, and experience is prioritised over hypothesis testing.

Contextual adaptability is another consideration embedded in the framework's design. Telecommunications organisations continually change and adapt due to their diverse regulatory, technological, and day-to-day operational environments. These changes and adaptations affect how cybersecurity culture is expressed and developed within companies. The framework's structure is designed to incorporate these environmental factors by recognising that the organisation's size, resource availability, regulatory requirements, and stage of technological maturity may determine the prominence and interconnections among the framework components. This adaptability makes the framework more suitable for conducting a study of cybersecurity culture in Namibia’s telecommunications sector.

Lastly, the structure was designed to allow the study to be reflective at each stage. It does this by making the living, moving, and changing relationship among organisational structures, human behaviour, and technology explicit. Thus, the framework acts as a 'mirror,' inviting

researchers to reflect on how their assumptions, participants' roles, and organisational contexts may shape their interpretation of the data. This ongoing self-questioning of the investigator's perspective, the participant's viewpoint, and the social setting enhance the study's trustworthiness and rigor and ensures that the framework is used as a tool for thinking rather than a blueprint for action.

2.11 Distinction from Existing Cybersecurity Frameworks

The theoretical cybersecurity framework presented in this article differs substantially from current frameworks in both scope and approach. On the one hand, commonly used frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework (CSF) 2.0 provide structured guidance for managing cybersecurity risks through controls, processes, and compliance mechanisms. These frameworks primarily examine elements from a technical and governance perspective. On the other hand, the preliminary framework in this study is based on a view of cybersecurity culture as a socio-organisational concept shaped by the interplay of human behaviour, organisational practices, and technological systems.

One major difference is that the preliminary conceptual framework places human behaviour and culture as its main components, rather than external factors. Previous frameworks generally assume that secure behaviour will automatically follow the rollout of technical controls and policies. However, the studies reviewed here indicate that leadership, employee perceptions, social norms, and reinforcement are key drivers of the implementation of cybersecurity practices and, consequently, of employees’ behaviours. These aspects of the culture have been integrated into the preliminary framework, which presents them as neither separate nor individual components influencing cybersecurity culture.

Another characteristic of the framework is its high context sensitivity. Most leading cybersecurity frameworks aim to be universally applicable across sectors and regions; as such, they may be less relevant to environments characterised by resource constraints, legacy systems, and changing regulatory landscapes. The structure of this study is based on the identified deficits in the literature regarding telecommunications organisations and the Namibian context. As a result, it acknowledges the importance of sectoral and geographic

specificity. In this context, therefore, the development of this framework differs from generic frameworks, which may be unaware of the operational realities of the Namibian telecommunications sector.

Additionally, this framework is drawn from a versatile, nonlinear perspective on security culture. While maturity frameworks can be interpreted as linear developments toward predetermined goals, this framework considers culture as a dynamic outcome of the continuous mutual interaction among organisational, behavioural, and technological factors. This difference aligns with the modern literature questioning static conceptions of culture and emphasising that culture adapts in response to changes in threat environments and organisational transformation.

Finally, the framework is distinguished by its analytical rather than prescriptive purpose. It is designed to guide empirical and interpretive analyses, not to serve as a checklist or an implementation blueprint. This positioning differentiates the framework from practice-oriented standards and underscores its role as a research contribution that advances existing knowledge while addressing identified conceptual and empirical gaps. Collectively, these distinctions highlight the framework's contribution to the cybersecurity culture literature by offering a theoretically informed, context-aware, and behaviourally grounded lens for reviewing cybersecurity culture within telecommunications organisations. The framework's originality lies not in replacing existing cybersecurity standards, but in complementing them by addressing dimensions that remain underrepresented in dominant frameworks. Therefore, implementing the conceptual framework can help organisations operationalise cybersecurity culture, strengthen resilience, reduce human vulnerability, and promote continuous awareness.

2.12 Anticipated Impact of the Conceptual Framework

The preliminary conceptual framework is expected to contribute to the body of knowledge on cybersecurity culture. The study provides a well-organised, behaviourally informed perspective that could inform further research on cybersecurity culture in telecommunications organisations. At a conceptual level, the article's framework synthesises existing research on

behaviour, organisation, and technology into a single system, with cybersecurity culture as the central socio-organisational phenomenon. The study synthesises findings from multiple studies into a coherent framework. Thus, it first addresses the problem of concept disintegration and, second, responds to calls for more comprehensive methods for grasping the essence of cybersecurity culture.

Methodologically, the framework provides a structured rationale for qualitative empirical research in cybersecurity. By clearly identifying essential elements and their interrelations, the framework facilitates the formulation of data-collection tools and analytical techniques that need not be based on known variables or causal hypotheses. Such freedom of choice is especially important for studies that probe the study area from the inside and in detail, i.e., in the field, aiming to reveal the context in which employees' understanding and organisational patterns are most often overlooked by quantitatively oriented cybersecurity research.

The framework also has practical relevance by offering organisations a conceptual reference for reflecting on the cultural dimensions of cybersecurity. While not intended as an implementation blueprint, the framework highlights organisational areas that warrant attention when examining cybersecurity culture, such as leadership engagement, learning processes, governance alignment, communication practices, technology usability, and behavioural reinforcement. In this sense, the framework may support reflective assessment and dialogue among stakeholders regarding the human and organisational factors that influence cybersecurity practices.

The expected influence of the framework largely depends on the context in which it is situated. Focusing on the Namibian telecommunications sector, the framework directly addresses the lack of African and industry-specific perspectives in the literature on cybersecurity culture. This awareness of context enhances the framework’s applicability to companies operating in similar environments. It also adds to the diversity and inclusivity of cybersecurity research. In general, the conceptual framework is understood as a unifying, context-aware work that connects theoretical insights with empirical study. Its impact will very likely be in its ability to lead academic research, guide methodological planning, and enable a reflective organisational

understanding of cybersecurity culture. Thus, providing a strong basis for the subsequent empirical chapters.

2.13 Synthesis of Literature and Identified Research Gaps

This chapter synthesised the multidisciplinary literature on cybersecurity culture, drawing on behavioural theory, organisational practice, governance mechanisms, and existing cybersecurity frameworks. Published works agree that a strong cybersecurity culture is not only about the presence of technical controls, but is also a resulting factor of leadership commitment, continuous learning, employee engagement, supportive governance, and human technology alignment. Studies of behaviour indicate that individuals' security actions are primarily influenced by their perceptions, motivations, social influence, and the environment, whereas research within the organisation highlights that leadership visibility, targeted training, and clear communication are important for making cybersecurity a shared responsibility in which everyone contributes.

Several major gaps remain in the picture despite the revelations mentioned above. Firstly, a significant portion of current research focuses solely on one-factor determinants of cybersecurity culture, thereby producing a disjointed understanding of employee behaviour. While awareness and training programs are widely advocated, evidence indicates that knowledge acquisition does not always lead to sustained safe behaviour; a gap remains between theoretical assumptions and practical outcomes. In addition, the main cybersecurity frameworks remain generic and control-focused, providing little guidance on how to implement behavioural, cultural, and situational factors, particularly in low-resource, low-capability settings.

Moreover, the geographic and sectoral focus of previous studies imposes additional limitations. Empirical research, in general, is concentrated in advanced economies, with only a few studies addressing the African and Namibian contexts and virtually none focusing on the telecommunications sector, even though this sector is critical to national digital infrastructure and is highly exposed to cyber threats. Consequently, current frameworks offer little insight into

how a cybersecurity culture can be developed in the telecommunications environment of a developing country, where organisational conditions, levels of regulation, and workforce characteristics vary widely.

Such gaps have necessitated a context-sensitive and integrative approach. This study aims to fill this gap by designing a cybersecurity culture framework for the telecommunications sector in Namibia, grounded in behavioural theory, organisational practice, and policy, informed by empirical insights from key stakeholder groups. By departing from patchwork and generic frameworks, the preliminary conceptual framework provides a logical basis for identifying, evaluating, and reinforcing cybersecurity culture in a high-risk, developing-country context, thereby guiding the study design and methodology detailed in Chapter Three.

2.14 Chapter Summary

This chapter reviewed a wide range of literature on the creation of a robust cybersecurity culture within an organisation, with a primary focus on its organisational, behavioural, and contextual dimensions. It delved into the basic concepts of cybersecurity and cybersecurity culture, unpacked the most influential behavioural theories that guide secure behaviour, and dissected current cybersecurity frameworks. It also assessed the most effective methods and strategies for developing a cybersecurity culture in organisations. The review demonstrated that cybersecurity culture is shaped by the interaction of leadership commitment, employee awareness and training, governance structures, communication practices, and human technology interaction. Behavioural theories clarified how perceptions, motivation, and social influence affect cybersecurity behaviour, while studies of organisations emphasise that cybersecurity should be part of normal work activities, not just a technical or compliance-function.

The chapter also included a critical review of various cybersecurity frameworks and noted that these frameworks do not account for behavioural and contextual factors, particularly in developing countries and high-risk sectors such as telecommunications. Numerous frameworks remain general and technically focused; thus, their capacity to effect a permanent

change in behaviour is limited. Essentially, this chapter provided a foundation, from both conceptual and empirical perspectives, for the study by synthesising existing knowledge and identifying major gaps in the literature. These gaps provide a strong rationale for developing a context-specific cybersecurity culture framework for Namibia's telecommunications sector. The knowledge acquired is instrumental in the research design, data collection methods, and data analysis plan presented in Chapter Three.

CHAPTER THREE: RESEARCH METHODOLOGY

Building on the deliverables identified in the previous chapter, this chapter outlines the methodological approach that further guides the study's data collection and analysis. Figure 3-1 depicts the layout of this chapter.

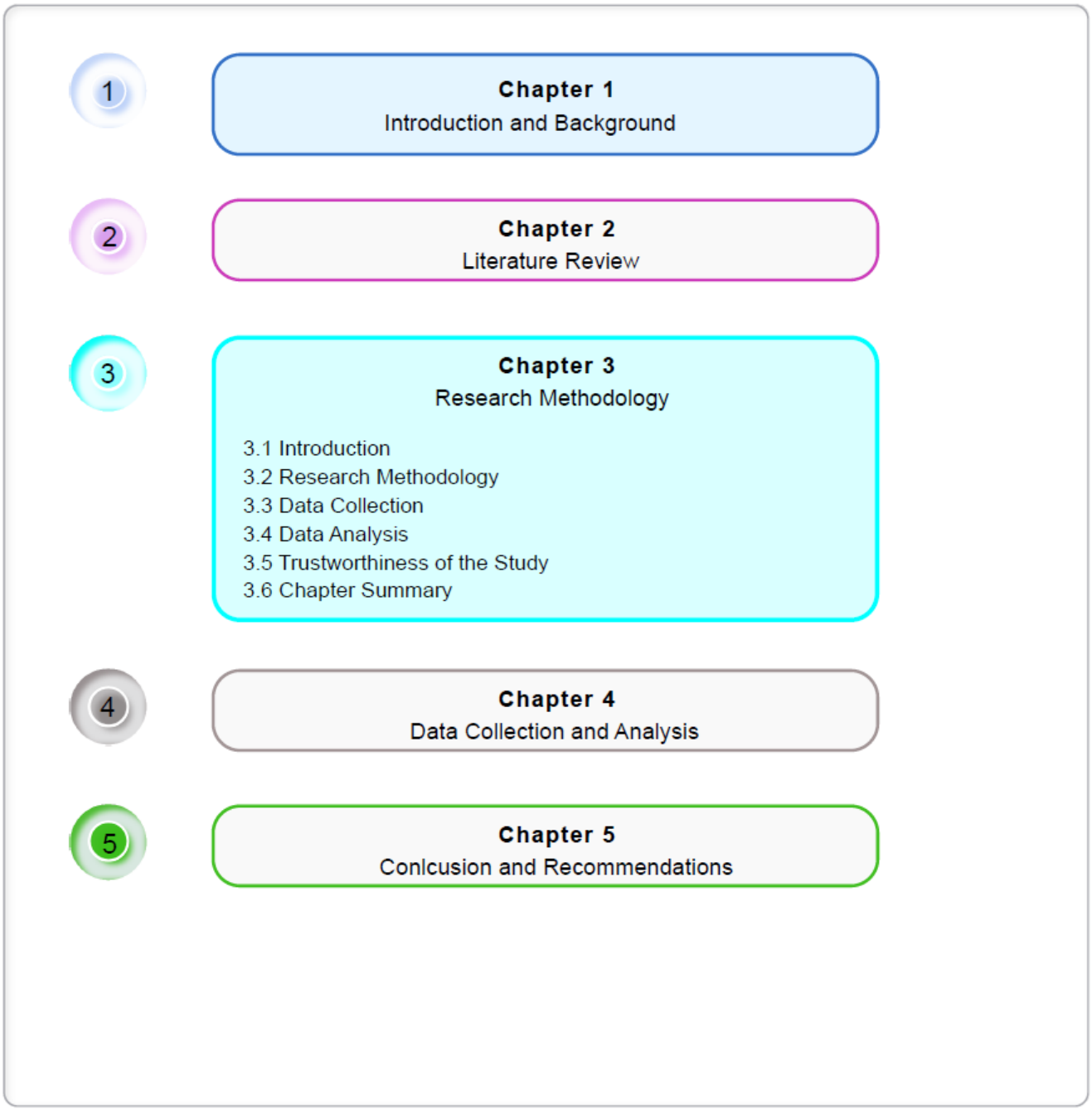


Figure 3-1: Chapter Three Layout

3.1 Introduction

The preceding chapter examined the relevant literature, including the theories that underpin this study. This chapter describes the study approach that guides the design of a conceptual framework to promote a cybersecurity culture in Namibia's telecommunications sector. The chapter discusses the methodologies used to achieve the study objectives, informed by the literature review and the initial conceptual framework presented in Chapter Two. The study aimed to develop a framework that would secure practices, reduce the number of cyber incidents, and increase organisational resilience. The research philosophy approaches to theory development, methodological decisions, research strategy, research time horizons, procedures, and techniques are all considered in this study and are included in the methodology. The approach follows the structure of the research onion framework by Saunders et al. (2023). This chapter discusses the ethical issues in research, examines the reliability of the research, and provides further details on the data-gathering and processing methods. It ends with a summary of the chapter.

3.2 Research Methodology

This section details the study methodology, thereby providing a clear explanation of the study process and the key methodological decisions made throughout. The purpose is to ensure that the approach taken is transparent and consistent with the study's objectives, which are to identify the components that contribute to the design of a cybersecurity culture within Namibia’s telecommunications sector. According to Creswell and Poth (2018), the research methodology is the overarching plan that determines how a study is conducted. It involves philosophical assumptions, the overall methodology (qualitative, quantitative, or hybrid), and the specific data-collection and processing tools. In contrast, the study process can be viewed as a sequence of phases, from problem identification and research question formulation to data analysis and reporting of findings.

Although the term "research design" is often conflated with "methodology," it is better understood as a blueprint that integrates the study topic, problem, questions, and methods into a coherent, logical whole (Creswell & Creswell, 2018). Although the study is designed

qualitatively, this chapter examines the methodology, which explains the rationale for the methods and instruments used. A qualitative approach is suitable to gain deep insights into participants' experiences, perceptions, and behaviours in their natural organisational settings (Kumar, 2019). To organise and present these methodological choices in a structured manner, this study adopts the research onion framework developed by Saunders et al. (2023). The framework provides a visual and conceptual structure that organises researchers across the layers of the research process, from the outer to the inner layer. Each level of the research onion can be viewed as a decision point corresponding to different research phases, and the order implies that the inner layers should be addressed only after the matters of the outer layers are resolved.

The onion's outer layers address core elements of research, such as the research philosophy and the methodology for theory development. These explain the beliefs about reality and knowledge that underpin the study. The middle levels discuss several methodological approaches, including qualitative methodologies, single-case study designs, and a cross-sectional time horizon. Finally, core layers address the substantive research tasks, including obtaining participant consent, addressing ethical considerations, selecting sampling techniques, collecting data, and processing data. Figure 3-2 illustrates the research onion, which is colour-coded and systematically divided into six hierarchical layers to support a logical research methodology.

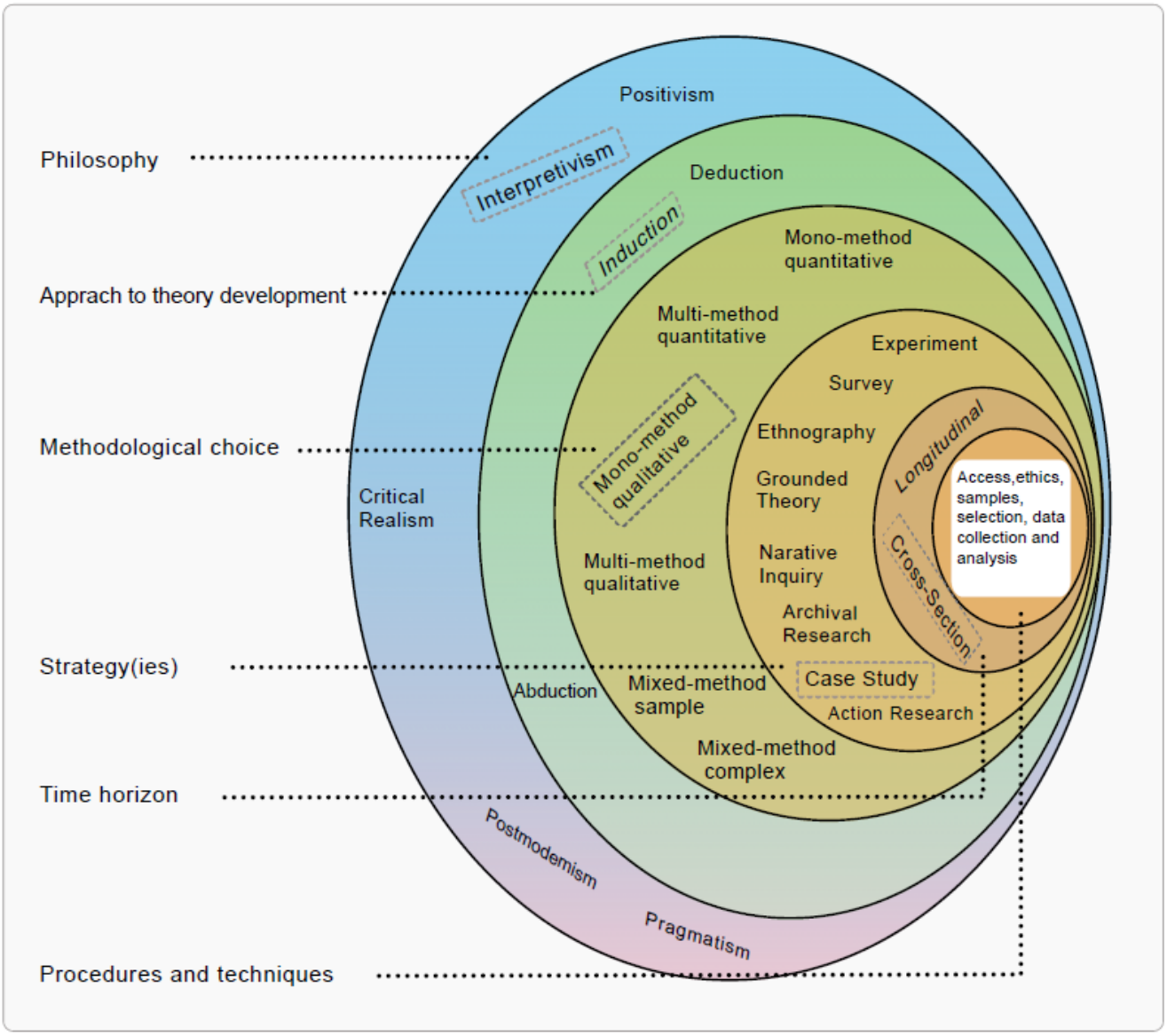


Figure 3-2: Research Onion

Source: Saunders et al., (2023)

The study adopted a tiered strategy to ensure that the choice of methodology was well considered and aligned with the overall research aims. Each layer of the research onion used in this study is detailed in the subsections below, along with the rationale for the decisions made at each level.

3.2.1 Philosophy

Research philosophy concerns the basic beliefs and assumptions on which the development of knowledge is based. Research philosophy is the foundational layer of any review; it articulates the core assumptions about reality, knowledge, and the researcher's role in the study. These philosophical stances shape how knowledge is developed and how meaning is understood within a study (Saunders et al., 2023). In management research, the five philosophies most frequently discussed are positivism, critical realism, interpretivism, postmodernism, and pragmatism. Interpretivism is the appropriate approach for this research because, according to interpretivism, reality is socially constructed and subjective. It is concerned with understanding human experiences in their specific social settings; that is, it recognises that people ascribe different meanings to the same phenomenon (Collis & Hussey, 2021). According to Saunders et al. (2023), knowledge is co-created through discourse between researchers and participants, with an emphasis on subjective interpretation of events.

The interview guide included questions that examined how participants perceived, understood and responded to cybersecurity awareness initiatives. The interpretivist standpoint allows for the investigation of participants' life experiences in their natural habitats. Thus, it is possible to understand how the staff conduct security proceedings and what they do through their interpretations. Whereas positivism seeks objective laws, this approach emphasises depth, context, and understanding. Consistent with the research philosophy, the attention will shift to the approach layer, which is discussed in the following section.

3.2.2 Approach to Theory Development

The study approach to theory development explains how researchers create knowledge and solve research problems. According to Saunders et al. (2023), research approaches can be categorised into three main types: deductive, inductive, or abductive. The selection should be based on the study objectives, questions, and philosophical standpoints. An abductive approach is a hybrid of induction and deduction. It begins with the observation of phenomena and the recognition of patterns, ultimately leading to the development or modification of theory (Saunders et al., 2023). On the other hand, deduction is about verifying a theory through a

reasoning process that moves from general ideas to specific conclusions (Saunders et al., 2023). With the inductive approach, a theory is developed by thoroughly examining the data, and themes are derived from observations (Collis & Hussey, 2021; Saunders et al., 2023). It is essential to make the correct decision regarding the study approach. It determines the methodology, design, and data collection, thus providing a consistent flow throughout the study (Saunders et al., 2023).

This study took an inductive approach, which is consistent with an interpretivist stance and the qualitative methods used. Inductive reasoning facilitates the examination of social realities and the formulation of specific theories grounded in rich, detailed data (Bell et al., 2019). Instead of confirming existing theories, the inductive approach uncovers new insights rooted in participants' experiences (Creswell & Poth, 2018). The following section explains the methodological approach used in this research.

3.2.3 Methodological Choice

The methodological choices layer of the research onion framework offers three categories for data collection and analysis: mono-method, multi-method, and mixed-methods (Saunders et al., 2023). These choices depend on the research philosophy, approach, and goals. A monomethod uses a single technique, either qualitative or quantitative. In a qualitative study, for example, a researcher may conduct interviews and then thematically examine the results. This method is well-suited to focused studies that require in-depth exploration of specific questions.

On the other hand, a mixed-methods approach combines both qualitative and quantitative data collection and analysis within a single study. This design enables researchers to triangulate their findings, resulting in a comprehensive understanding of the phenomenon (Saunders et al., 2023). Mixed methods are practical when research aims to explore meanings and test relationships between variables. The multi-method design uses various techniques within a single research paradigm. For instance, in a quantitative study, a researcher might collect data through questionnaires and structured observations, analysing them using different but

complementary statistical methods (Saunders et al., 2023). This strategy strengthens findings by using diverse data sources without crossing paradigmatic lines (Bell et al, 202).

This study employed a qualitative, mono-method approach, aligning with an interpretivist philosophy and an inductive research design. This study set out to identify social realities and behaviours related to the cybersecurity culture of a telecommunications organisation in Namibia. The researcher collected data primarily through semi-structured interviews. The researcher delved into participants' experiences and perceptions to obtain context-specific, detailed insights. Qualitative research is adequate for understanding meanings, values, and behaviours in complex organisations. It captures rich narrative data that highlights differences in human experience, particularly in attitudes towards cybersecurity (Bell et al., 2022). The mono-method design ensured consistency in data analysis, thereby enhancing coherence throughout the study.

Semi-structured interviews supported an in-depth exploration of participants' perceptions, experiences and organisational practices related to cybersecurity culture within the selected telecommunications organisation. However, the study does not claim a full ethnographic design, as it did not involve prolonged immersion, sustained participant observation or long-term field engagement. Instead, the study is positioned as a qualitative single-case study with a context-sensitive qualitative orientation, consistent with interpretivist case study research (Creswell & Poth, 2018; Yin, 2018). The following section explains the selection of the strategy layer.

3.2.4 Research Strategy

The research strategy outlines the steps taken to address the study questions and achieve the study's objectives. It is necessary to determine the study discipline, data sources, and methods for data collection and analysis. Any of these decisions should align with the research philosophy and approach (Saunders et al., 2023). The selected strategy should also reflect the study problem, the nature of the questions, and the expected results (Bell et al., 2022).

This study employed a qualitative, inductive, single-method approach within an interpretivist mindset. These decisions led to the selection of the case study approach. According to Yin (2018), a case study is an effective way to examine a topic in its real-world context. This allows the investigator to delve deeply into the issue when it is in-depth and difficult to separate from its context (Bell et al., 2022). The study focused on a telecommunications organisation in Namibia to examine how employees perceive and engage with cybersecurity procedures. A case study is well-suited because it helps to understand behaviours, culture, and perceptions in a real organisational setting. The case study approach also supports an interpretivist perspective, enabling researchers to understand experiences from participants' perspectives (Saunders et al., 2023). Semi-structured interviews are used to gather personal stories and rich insights. These insights help uncover how the cybersecurity culture is formed and experienced.

The case study strategy was more appropriate than an ethnographic strategy because the study focused on understanding cybersecurity culture within a bounded organisational context rather than observing an organisational culture over an extended period. Semi-structured interviews enabled the researcher to explore participants' perceptions, interpretations and reported organisational practices in depth. However, the study does not claim full ethnography because it did not involve long-term immersion, sustained participant observation or prolonged fieldwork. The research strategy is therefore best described as a qualitative single-case study with a context-sensitive orientation, consistent with case study research that investigates a contemporary phenomenon within its real-life organisational context (Creswell & Poth, 2018; Yin, 2018).

Since the study is inductive, the goal was to build understanding rather than to test a theory. The flexibility of the case study strategy facilitates the exploration of complex issues and generates new ideas (Bell et al., 2022). It further aligned with the study's philosophy, methodology, and goals; the case study approach was suitable for this research. It offers a solid foundation for understanding the behavioural and cultural aspects of cybersecurity within

a particular organisational context. The following section provides a detailed explanation of the time-horizons layer.

3.2.5 Time Horizons

The time horizon refers to the period during which data collection and analysis occur. According to Saunders et al. (2023), there are two types of time horizon in research design: longitudinal and cross-sectional. When a longitudinal time horizon is used, the researcher makes repeated observations over an extended period, which is appropriate for studies that examine changes and progress over time. In comparison, a cross-sectional time horizon is one in which data are collected at a single point in time; it is generally used to obtain an accurate picture of situations, perceptions, or practices within a specific context. Longitudinal designs are ideal for analysing temporal change. The primary objective of this study was to examine employees' current attitudes, behaviours, and experiences regarding cybersecurity culture within the organisation. As a result, a cross-sectional temporal horizon was deemed appropriate because it allows investigation of the social realities and organisational practices as observed and experienced at the time of the study.

The cross-sectional design is consistent with qualitative research approaches, particularly case study research, which aims to achieve a rich understanding of a phenomenon in its natural setting without extensive time commitment (Bell et al., 2022). This approach enables a systematic examination of cybersecurity culture as it is currently enacted within the organisation. Therefore, providing a suitable temporal framework is necessary to address the study’s research objectives.

3.2.6 Techniques and Procedures

Techniques and procedures are various ways of obtaining, organising, and analysing data in research. This step operationalises the study plan by translating the philosophy, strategy, and methodological approach into concrete actions for data collection and analysis (Saunders et al., 2023). The alignment between these procedures and the general research design is essential for methodological coherence (Bell et al., 2022). This research utilises qualitative

methods aligned with the interpretivist approach and a case study strategy. The primary data-gathering method was semi-structured interviews, which enabled the researcher to delve deeply into the interviewees' experiences, perceptions, and practices regarding cybersecurity culture, and also facilitated clarification of points that arose (Silverman, 2021). The methods and stages used in this study involve establishing the target population, selecting the sampling method, designing the interview instrument, and estimating the expected sample size. Later in this chapter, we will explore ethical implications, as well as reliability and validity issues.

3.2.6.1 Population

This study population refers to the broader group of individuals relevant to the study context from which participants may be drawn. In this study, the population comprises employees in Namibia's telecommunications sector who are directly or indirectly exposed to organisational cybersecurity practices. The target population is a subset of the broader population and refers to the group most directly related to the study problem from which meaningful insights can be obtained (Saunders et al., 2023). Consistent with a qualitative, arts-based study approach, greater attention is paid to the relevance and depth of understanding than to statistical representativeness. Participants were purposively selected to provide rich, highly contextual insights into the organisation's cybersecurity culture (Bell et al., 2022).

The study target population included Namibian employees within a Namibian telecommunications organisation whose roles exposed them to cybersecurity policies, practices, or decision-making processes. To ensure coverage across organisational levels and functional responsibilities, three participant groups were identified. These included IT staff members, who are directly involved in the implementation and management of cybersecurity controls; non-IT staff members, who interact with cybersecurity requirements as part of their routine work; and management personnel who are responsible for oversight, policy implementation, and strategic direction related to cybersecurity governance.

By identifying these categories, the study gained diverse perspectives on cybersecurity culture across the technical, operational, and managerial domains. Therefore, it is the embodiment of

a review of cybersecurity activities within the organisation that is supported and valued (Bell et al, 2022).

3.2.6.2 Sampling

Sampling in qualitative research involves the deliberate selection of participants who possess knowledge and experience relevant to the study objectives (Saunders et al., 2023). Unlike probability-based approaches used in quantitative studies, qualitative research typically uses non-probability sampling techniques that prioritise information-rich cases and contextual insight (Bell et al., 2022). Purposive sampling was used in this study to identify participants who had direct roles and responsibilities. Purposive sampling is particularly appropriate for interpretivist research, as it allows the researcher to exercise informed judgment in selecting participants who can provide detailed and meaningful accounts of the phenomenon under investigation (Saunders et al., 2023). Using this strategy meant that the study data were collected from individuals who could provide in-depth insights into the organisational cybersecurity culture, rather than from a representative sample of the population, which is less relevant.

3.2.6.3 Sample Size

The sample size in qualitative research is mainly determined by the point at which data saturation occurs, meaning that researchers continue to collect data until they believe that no new themes or perspectives will be identified (Fusch, Ness & Booker, 2018). However, the method section of the study views the sample size as the scope of data to be collected, that is, either planned or expected, rather than the number of participants who took part. The sampling frame in this study was designed to recruit participants from three groups within the organisation. IT personnel, non-IT staff, and management would thus have ensured that the perspectives of all sides were fairly represented and that the principles of a cybersecurity culture were understood. Based on qualitative research guidelines, a sample size of approximately 20 to 30 participants was considered sufficient to support an in-depth exploration of the study phenomenon within a single organisational case (Creswell & Poth, 2018).

The final determination of the achieved sample size and confirmation of data saturation are reported in Chapter Four, which presents the data collection process and participant

characteristics empirically. At the methodological design stage, the planned sample size was considered appropriate to support the study's exploratory objectives and interpretivist orientation.

This study employed a qualitative data collection technique consistent with its interpretivist research philosophy and case study strategy. Data were collected using semi-structured interviews, which are appropriate for exploring participants lived experiences, perceptions, and interpretations of cybersecurity culture within an organisational context (Creswell & Poth, 2018; Saunders et al., 2023). Ethical clearance was obtained prior to data collection, and participation was voluntary. Informed consent was secured from all participants, and confidentiality and anonymity were maintained throughout the research process.

3.2.6.4 Instrument Development

The primary data collection instrument was a semi-structured interview guide, developed specifically for this study. The instrument was intentionally designed to align with the study objectives and the preliminary cybersecurity culture framework. Its development was informed by an extensive review of relevant literature on cybersecurity culture, organisational behavioural and human-centric security practices. This approach informed the identification of the framework's core components (Bell et al., 2022; Saunders et al., 2023).

The interview guide consisted of open-ended questions intended to elicit participants' perspectives on key framework components, including leadership commitment, training and awareness, policy communication, collaboration, technology use and behavioural reinforcement. The semi-structured format ensured consistency across interviews while allowing flexibility for probing and clarification where necessary (Hennink & Kaiser, 2022). The interview guide was developed specifically to reflect the contextual realities of the Namibian telecommunications sector and the study's objectives. This method encourages in-depth contemplation and discovery of unexpected, yet relevant ideas supported depth of reflection and enabled the emergence of unanticipated yet relevant insights. The interview guide was structured into two main sections, each serving a distinct methodological purpose.

1. *Section A: Demographic and Role Context (All Participants)*

This section collected background information on participants, including gender, age group, organisational role, highest qualification, and years of service. The purpose of this section was not statistical analysis, but contextualisation. Understanding participants' roles and organisational positioning enabled the researcher to interpret responses regarding exposure to cybersecurity policies, responsibilities, and decision-making authority.

2. *Section B: Cybersecurity Culture Themes (All Participants)*

This section comprises open-ended questions designed to elicit participants' perceptions, experiences, and behaviours related to cybersecurity culture. The questions were aligned with the core elements of the preliminary framework and addressed the following thematic areas:

- ◊ **Understanding of Cybersecurity Culture:** The study explored participants' perceptions of cybersecurity culture and its influence on daily work practices.
- ◊ **Communication and Policy Awareness:** The study examined how cybersecurity policies, expectations, and practices are communicated and understood within the organisation.
- ◊ **Behavioural Challenges and Barriers:** Investigated obstacles to secure behaviour, including organisational, behavioural, and technological constraints.
- ◊ **Training, Awareness and Reinforcement Mechanisms:** Assessed the availability and effectiveness of awareness initiatives and training programmes in promoting secure practices.
- ◊ **Improvement Opportunities and Best Practices:** Captured participants' recommendations for strengthening cybersecurity culture, directly informing framework refinement.
- ◊ **Open Reflection**: Provided space for additional insights not captured by earlier questions, supporting completeness and data richness.

3. *Purpose of the Interview Guide*

The interview guide served three key purposes. First, it enabled an in-depth exploration of participants' knowledge and lived experiences of cybersecurity culture within their

organisations. Second, it facilitated the evaluation of how the preliminary framework components align with real organisational practices. Third, it generated empirical input to refine and contextualise the cybersecurity culture framework based on actual workplace experiences. All interviews were conducted online via Microsoft Teams to enhance accessibility and flexibility. With participants' consent, interviews were recorded to ensure accurate capture of responses, while the researcher also recorded reflective notes and contextual observations to support data interpretation.

In this way, the data collection was systematically aligned with the conceptual framework, the research questions, and the study's interpretivist approach. The information obtained from this method formed a solid basis for the thematic analysis given in Chapter Four and for the further development of the cybersecurity culture framework.

3.2.6.5 Data Collection and Analysis

Participants were selected using purposive sampling, based on their roles, responsibilities, and exposure to cybersecurity practices within the organisation. Access to participants was facilitated through organisational gatekeepers. Interviews were conducted online using Microsoft Teams to enhance accessibility and minimise disruption to participants' work schedules. This procedure ensured that data collection was systematically aligned with the study's research questions and conceptual framework.

Qualitative data analysis was conducted using Reflexive Thematic Analysis (RTA), following the approach preliminary by Braun and Clarke (2021). This analytical technique was selected because it is well-suited to exploring socially constructed meanings, perceptions, and behavioural patterns within organisational settings. Thematic analysis aligns with the study's interpretivist orientation by enabling the identification and interpretation of patterns across participants' without imposing a predetermined coding structure. This approach supported the derivation of themes grounded in the empirical data while remaining theoretically informed by the study's conceptual framework.

Figure 3-3 illustrates the thematic analysis process applied in this study and demonstrates how interview data were systematically transformed into analytically meaningful themes. Detailed presentation and interpretation of the findings are provided in Chapter Four.

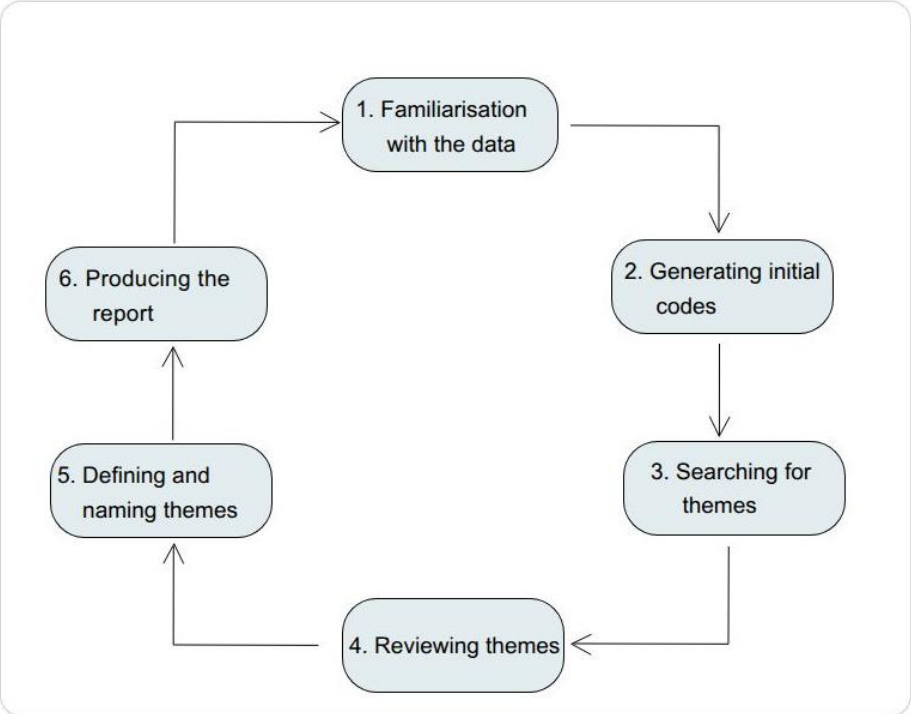


Figure 3-3: Thematic Analysis Process Flow

Source: Braun & Clarke (2021)

Instead of measuring variables, Figure 3-3 demonstrated how the RTA enabled the researcher to interpret how cybersecurity culture is understood, enacted, and reinforced across different organisational levels. The chosen method, therefore, aligns closely with the study's epistemological stance and its aim of generating a deeply contextualised understanding of cybersecurity cultural enablers.

3.3 Trustworthiness of the Study

Qualitative research quality and rigour are assessed through trustworthiness rather than statistical validity and reliability. Trustworthiness entails that research results are believable, coherent, and consistent, representative of the data, and extendable to other situations

(Gunawan, 2022). The research team adhered to qualitative research standards to enhance trustworthiness by systematically addressing credibility, dependability, transferability and confirmability.

Credibility refers to the extent to which the findings align with participants' experiences and perceptions. One-way credibility was enhanced was by conducting semi-structured interviews, which gave participants the freedom to express their views in their own words, and, at the same time, follow-up questions provided clarity and in-depth understanding. The correspondence between the interview questions, research objectives, and framework components also ensured that the data collected corresponded directly to the study's purpose (Saunders et al., 2023). The ongoing immersion in the data through re-reading and thematic analysis also contributed to the credibility interpretations.

Reliability is not only a matter of the consistent conduct of the research but also of the openness of its reporting. The research is reliable in its documentation of the design, data collection, and analysis procedures. To analyse the data, a well-structured and thorough thematic analysis was utilised; therefore, the results were clearly and systematically linked to the data rather than to the researcher's interpretations (Braun & Clarke, 2021).

Transferability refers to the extent to which findings are applicable to similar contexts. Instead, aiming for statistical generalisation, this study provides rich, contextualised descriptions of the organisational environment, participant roles, and cybersecurity practices within a Namibian telecommunications organisation. This level of contextual detail enables the reader to assess the findings in comparable organisational or sectoral settings (Creswell & Poth, 2018).

Confirmability is a quality component of qualitative research that concerns the extent to which results are shaped by participants' responses rather than by the researcher's bias. Therefore, to ensure confirmability, we took a systematic approach to coding the interviews and allowed the themes to emerge directly from the data. The researcher was also reflexive throughout the research process, that is, aware of her own assumptions and ensured that her interpretations were supported by the data. The clear linkage between raw data, themes, and the preliminary

framework further supports the neutrality of the findings (Stahl & King, 2021). When addressing these four components, the study ensured that trustworthiness in qualitative research, as shown in Figure 3-4.

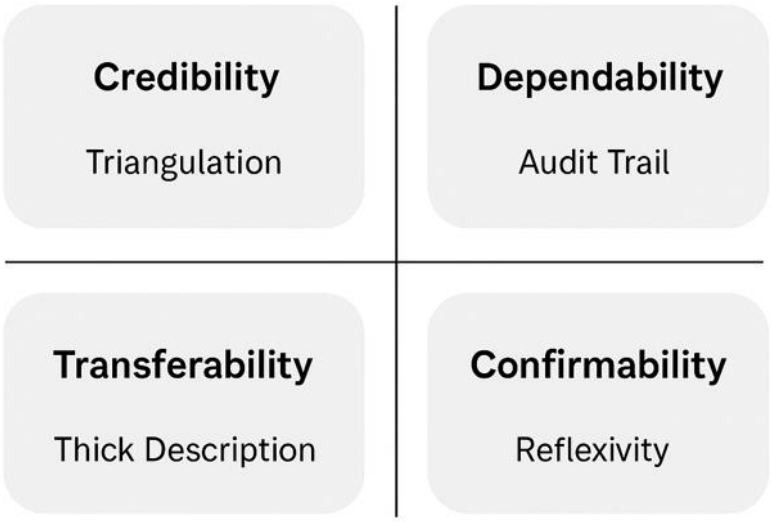


Figure 3-4: Trustworthiness Four-Quadrant

Figure 3-4 depicts a conceptual framework for assessing the trustworthiness of a study and how credibility, dependability, transferability, and confirmability come together to maintain the integrity of the research process. Each section presents the various approaches used to ensure the results were genuine, both in terms of content and methodology.

Altogether, these trustworthiness criteria were applied to ensure that the research was thorough, transparent, and ethically responsible. With a focus on credibility, dependability, transferability, and confirmability, the study provides a robust qualitative foundation for developing and validating a cybersecurity culture framework specifically designed for Namibia's telecommunications sector.

3.4 Chapter Summary

The chapter described the methodology used to conduct the research. It was a qualitative case study designed to investigate the factors influencing cybersecurity culture at a telecommunications company in Namibia. The research was grounded in an interpretivist

worldview and employed inductive reasoning. The purpose of the methodology was to provide a detailed study of the participants' views, experiences, and organisational context regarding cybersecurity culture. The data collection instrument was a series of semi-structured interviews that provided a clear picture of participants' thoughts, while Chapter Two of the literature review. A purposive sampling strategy was planned to provide a set of participants who were the most informative, from the main organisational groups, i.e., management, IT, and non-IT staff, whose roles together have an impact on cybersecurity culture. Thematic analysis was initially intended as a data analysis method, particularly appropriate for identifying themes and meanings in qualitative data. Atlas.ti software would have been used to facilitate systematic coding and analysis.

The chapter also detailed the measures taken to maintain the study's trustworthiness, including addressing credibility, dependability, confirmability, and transferability through reflexivity, transparent documentation, and participant validation. Through a well-constructed, theory-based methodological approach, this chapter establishes a solid foundation for the empirical part of the research. Chapter Four presents the results of implementing this method, revealing the topics that emerged from the interview data and their significance for developing a context-specific cybersecurity culture framework.

CHAPTER FOUR: DATA COLLECTION AND ANALYSIS

This chapter describes the methods and procedures used in this study for data collection and analysis. Figure 4-1 depicts the layout of this chapter.

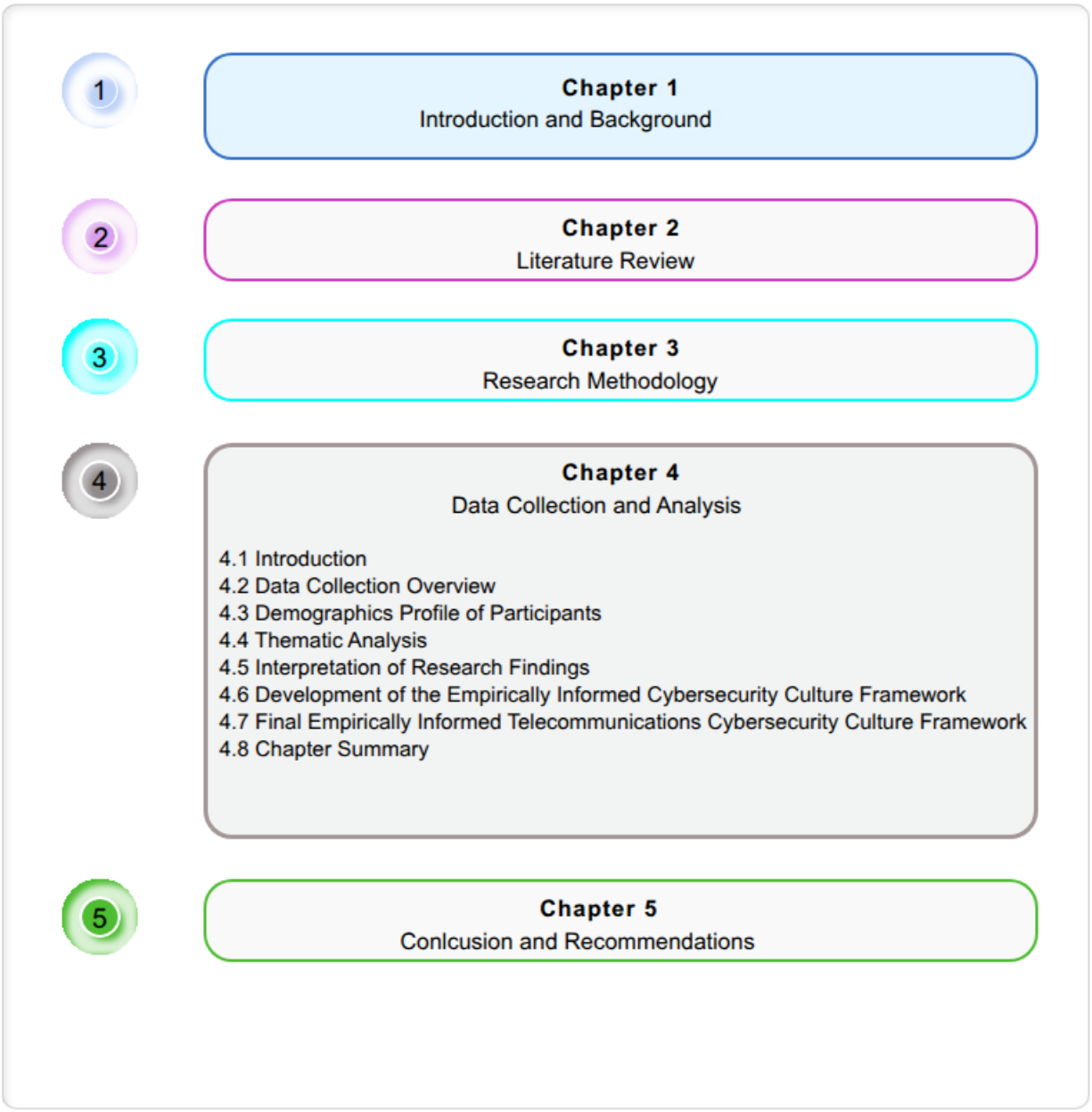


Figure 4-1: Chapter Four Layout

4.1 Introduction

This chapter discusses the study's empirical findings, which are based on qualitative data obtained through semi-structured interviews within a telecommunications organisation in Namibia. After establishing the conceptual and methodological foundations in Chapters Two and Three, this chapter reports and analyses the participants' viewpoints, experiences, and knowledge of organisational-level cybersecurity culture. This chapter sets out to empirically analyse the factors affecting cybersecurity culture, which are the research objectives of the study: (i) To determine the organisational, behavioural and technological factors that affect the cybersecurity culture; (ii) To consider how these factors are felt and understood by the various stakeholders within the organisation; and (iii) To come up with ideas that will help to adjust and give a proper local touch to the cybersecurity culture framework developed for the telecommunications sector.

Data were analysed using Thematic Analysis, enabling patterns and themes to emerge from participants' narratives. The findings are organised around key themes that correspond to the elements of the conceptual framework developed in Chapter Two, thereby maintaining consistency among the literature, the research design, and the empirical results. The study has combined the viewpoints of management, IT, and non-IT staff, and the synthesis of their perspectives formed the basis for developing an integrated understanding of cybersecurity culture across different organisational levels. This chapter is more concerned with a thorough analytical approach than with providing descriptive details. To justify the main interpretations and highlight the major points, the direct speech of the interviewees (Saunders et al., 2023) was used as the sole data source. The focus, however, is on identifying repeated patterns, connections, and conflicts within the information. At the end of the chapter, the major findings are synthesised, demonstrating how the empirical results address the research questions and setting the stage for Chapter Five, where the findings will be discussed with respect to their theoretical implications, practical recommendations, and the developed cybersecurity culture framework.

4.2 Data Collection Overview

This study employed a qualitative data collection technique consistent with its interpretivist research philosophy and case study strategy. Data were collected using semi-structured interviews, which are appropriate for exploring participants lived experiences, perceptions, and interpretations of cybersecurity culture within an organisational context (Creswell & Poth, 2018; Saunders et al., 2023).

Semi-structured interviews were selected because they allow the researcher to follow predefined themes while retaining flexibility to probe emerging issues relevant to the study objectives (Yin, 2018). This technique is particularly suitable for investigating behavioural and cultural phenomena, as it supports the collection of rich, context-specific insights across different organisational roles. Ethical clearance was obtained prior to data collection, and participation was voluntary. Informed consent was secured from all participants, and confidentiality and anonymity were maintained throughout the research process.

The research data was collected through semi-structured interviews with staff members of a Namibian telecommunications organisation. A total of fifty (50) invitations were distributed across three participant groups: management, IT staff, and non-IT staff. Of these, twenty-five (25) participants consented and completed the interviews, resulting in an overall response rate of 50%. Table 4-1 summarises the distribution of invitations and responses by participant group.

Table 4-1: Participant Group Invitation and Response Distribution

Participant Group	**Invited (n)**	**Responded (n)**	**Response Rate (%)**
IT Staff	20	8	40.0
Non-IT Staff	15	9	60.0
Management	15	8	53.3
Total	**50**	**25**	**50.0**

Participants were assigned unique pseudocodes to maintain confidentiality and ensure consistency throughout the analysis. Each pseudocode was a combination of a sequential

number and an abbreviation of the participant group (e.g., 1_ITP, 9_NIT, 18_MGT). The final set of data consisted of 25 valid interviews, with management participants making up eight (8), IT staff members eight (8), and non-IT staff members nine (9). All interviews met the inclusion criteria and were suitable for analysis. Therefore, no exclusions were necessary.

Data were gathered using the qualitative case study approach outlined in Chapter 3 to investigate how organisations develop their cybersecurity culture and the practices and requirements involved. An ethical clearance certificate was obtained and attached as Appendix A. Over three months, the interviews were conducted via Microsoft Teams, a convenient and secure online platform. Content-wise, each recording ranged from 30 to 45 minutes, and it was conducted only with participants' explicit consent. The tapes were transcribed verbatim. All information has been properly secured and is intended solely for academic use. Confidentiality was rigorously maintained; therefore, pseudocodes were used for the transcripts and the analysis results.

4.2.1 Response Rate

The overall response rate of 50% reflects adequate participation for qualitative research, ensuring a diverse range of perspectives across operational and strategic levels. Purposive sampling was used to select participants from three primary groups: IT staff, non-IT staff, and management based on their distinct roles in shaping, implementing, and experiencing the organisation’s cybersecurity culture. This diversity strengthens the credibility and richness of the thematic analysis presented in subsequent sections.

4.3 Demographic Profile of Participants

This section describes the demographics of the participants. Presenting detailed information about participants’ job titles and responsibilities clarifies the diversity and representativeness of organisational roles within the sample. This specificity enables readers to determine whether the study’s findings are relevant and credible across different levels and functions of the organisation, thereby strengthening the interpretation and generalisability of the results. A total

of twenty-five (25) participants were interviewed, drawn from three primary groups: management (n = 8), IT staff (n = 8), and non-IT staff (n = 9).

The demographic profile is summarised across four key variables: gender, age group, highest qualification, and years of employment within the organisation. The gender distribution consisted of twelve (12) males and thirteen (13) female participants. Table 4-2 presents a comparative summary of these characteristics across the three participant groups.

Table 4-2: Demographic Profiles of Participants

Demographic Variable	**Management (n=8)**	**IT Staff (n=8)**	**Non-IT Staff (n=9)**	**Total (N=25)**
Gender	4 Male, 4 Female	5 Male, 3 Female	3 Male, 6 Female	12 Male, 13 Female
Age Group (Years)	31–50: 6 51+: 2	21–30: 3 31–40: 5	21–30: 5 31–40: 3 41–50: 1	25
Highest Qualification	Master's: 4 Degree: 3 Diploma: 1	Degree: 5 Master's: 3	Degree: 6 Master's: 3	25
Years in Organisation	6–10: 3 10+: 5	3–5: 4 6–10: 4	3–5: 6 6–10: 2 10+: 1	25

The sample reflects a balanced representation of organisational roles, with a slight majority of female participants (52%). Most management respondents were older than 30 years and held at least a bachelor's degree, reflecting their seniority and professional experience. Many IT employees were younger (31 40 years) and had technical qualifications, while non-IT staff were mainly a mixture of support functions, among which there were a considerable number of early-career participants aged 21 30 years. Such demographic diversity guarantees diverse viewpoints on the organisation's cybersecurity culture.

The demographic summary provides a basis for understanding the participants' perspectives, which are discussed further in the thematic analysis. The section below first explains the analytical method and then introduces the primary themes identified from the interview data, which represent participants' experiences, practices, and perceptions of cybersecurity in the organisation.

4.4 Thematic Analysis

This section outlines the techniques used to prepare and analyse the qualitative data collected through semi-structured interviews. Prior to commencing thematic analysis, a systematic verification process to ensure its completeness, accuracy, and suitability for further examination. Specifically, each interview transcript was meticulously checked for missing or incomplete responses, and any inconsistencies in the text were cross-checked against the original audio recordings. Audio recordings were used to compare and check the transcripts for word-for-word accuracy and to correct any mistakes. During this process, data deemed irrelevant to the research objectives were excluded to maintain focus and clarity. Such data typically arose when participants provided information that, while potentially interesting, did not directly address the study's objectives.

For example, general opinions unrelated to cybersecurity culture or responses that diverged from the interview questions. The identification of irrelevant data was guided by the research questions and objectives, with each transcript carefully reviewed against the interview guide. Responses not aligned with the thematic focus of the study were flagged and excluded from the analysis. This was done to ensure that the resulting themes accurately reflected the factors influencing organisational cybersecurity culture. The cleaned dataset was then analysed following the six-phase approach as proposed by Braun and Clarke (2021), as described in Chapter Three.

Thematic analysis is employed for its flexibility and its capacity to identify patterned meanings across qualitative data, particularly in relation to organisational, behavioural, and technological factors influencing cybersecurity culture within the Namibian telecommunications sector. To support coding and data management, Atlas.ti was employed to enable the systematic organisation of codes, memos, and thematic structures. Figure 4-2 illustrates the six-phase thematic analysis process applied in this study, showing the progression from raw interview data to the development of themes and their interpretation.

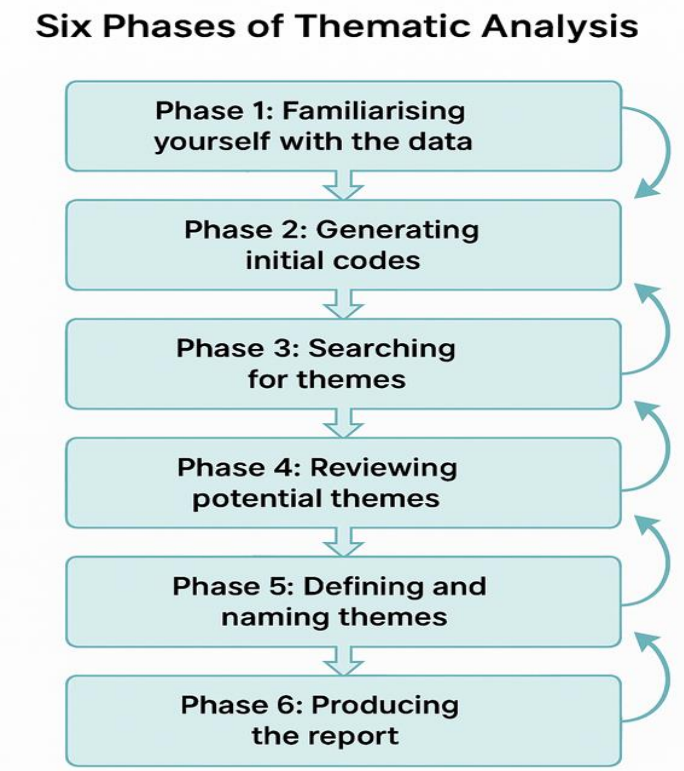


Figure 4-2: Thematic Analysis Phases
Source: Braun & Clarke (2021)

The thematic analysis process is presented in the following subsections, which outline the different phases.

4.4.1 Phase 1: Familiarisation with the Data

Braun and Clarke (2021) described the initial phase of their six-phase Reflexive Thematic Analysis as critical for developing a deep understanding of the data's content and context. In this phase, verbatim transcripts of all the interviews were produced and systematically compared against the original audio recordings to identify and correct errors or omissions. The researchers then engaged in multiple readings of the transcripts, noting their initial reactions and impressions. Through analytic and reflexive memos, preliminary ideas and potential patterns were documented, facilitating early insights into emerging themes. All steps of this process were recorded and managed within Atlas.ti to maintain a comprehensive audit trail and ensure transparency throughout the analysis.

To organise the data, a participant worksheet was created that lists all participants and their pseudocodes. Each transcript was stored in a structured format aligned with the approved interview guide to ensure coverage of all questions. For confidentiality, participants were anonymised using role-based identifiers: IT staff (ITP), non-IT staff (NIT), and management (MGT). Table 4-3 summarises the qualitative data sources and familiarisation activities undertaken prior to formal coding.

Table 4-3: Data Sources and Familiarisation

Data Source	**Participant Group**	**Number of Participants**	**Data Volume**	**Familiarisation Activities**
Semi-structured interviews	IT staff	8	16 pages	Transcription, repeated reading, memo writing
Semi-structured interviews	Non-IT staff	9	18 pages	Initial notes, reflexive journaling
Semi-structured interviews	Management	8	16 pages	Pattern noting, preliminary observations

Table 4-3 demonstrates that participants' interviews were thoroughly transcribed and read multiple times, and that reflective and analytical memos were written in Atlas.ti. This enabled the researcher to gain a deep understanding of the perspectives of participants from IT, non-IT, and management groups; thus, the researcher was well prepared for the subsequent steps of coding and theme development.

Following data familiarisation, the study proceeded to formal coding and theme development. Table 4-4 illustrates how raw interview data were iteratively coded and synthesised into higher-order themes. A sample of three participants from each group is included for illustrative purposes.

Table 4-4: Thematic Analysis Illustration

Raw Data Extract	Initial Code	Category/Cluster	Researcher Theme
“We receive policy emails, but the workflow is confusing. I’m never sure who approves the cyber risk.” (P07_ITP)	Ownership ambiguity	Governance communication	Implementation Gap
“Training is available, but it’s too generic. It doesn’t show how to apply controls in our context.” (P12_NIT)	Training relevance	Capability development	Competency and Awareness Challenges
“Leadership talks about cybersecurity, but priorities shift when deadlines hit.” (P18_MGT)	Leadership messaging inconsistency	Organisational commitment	Leadership Influence on Culture

Table 4-4 demonstrates the analytic chain of evidence, showing how meaning was constructed through iterative coding and theme development. Full coding outputs and theme definitions are provided in Appendix G. The familiarisation phase was not a passive reading exercise but an active analytic engagement. The researcher noted recurring issues, such as unclear control, ownership, and the relevance of training, while also reflecting on personal assumptions. This phase laid a conceptual foundation for subsequent coding and theme development.

4.4.2 Phase 2: Generating Initial Codes

The second phase of the project was mainly dedicated to making initial codes from the interview transcripts. The coding was conducted using Atlas.ti, which facilitated consistent tagging, retrieval, and comparison of data segments across participants. The process was inductive, in that it allowed the code to emerge from the data rather than being derived from a preexisting framework. This method aligns closely with Braun and Clarke's (2021) perspective, as it enables iterative coding and encourages researchers to actively interpret emerging data themes, rather than imposing rigid or pre-determined categories. Braun and Clarke (2021), leading scholars in qualitative research, highlight that reflexive thematic analysis requires a flexible approach and deep analytic engagement, with researchers continually adapting their methods to the nuances of the data. By embracing this flexibility and interpretive stance, our

analysis can capture the complex and evolving nature of participants' experiences and perspectives.

The researchers identified key sections of the text that revealed recurring ideas and patterns related to cybersecurity culture. Coding was iterative: new code was added when further understanding appeared, and similar code was combined or revised to prevent duplication. Reflective memos are kept throughout the process to record analytical decisions and the researcher's assumptions. Table 4-5 illustrates how initial codes were derived from participant responses to interview questions across IT, non-IT, and management groups.

Table 4-5: Generating Initial Codes

Interview Question	Participant (ITP)	Participant (NIT)	Participant (MGT)	Initial Codes Identified
1. Describe your understanding of cybersecurity culture and its impact on your daily work.	Cybersecurity is viewed as a technical responsibility focused on system protection and compliance with policies and procedures	Cybersecurity is widely recognised as important, but is often secondary to operational priorities, despite the existence of a dedicated department	It is regarded as a strategic and organisational responsibility	Perceived ownership of security: Strategic vs operational focus
2. Describe how the communication of cybersecurity policies and expectations is within your department or across the organisation?	This policy was communicated through IT briefings and, at times, via system notifications and emails.	Mainly through email circulars and informal guidance on different platforms, employees are expected to read and familiarise themselves with the policies and procedures	Policies are communicated via formal policies, management meetings, and governance forums	Policy communication methods; Clarity of expectations and consequence management
3. What challenges or barriers do you experience or observe when it comes to secure practices?	User awareness gaps and resistance to security controls are the primary challenges at present.	Limited training and unclear role-specific training expectations	Resource constraints and inconsistent or limited organisational engagement	Awareness gaps; Behavioural resistance; Resource limitations
4. What awareness or behaviour-reinforcing initiatives are in place?	Periodic online and web-based training sessions and system alerts to remind of trainings to be completed	Occasional awareness messages and reminders to complete web-based training are shared, and online session attendance is voluntary	Formal awareness campaigns, online and web portal training, and policy dissemination	Training frequency; Awareness mechanisms

5. What are the best practices you would recommend to strengthen cybersecurity culture in your organisation?	More frequent and role-specific training to empower the staff members	Practical, relatable awareness aligned to daily tasks, reward and incentives	Stronger leadership visibility and accountability mechanisms at all levels	Leadership influence; Training relevance
6. Additional suggestions for improving overall cybersecurity in your workplace?	Increased user involvement in security initiatives, gamified and mandatory training for better enforcement	Simplified guidance and clearer communication, security championship, and ambassadors	Integration of cybersecurity into organisational strategy	Employee engagement; Strategic alignment

Table 4-5 illustrates how initial codes were derived from participants' responses to the interview questions. For example, responses to Question 1 revealed differences in perceived responsibility for cybersecurity. IT staff framed cybersecurity primarily as a technical function, non-IT staff viewed it as secondary to operational priorities, while management emphasised strategic responsibility. These differences shaped the first codes *Perceived ownership of security and its strategic versus operational focus of cybersecurity*. In the same way, answers to Question 3 revealed obstacles such as *limited awareness, training limitations and resource shortages*, which were classified *as Awareness gaps, Behavioural resistance, and Resource limitations*. This demonstrates that the coding process captured not only share patterns but also role-based nuances among the participant groups.

Following the illustration of the coded data in Table 4-5, the researcher reviewed all generated codes across the full participant dataset. Table 4-6 presents a refined set of initial codes, with descriptions, supporting quotations, and links to emerging thematic categories.

Table 4-6: Refined Initial Codes

Initial Code	Description	Representative Quotation	Participant Group(s)	Participants (n)	Linked Theme
Policy Accessibility	References to unclear or outdated security policies	*"The security policy still talks about once awareness at induction of new employees, not reviewed." (7_NIT)*	NIT, ITP	9	Policy Clarity and Effective Communication
Policy Communication	Mentions of how policies are shared or communicated to staff	*"Cybersecurity is mentioned in the agenda at management forums only when something goes wrong." (19_MGT)*	MGT	5	Policy Clarity and Effective Communication
Role-Specific Training	Describes tailored awareness or training sessions for specific functions	*"We need training that fits what we actually do every day." (10_ITP)*	ITP, MGT	7	Continuous and Role-Specific Cybersecurity Training
Training Frequency	Refers to how often cybersecurity sessions are held	*"We haven't had any training this year." 14_NIT)*	NIT, ITP	8	Continuous and Role-Specific Cybersecurity Training
Collaboration Between Departments	Mentions cooperation or communication across departments	*"When IT and HR work together, things improve." (18_MGT)*	MGT, NIT, ITP	10	Collaborative Feedback and Cross-Organisational Engagement
Feedback Mechanisms	Comments on sharing security concerns or reporting issues	*"Sometimes we just fix it ourselves instead of reporting." (2_ITP)*	ITP, NIT	6	Collaborative Feedback and Cross-Organisational Engagement
Leadership Visibility	Mentions of leadership being	*"When our Chief Officer joined the awareness*	MGT	6	Visible Leadership

	visible or involved in cybersecurity initiatives	*session, everyone paid attention." (15_ITP)*			Commitment and Cultural Modelling
Executive Advocacy	Comments about top management driving or modelling cybersecurity culture	*"The CTO should lead by example and show that cybersecurity matters." (21_MGT)*	MGT	4	Visible Leadership Commitment and Cultural Modelling
Employee Motivation	References to rewards or recognition for secure behaviours	*"Rewarding people who complete their security training would motivate them." (15_NIT)*	MGT, ITP	5	Recognition, Incentives, and Sustained Employee Engagement
Awareness Campaigns	Mentions of posters, internal campaigns, or reminders	*"There are posters, but people hardly pay attention." (25_MGT)*	MGT, NIT	7	Recognition, Incentives, and Sustained Employee Engagement

**(n = Number of participants referencing the code)*

Table 4-6 provides a refined set of initial codes, their descriptions, and representative quotations, demonstrating how codes were grounded in participant narratives. For example, in the survey, the two pairs of codes, "Policy Accessibility" and "Policy Communication," were most often cited by both the IT and non-IT groups, indicating that these groups shared a common concern about the clarity and communication of cybersecurity policies. Likewise, the themes "Role-Specific Training" and "Training Frequency" indicate a lack of systematic learning, whereas "Leadership Visibility" and "Executive Advocacy" indicate the perceived importance of leadership modelling. These codes collectively reflect the organisational, behavioural, and communicative aspects of cybersecurity culture that constitute the conceptual basis for Phase 3.

The distribution of initial codes across participant groups, used to demonstrate coverage and saturation, is presented in Table 4-7.

Table 4-7: Code Distribution Frequency Summary

Code Category	**ITP (n)**	**NITP (n)**	**MGT (n)**	**Total Mentions**
Policy Clarity and Communication	4	5	5	14
Continuous and Role-Specific Training	5	4	3	12
Collaborative Engagement	3	4	3	10
Leadership Commitment	2	1	6	9
Employee Motivation and Incentives	2	3	2	7
Awareness Mechanisms	3	2	2	7

Table 4-7 summarises the distribution of initial codes across participant groups, indicating broad coverage and thematic saturation. For instance, references to "Policy Clarity and Communication" were found 14 times across all groups, whereas "Leadership Commitment" was most frequently mentioned among management participants. Such a spread of mentions justifies the sufficiency of the dataset in reflecting a variety of views on the cybersecurity culture.

Overall, this phase produced the initial set of 72 open codes, which were later consolidated into six code clusters aligned with emerging themes: policy clarity and communication; continuous and role-specific learning; collaborative engagement; leadership commitment; employee motivation and incentives; and awareness mechanisms. The full codebook list and supporting quotations are provided in Appendix F for transparency and external review. The codes were used to develop themes in Phase 3. To reduce bias, the researcher intentionally sought and coded passages that demonstrated employee motivation and collaboration, thereby ensuring that the behavioural and cultural aspects were not overlooked in the focus on structural issues. Such a reflexive practice aligns with Braun and Clarke's view that researcher subjectivity is a resource.

4.4.3 Phase 3: Constructing Initial Themes

After generating the initial codes in the second stage, the third stage examined these codes and combined them into conceptual clusters that symbolised the wider patterns of meaning. The stages here are more interpretive than automatic: the codes were grouped based on their shared conceptual relationships and their relevance to the research objectives. The aim was to move beyond descriptive coding toward identifying researcher themes with a central organising concept, as recommended by Braun and Clarke (2021).

The researcher reviewed all 72 open codes and organised them into six preliminary clusters. These clusters were then refined into the researcher themes that captured organisational, behavioural, and cultural dimensions of cybersecurity practice. Reflexive memos were used to document decisions, particularly where codes overlapped or required splitting. Table 4-8 illustrates the analytical progression from the initial codes to the researcher's themes.

Table 4-8: Code Clusters and Researcher Themes

Cluster (Mid-Level Category)	**Constituent Codes (Examples)**	**Researcher Theme (Working Title)**	**Central Organising Concept**
Governance Communication	Policy Accessibility; Policy Communication; Clarity of expectations	Policy Clarity and Effective Communication	Policies exist but lack clarity and consistent dissemination, creating gaps in understanding and compliance
Capability Development	Role-Specific Training; Training Frequency; Awareness mechanisms	Continuous and Role-Specific Cybersecurity Training	Staff recognise the need for ongoing, contextualised training to enable secure practices
Collaborative Engagement	Collaborative Feedback and Cross-Organisational Engagement	Collaborative Feedback and Cross-Organisational Engagement	Effective cybersecurity culture requires interdepartmental cooperation and feedback loops
Leadership Commitment	Leadership Visibility; Executive Advocacy	Visible Leadership Commitment and Cultural Modelling	Leadership behaviours and advocacy shape organisational priorities and influence cultural norms
Employee Motivation	Employee Motivation: Awareness Campaigns	Recognition, Incentives, and Sustained Employee Engagement	Incentives and recognition mechanisms reinforce secure behaviours and sustain engagement
Strategic Integration	Strategic alignment; Employee engagement	Cybersecurity Embedded in Organisational Strategy	Cybersecurity culture is strengthened when integrated into strategic planning and operational priorities

Table 4-8 illustrates the progression from mid-level code clusters to researcher themes by demonstrating how meaning was systematically developed from the qualitative data.

Conceptually related codes were grouped into coherent clusters, which then informed higher-order themes representing shared patterns across participant accounts.

For example, codes such as policy accessibility, policy communication, and clarity of expectations were clustered under Governance Communication, leading to the researcher's theme, Policy Clarity and Effective Communication. This theme reflects a common concern that, while cybersecurity policies exist, limitations in their clarity and dissemination create gaps in understanding and compliance. Similarly, codes related to training frequency and role-specific learning were grouped within Capability Development, informing the theme Continuous and Role-Specific Cybersecurity Training, which captures participants' recognition of the need for ongoing, contextualised training.

The remaining themes were developed through a similar interpretive process, highlighting the interrelated roles of collaboration, leadership, employee engagement, and strategic alignment in shaping cybersecurity culture. Consistent with Braun and Clarke's thematic analysis. These themes function as central organising concepts rather than descriptive topic summaries, reflecting patterned meanings generated through the researcher's interpretive engagement with the data. Therefore, this information guides the researcher into the thematic mapping. Figure 4-3 presents the Initial Thematic Map, which illustrates how the six clusters inform the six researcher themes.

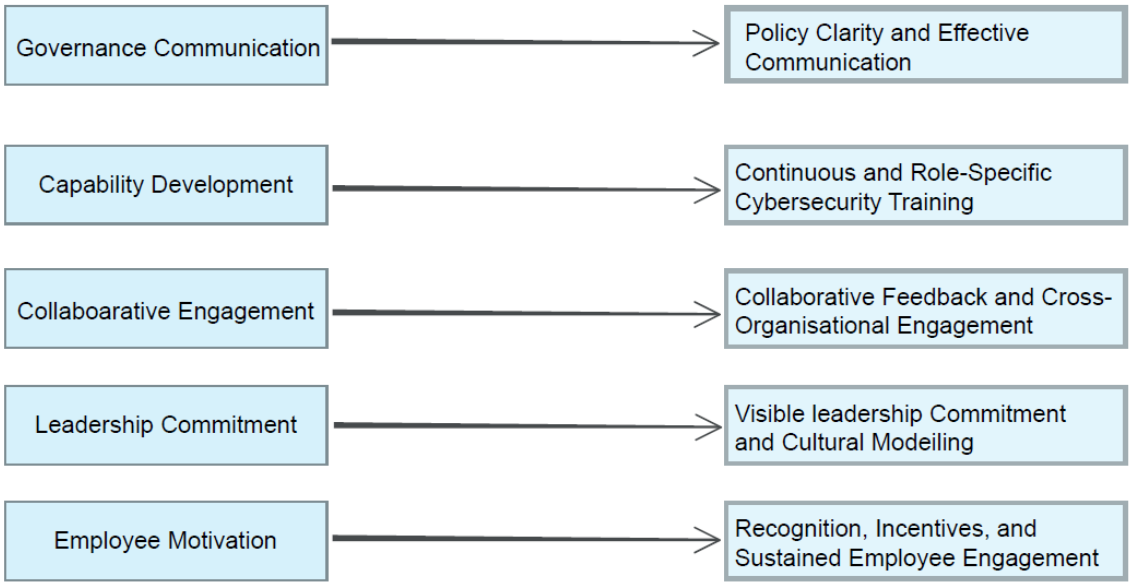


Figure 4-3: Initial Thematic Mapping

Figure 4-3 illustrates that clusters informed the researcher's themes, which encapsulate the organisational and behavioural drivers of cybersecurity culture. These themes were provisional and subject to refinement in phase 4, where coherence and boundaries were tested.

4.4.4 Phase 4: Reviewing and Refining Themes

Phase 4 focused on a detailed examination and further refinement of the initial themes to ensure that they were internally consistent and sufficiently distinct from one another. Since this process concerned the themes, it was natural to go back to the coded extracts in Atlas.ti, check if the theme adequately represented the same pattern of meaning across different participant groups, and confirm that the theme was in line with the research objectives. Where necessary, overlapping ideas were merged, weak codes were discarded, and theme boundaries were clarified. Conducting the review in this way is key to developing strong, conceptually valid themes rather than merely superficial topic summaries (Braun & Clarke, 2021). Table 4-9 clearly shows how preliminary themes changed through repeated examination.

Table 4-9: Themes Review Log

Preliminary Themes	Supporting Patterns Identified	Revision Action	Final Theme
Leadership involvement	Leadership visibility, executive advocacy, and role modelling	Expanded to include accountability and cultural modelling	Visible Leadership Commitment and Cultural Modelling
Awareness and training	Infrequent training, lack of role relevance, and low engagement	Refined to emphasise role-specific, continuous learning	Continuous and Role-Specific Cybersecurity Training
Policy clarity	Policy awareness gaps, inconsistent communication	Merged with policy feedback gaps for a broader scope	Policy Clarity and Effective Communication
Collaboration	Siloed practices, limited feedback loops	Expanded to include cross-departmental engagement	Collaborative Feedback and Cross-Organisational Engagement
Motivation and engagement	Low motivation, lack of incentives, interest in gamification	Consolidated into recognition and sustained engagement	Recognition, Incentives, and Sustained Employee Engagement
Informal advocacy	Ad-hoc peer guidance, absence of formal champions	Formalised as structured advocacy roles	Security Champions and Ambassadors

With reference to Table 4-9, as a case in point, the theme "Leadership involvement" was expanded to encompass not only leadership taking responsibility but also leaders serving as role models; hence, the new theme "Visible leadership commitment and cultural modelling". Likewise, the "awareness and training" subtheme was reworded to emphasise continuous, targeted learning rather than generic awareness sessions. The changes made the themes more conceptually coherent and distinct from one another, and each theme was supported by several data sources. The reviewed themes were organised into a thematic structure that informed the thematic map, which is summarised in Table 4-10.

Table 4-10: Summary of Themes Refinement

Preliminary Category	Revision Action Taken	Final Theme
Policy clarity and communication issues	Merged with “policy awareness” and “policy feedback gaps”	Policy Clarity and Effective Communication
Training gaps and behavioural control	Refined to emphasise role-specific, gamified learning and adaptive modules	Continuous and Role-Specific Cybersecurity Training
Collaboration and transparency	Expanded to include cross-departmental feedback loops and knowledge sharing	Collaborative Feedback and Cross-Organisational Engagement
Leadership visibility and engagement	Reframed to include accountability, modelling, and advocacy for security values	Visible Leadership Commitment and Cultural Modelling
Employee motivation and reward systems	Consolidated into recognition, reinforcement, and sustained engagement mechanisms	Recognition, Incentives, and Sustained Employee Engagement
Role models and peer influencers	Identified as a cross-cutting construct linking Themes 2–5; emphasises peer-led advocacy and departmental champions	Security Champions and Ambassadors

The summary of the table 4-10 review produced a stable set of six themes that were distinct, yet interconnected, each supported by rich qualitative evidence. These themes were then organised into a thematic structure and visualised on the thematic map (Figure 4-3), forming the basis for Phase 5, where themes were formally defined and named.

4.4.5 Phase 5: Defining and Naming Themes

In Phase 5, the researcher's themes were refined to reflect the final form by clarifying their scope, boundaries, and central organising concept. A short, clear name that reflects the theme and its relevance to the research objectives was assigned to each theme. If a level below the

theme was necessary to provide division and detail, then subthemes were created. Quotations from theme representatives were used to illustrate the themes and to demonstrate that the interpretations were grounded in participants' stories. Hence, this phase is critical to moving beyond descriptive summaries to analytic themes that tell a story about cybersecurity culture within the organisation (Braun & Clarke, 2021). Table 4-11 presents the final group of six themes, each characterised by its range, limitations, and main organising idea.

Table 4-11: Final Theme Definitions

Theme (Final Name)	**Definition (Scope)**	**Limits (Not About)**	**Central Organising Concept**	**Subthemes**	**Representative Quotations**
Policy Clarity and Effective Communication	The extent to which cybersecurity policies are accessible, understandable, and consistently communicated across the organisation	General organisational communication unrelated to cybersecurity	Policies exist but lack clarity and consistent dissemination, creating gaps in compliance	Policy accessibility; Communication channels	“Policies are shared, but they’re too technical for most staff.” (P07_NIT)
Continuous and Role-Specific Cybersecurity Training	Ongoing, contextualised training tailored to specific roles and responsibilities	Generic awareness campaigns without practical application	Staff recognise the need for applied learning to enable secure practices	Role-specific modules; Training frequency	“We need training that fits what we actually do every day.” (P10_ITP)
Collaborative Feedback and Cross-	Mechanisms for interdepartmental cooperation and feedback loops	Informal chats without structured feedback	Effective cybersecurity culture requires	Incident reporting; Departmental coordination	“When IT and HR work together, things

Organisational Engagement	on security practices		collaboration and shared responsibility		improve." (P18_MGT)
Visible Leadership Commitment and Cultural Modelling	Leadership behaviours and advocacy that signal cybersecurity as a priority	Leadership style critiques unrelated to security	Leadership visibility and accountability shape cultural norms	Executive advocacy; Role modelling	"When our Chief Officer joined the awareness session, everyone paid attention." (P15_ITP)
Recognition, Incentives, and Sustained Employee Engagement	Reward systems and motivational strategies that reinforce secure behaviours	General HR reward programmes unrelated to security	Incentives and recognition mechanisms sustain engagement and compliance	Gamification; Recognition programs	"Rewarding people who complete their security training would motivate them." (P15_NIT)
Security Champions and Ambassadors	Formalised peer advocacy roles that promote cybersecurity culture within departments	General peer support without structured responsibility	Champions act as cultural influencers and knowledge brokers	Departmental champions; Advocacy networks	"Security advice shared as an ad-hoc activity—formal champions would help." (P25_MGT)

Table 4-11 presents the final set of six themes, each defined by its scope, boundaries (i.e., what the theme does not capture), central organising concept, associated subthemes, and illustrative quotations. For example, Policy Clarity and Effective Communication focuses specifically on how cybersecurity policies are accessed and communicated, rather than on

broader organisational communication practices. Subthemes such as policy accessibility and communication channels provide further structure. While participant quotations illustrate how these issues are experienced in practice, they also enhance the trustworthiness of the analysis.

Collectively, the six themes capture key organisational, behavioural, and cultural dimensions of cybersecurity practice. These dimensions underpin the thematic map and interpretive narrative presented in Section 4.5, in which each theme is explored in greater depth and theoretically contextualised using Social Cognitive Theory and Protection Motivation Theory. Therefore, this phase represents a critical link between the analytic process and the detailed empirical presentation of findings in Phase 6.

4.4.6 Phase 6: Producing the Report and Interpreting the Findings

This section presents the final themes derived from the data, explains their significance with respect to the research questions, and synthesizes theoretical perspectives to inform the preliminary cybersecurity culture framework. Phase 6 involves telling a coherent analytic story supported by carefully chosen extracts.

4.4.6.1 Overview of Final Themes

Table 4-12 summarises the analytic structure derived in Phases 3–5 and outlines the basis for the narrative below. Each theme is consistently defined by a single concept.

Table 4-12: Final Themes, Definitions and Illustrative Extracts

Theme (final name)	Concise definition	Quoted extract
Policy Clarity and Effective Communication	Policies are present but often inaccessible or inconsistently communicated, creating gaps in shared understanding and compliance	"The security policy still talks about once awareness at induction… not reviewed." *(P07_NIT)*
Continuous and Role-Specific Cybersecurity Training	Ongoing, contextualised training is required to enable task-level enactment of secure practices	"We need training that fits what we actually do every day." *(P10_ITP)*
Collaborative Feedback and Cross-Organisational Engagement	Effective culture depends on cross-departmental cooperation and structured feedback/incident loops	"When IT and HR work together, things improve." *(P18_MGT)*
Visible Leadership Commitment and Cultural Modelling	Leadership visibility, accountability, and modelling signal cybersecurity as a strategic priority	"When our Chief Officer joined the awareness session, everyone paid attention." *(P15_ITP)*
Recognition, Incentives, and Sustained Employee Engagement	Reinforcement mechanisms (recognition, gamification, incentives) sustain secure behaviours	"Rewarding people who complete their security training would motivate them." *(P15_NIT)*
Security Champions and Ambassadors	Formalised peer-advocacy roles diffuse norms, translate policy into practice, and broker knowledge	"Security advice is ad-hoc—formal champions would help." *(P25_MGT)*

4.4.6.2 Narrative Presentation and Interpretation of Themes

The following subsections present each theme in the format: (a) analytic summary; (b) key supporting extract(s); (c) interpretation linked to the research questions; (d) brief theoretical integration (SCT/PMT) theories.

4.4.6.2.1 Theme 1: Policy Clarity and Effective Communication

The analytical process demonstrated that participants from all organisational levels acknowledged the existence of cybersecurity policies but described them as difficult to interpret, overly technical, and inconsistently communicated. This lack of clarity and accessibility diluted shared expectations and held up the consistent application of secure practices across the organisation. The supporting evidence was highlighted by the participants' next extracts.

“The security policy still talks about once awareness at induction… not reviewed.” (P07_NIT)

“Cybersecurity is on the agenda at management forums only when something goes wrong.” (P19_MGT)

The results for RQ1 indicate that making policies available and establishing regular, two-way communication channels are key to a strong cybersecurity culture. According to the data, if cybersecurity policies are not regularly updated and their distribution is not clearly explained, it becomes difficult for employees to grasp the expected behaviours, which then leads to varying levels of compliance. Regarding RQ2, the clear and workable communication of the policy can help the employees to respond more effectively and doubt less the efficiency of the proposed measures, and also, they would be more inclined to believe that the actions are both easy and effective, and at the same time, perceived barriers to secure behaviours are lowered.

Thus, from a theoretical perspective, these results support Social Cognitive Theory (SCT), which, among other things, considers the influence of reinforcement and social norms on behaviour. In fact, ones that can be directly enacted and are supported by the surrounding environment would constitute scaffolds that build one's self-efficacy and shape positive outcome expectations. Furthermore, Protection Motivation Theory (PMT) implies that readily available and comprehensible policies help elevate the sense of response efficacy and reduce the perception of response costs. Consequently, employees become more willing to implement and uphold security-related behaviours.

4.4.6.2.2 Theme 2: Continuous and Role-Specific Cybersecurity Training

The analysis demonstrates that participants consistently highlighted the need for ongoing, practical, and role-relevant cybersecurity training. They indicated that generic, infrequent awareness sessions were neither able to address emerging threats nor maintain engagement; by contrast, tailor-made, interactive training methods were more effective in developing skills and self-assurance. This has been supported by the participants' extract below.

“We haven’t had any training this year.” (P14_NIT)

“We need training that fits what we actually do every day.” (P10_ITP)

Interpretation of RQ1: The findings identify continuous, context-specific training as a critical enabler of cybersecurity culture. The data indicate that when training aligns with employees' work environments and is delivered frequently, it increases not only knowledge retention but also the ability to respond to new threats. In the case of RQ2, providing employees with role-specific training increases their self-efficacy and coping appraisal, thereby equipping them with the skills and confidence to engage in safe behaviours in their daily work.

According to Social Cognitive Theory (SCT), frequent and pertinent training not only provides employees with opportunities to learn through observation but also strengthens their self-efficacy (i.e., their belief in their ability to succeed in specific situations). This process enables employees to adopt secure behaviours that they have repeatedly observed modelled by their peers. While SCT emphasises learning through observation and self-belief, Protection Motivation Theory (PMT) further emphasises that employees' confidence in managing risks is crucial for motivating protective actions. In this context, PMT suggests that continuous training enhances coping appraisal and employees' evaluation of their ability to handle threats by increasing their perceived ability to manage cyber risks effectively, thereby motivating sustained protective behaviour.

4.4.6.2.3 Theme 3: Collaborative Feedback and Cross-Organisational Engagement

Participants recognised that collaboration between departments, such as through joint training sessions or cross-functional incident response teams, and regular feedback mechanisms, such as monthly security debriefs, play a major role in building a strong culture of cybersecurity. Such collaborative efforts and feedback channels help ensure consistent communication

across the organisation, enable the rapid identification of vulnerabilities, and foster shared responsibility for upholding security practices. By working together and openly discussing security issues, departments can learn from one another's experiences and collectively respond to emerging threats, thereby strengthening the organisation's cybersecurity culture. The findings showed that a lack of communication among departments and inadequate feedback mechanisms make it difficult for the organisation to learn together, reduce risks associated with awareness, and share less accountability for security practices. This analysis has been supported by the participants' extracts below.

"When IT and HR work together, things improve." (P18_MGT)

"Sometimes we just fix it ourselves instead of reporting." (P02_ITP)

With respect to RQ1, the findings highlight that an effective cybersecurity culture depends on formalised collaboration platforms and transparent feedback channels. Participants also noted that, in addition to securely sharing cybersecurity responsibilities with other departments, completing this task requires coordination across different roles and hierarchical levels. When there is no cooperation, the methods one seeks to apply are fragmented and lack organisational learning. To answer RQ2, collaborative setups and feedback networks not only increase social support but also strengthen individuals' sense of security, thereby enabling workers to learn from their colleagues, share their experiences, and collectively address security issues.

Social Cognitive Theory (SCT) offers a lens for understanding how collaboration and feedback can serve as tools to promote social learning and observational learning, thereby enabling employees to mimic the security behaviours they have observed in others. On the other hand, Protection Motivation Theory (PMT) describes the role of feedback in strengthening the coping appraisal process, as it provides both reassurance and guidance, thereby boosting employees' confidence in their ability to respond to cybersecurity challenges.

4.4.6.2.4 Theme 4: Visible Leadership Commitment and Cultural Modelling

Participants consistently identified visible leadership engagement as a decisive factor in shaping cybersecurity culture. The data analysis revealed that when leaders actively champion cybersecurity initiatives and model secure behaviours, employees are more likely to perceive cybersecurity as a strategic organisational priority. By contrast, absent or inconsistent leadership participation in team meetings was associated with decreased motivation and weaker adherence to security protocols. This association is illustrated in the following extracts, which detail instances in which a lack of leadership involvement led to decreased motivation and nonadherence to protocol.

“Top management, including the CTO, should advocate change.” (P24_MGT)

“When our Chief Executive Officer joined the awareness session, everyone paid attention.” (P15_ITP)

This theme addresses RQ1 by building on established findings that sustained leadership commitment and cultural modelling are foundational requirements for cultivating a resilient cybersecurity culture. Evidence demonstrates that leadership visibility, advocacy, and resource allocation legitimise cybersecurity as a shared responsibility and reinforce behavioural alignment across all organisational levels. For RQ2, leaders' active participation in cybersecurity initiatives improves both threat assessment and coping appraisal among employees, signalling organisational support and elevating the perceived importance of secure practices.

From a theoretical perspective, our findings that employees consistently adopt secure password practices align strongly with Social Cognitive Theory (SCT), in which leadership serves as the primary behavioural model. Specifically, when managers visibly demonstrate secure behaviours such as consistently locking their computers when leaving their desks or regularly updating passwords, employees learn and internalise these practices through observation and imitation. This modelling effect highlights the practical implications of SCT, illustrating how employees are more inclined to emulate secure habits when they see leaders prioritising cybersecurity in their everyday actions. Additionally, the Protection Motivation

Theory (PMT) posits that visible leadership engagement intensifies perceived threat and coping capacity; thus, employees are motivated by the organisation's commitment and by the support systems they observe.

4.4.6.2.5 Theme 5: Recognition, Incentives, and Sustained Employee Engagement

The participants highlighted that recognition, and rewards were key to maintaining interest in cybersecurity policies. The data analysed indicated that traditional compliance-driven approaches often failed to motivate long-term behavioural change, whereas reward-based and interactive initiatives fostered greater participation, accountability, and a sense of ownership among employees. These observations are supported by the following extracts.

“Rewarding people who complete their security training would motivate them.” (P15_NIT)

“There are posters, but people hardly pay attention.” (P25_MGT)

This theme addresses RQ1 by highlighting the findings that identity recognition, incentives, and sustained engagement are essential organisational levers for embedding secure behaviours. The evidence demonstrates that when employees receive acknowledgement for positive security actions, whether through formal rewards, gamified activities, or public recognition, motivation and adherence to cybersecurity protocols are significantly enhanced. For RQ2, the presence of incentive structures and ongoing engagement reinforces behavioural consistency by increasing employees' perceived value and relevance of secure practices.

One theory that can explain this is Social Cognitive Theory (SCT), whereby recognition and rewards serve as positive reinforcers that encourage the repetition and social modelling of secure behaviours not only within a department but throughout the organisation. Moreover, the Protection Motivation Theory (PMT) supports this interpretation, as reward mechanisms enhance coping appraisal and response efficacy, leading employees to engage in protective behaviours when their efforts are recognised, valued, and effective.

4.4.6.2.6 Theme 6: Security Champions and Ambassadors

The participants consistently recognised the merit of assigning departmental security champions and ambassadors to promote secure practices and sustain engagement. The data analysis showed that peer-led advocacy helps narrow the gap between policy intent and day-to-day practice by providing easily understandable guidance and promoting cybersecurity values at the grassroots level. The supporting extract is next.

"Security advice shared as an ad-hoc activity, a formal champion would help." (P25_MGT)

"Having someone in the department who understands cybersecurity makes it easier to ask questions and follow good practices." (P17_NIT)

In relation to RQ1, the findings identify the establishment of security champions and ambassadors as a critical organisational mechanism to support cybersecurity culture. The evidence demonstrates that when trusted peers serve as advocates and role models, employees are more likely to internalise secure behaviours and seek guidance, thereby enhancing collective responsibility and behavioural consistency. As far as RQ2 is concerned, departmental champions appear to strengthen both pathways for spreading cybersecurity norms, i.e., observational learning (social interaction) and protective motivation (coping appraisal), resulting in sustained commitment across organisational boundaries.

Drawing on Social Cognitive Theory (SCT), security champions and ambassadors function as proximate role models, enabling observational learning and reinforcing self-efficacy through peer influence. Protection Motivation Theory (PMT) also backs up this kind of interpretation. Peer advocacy will help individuals identify coping strategies and response efficacy; therefore, employees are motivated to adopt and maintain security behaviours through peer support, which is consistently available alongside peer advocacy, reinforcing the relevance of cybersecurity practices.

4.4.6.3 Integrated Thematic Interpretation

This section discusses the results of the six data-driven themes, explaining how these enablers work together as a holistic system that ultimately determines the organisation's cybersecurity

culture. Rather than operating independently, the themes work together and reinforce one another, thereby increasing their combined effect on organisational behaviour.

The thematic map illustrates this systemic relationship. The six themes operate as an interdependent system: leadership commitment (Theme 4) legitimises role by prioritising cybersecurity, endorsing policy clarity (Theme 1) and funds allocation of resources for continuous and role-specific training (Theme 2); in turn, collaboration feedback and cross-organisational engagement (Theme 3) converts knowledge gained through training into shared practice; recognition and incentives (Theme 5) reinforce and sustains secure behaviours over time; champions and ambassadors (Theme 6) facilitate the diffusion of cybersecurity norms and provide situated localised guidance and peer-based coaching within departments. This systemic view aligns with guidance to map relationships among themes. These themes support the diffusion of cybersecurity values across different functional areas. Figure 4-4 illustrates the thematic map of the conceptual interaction diagram for cybersecurity culture enablers.

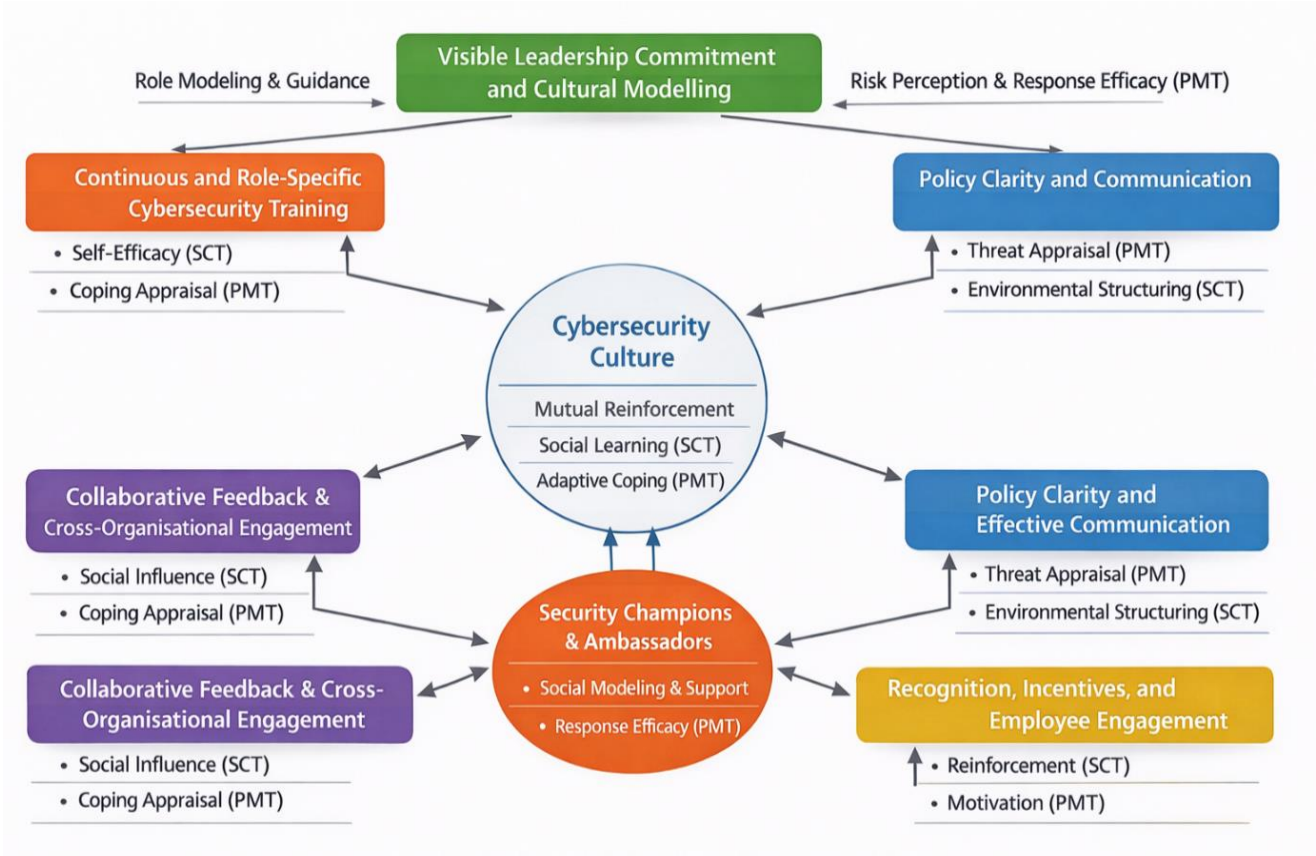


Figure 4-4: Thematic Map of Cybersecurity Culture Enablers

Figure 4-4 presents this thematic map as a conceptual interaction diagram, visually demonstrating how the six enablers collectively support the diffusion and reinforcement of cybersecurity values across the organisation. The map highlights that cybersecurity culture emerges through the dynamic interaction of strategic, structural, behavioural, and social mechanisms, rather than through isolated interventions.

Collectively, these interrelationships demonstrate that the effectiveness of each enabler is amplified when implemented in concert with the others, resulting in a cohesive and self-reinforcing system of influence. The thematic map was refined to ensure that each data-driven theme is represented and integrated consistently with qualitative thematic analysis

principles. This integrated perspective provides the empirical foundation for developing the final cybersecurity culture framework, as presented in the following section.

4.4.6.4 Integrated Thematic Evidence Matrix

To support cross-theme synthesis and enhance analytical transparency, an integrated thematic evidence matrix (mapping themes to empirical indicators, theory, and framework components) was developed to consolidate evidence across themes 1-6. Table 4-13 illustrates the evidence matrix findings and concepts.

Table 4-13: Integrated Evidence Matrix for Cybersecurity Culture Enablers

Theme Name	Empirical Indicators	SCT/PMT Theories and Constructs	Framework lever (design implication)	Example Measure (KPI)
Policy Clarity & Effective Communication	Mentions of outdated policy; sporadic comms (P07_NIT; P19_MGT)	PMT: response efficacy increases; response cost decreases. SCT: outcome expectations clarified	Plain-language policy; two-way comms; policy FAQs and owners	% staff passing policy comprehension checks; time-to-answer policy queries
Continuous & Role-Specific Training	Need for applied; frequent training (P10_ITP; P14_NIT)	SCT: self-efficacy increases; PMT: coping appraisal increases	Role-based micro-learning, task simulations, refresher cadence	Course completion & assessment scores; on-the-job task accuracy
Collaborative Feedback & Engagement	“Fix it ourselves” vs. report; inter-dept gains (P02_ITP; P18_MG	SCT: observational learning; collective efficacy. PMT: salient threat plus high response efficacy	Incident learning forums; feedback SLAs; shared dashboards	% incidents with feedback returned; cross-unit participation rate
Visible Leadership Commitment	Leader presence/modelling (P15_ITP; P21_MGT)	SCT: modelling & vicarious reinforcement; PMT: credible cues raise coping appraisal	Executive walk-throughs: leadership KPIs tied to cyber culture	# exec-led sessions/quarter; resource allocation stability
Recognition & Incentives	Motivation via rewards; low salience of posters (P15_NIT; P25_MGT)	SCT: reinforcement; PMT: response cost decreases, motivation increases	Gamified challenges; recognition programme	Participation rate; challenge completion; behaviour “streaks”
Champions & Ambassadors	Call for formal champions (P25_MGT)	SCT: peer modelling; PMT: response efficacy ↑ via local exemplars	Departmental champions network; office hours	# active champions; # interactions; local resolution rate

Table 4-13 illustrates an evidence matrix mapping themes to empirical indicators and theoretical components. The matrix serves as an analytical bridge between the thematic findings and the development of the refined cybersecurity culture framework presented later in

this chapter. It aligns each theme with its supporting data sources, including interview excerpts, frequency of occurrence, and theoretical interpretation informed by two theories (SCT and PMT). Additionally, it provides a structured overview of how individual data points contribute to a greater understanding of cybersecurity culture within the organisation. The integrated matrix performs three key analytical functions:

- ◊ The study initially synthesises evidence from various themes that illustrate how each element of the framework influences cybersecurity behaviour. Such a unification avoids the fragmentation of results and ensures that themes are understood as components rather than isolated observations.
- ◊ Second, the matrix strengthens analytical and traceability by explicitly linking empirical evidence to each theme. This enables one to trace how raw data informed theme development and how these themes, in turn, informed the conceptualisation of cybersecurity culture enablers.
- ◊ Thirdly, the matrix makes it visible how theoretical alignment works by relating each theme with the appropriate theories. Such a theoretical mapping guarantees that the matrix covers the behavioural, cognitive, and organisational aspects of cybersecurity culture.

These themes indicate that a holistic, multi-level approach is vital for developing a cybersecurity culture that integrates individual actions, organisational systems, and leadership. These findings inform the developed framework, which will be detailed in the next section.

4.5 Interpretation of Research Findings

This section provides an analytical interpretation of the six final themes derived from the qualitative data analysis. The purpose is threefold: first, to demonstrate how the findings collectively address the study's sub-research questions (RQ1, RQ2 and RQ3); second, to interpret the findings through the lens of Social Cognitive Theory (SCT) and Protection Motivation Theory (PMT); and third, to consolidate interview grounded insights that inform the design and refinement of the preliminary cybersecurity culture framework presented in

Sections 4.5 and 4.6. Instead of restating the thematic findings, this section interprets the themes by explaining why they matter, how they function behaviourally and organisationally, and what they imply for framework development within the telecommunications context.

4.5.1 Theme-by-Theme Interpretations

Theme 1: Policy Clarity and Effective Communication: From an organisational perspective (RQ1), the findings indicate that cybersecurity culture is strengthened when policies are accessible, contextualised, and routinely communicated through clear, two-way channels. Participants emphasised that unclear or outdated policies create ambiguity, reducing compliance and confidence in secure practices. Building on these organisational insights, it is evident that clarity and regular communication are not only administrative tasks but foundational to fostering trust and actionable understanding across the workforce.

Building on these organisational insights, theoretical analysis reveals that clear and actionable policy communication enhances response efficacy and reduces response costs (PMT), while also supporting self-efficacy and positive outcome expectations (SCT). These mechanisms collectively empower employees to enact secure behaviours with confidence, as they understand both the rationale for policies and their own ability to comply. In this way, the theories reinforce that effective policy communication is not only about delivering information, but also about motivating and enabling behavioural change at scale.

Translating these findings into a practical framework design (RQ3), this theme informs the framework by positioning policy clarity as a structural enabler. Specifically, the development of plain-language policy packs directly addresses ambiguity by ensuring that all employees, regardless of role or technical expertise, understand expectations and requirements, thus supporting both SCT's emphasis on self-efficacy and PMT's focus on reducing response costs.

Assigning named policy owners increases accountability and ensures that employees have clear points of contact for questions or clarification, thereby strengthening two-way communication and trust. Maintaining living FAQs provides an up-to-date, easily accessible resource that demystifies complex or evolving issues, reinforcing continuous learning and

positive outcome expectations. Implementing quarterly policy updates prevents policies from becoming outdated, which is vital for maintaining compliance and confidence, as it reassures employees that the guidance remains relevant to emerging threats and operational realities. Collectively, these actions address the identified challenges by making policies more understandable, accessible, and responsive, thus embedding the principles of SCT and PMT into the practical workings of the organisation's cybersecurity culture.

Theme 2: Continuous and Role-Specific Cybersecurity Training: In response to Research Question 1 (RQ1), the findings indicate that generic or isolated sessions are insufficient to address the practical challenges and evolving threats necessary to maintain secure behaviour. Instead, continuous, role-relevant training is essential to translate knowledge into consistent, secure practices. Participants. To begin with, role-specific modules positively influence self-efficacy (SCT) and further coping appraisal (PMT), which, in turn, leads to higher levels of protection motivation and behavioural adoption, thereby addressing the theoretical integration (RQ2). Implication for Framework Design (RQ3). In our view, training should be incorporated into a capability-building programme. The design actions are role-based micro-learning, scenario-driven interactive simulations, and a six-month training refresher.

Theme 3: Collaborative Feedback and Cross-Organisational Engagement: With respect to (RQ1), the findings highlighted that structured collaboration and incident-feedback loops foster shared responsibility and organisational learning. Participants highlighted that siloed practices and a lack of feedback hinder collective improvement. In theory (RQ2), peer learning encourages learning through observation and builds group confidence (SCT). It also helps increase awareness of threats and confidence in responses (PMT) through the sharing of experiences. For Framework Design (RQ3), collaborative strategies should serve as structures that support social reinforcement. Suggested steps include establishing incident-review forums, creating feedback SLAs, and forming communities of practice that bring together different functions.

Theme 4: Visible Leadership Commitment and Cultural Modelling: In answering (RQ1), the data confirm that leadership visibility and modelling signal organisational priorities, allocate

resources, and legitimise secure conduct. Participants consistently linked leadership engagement to employee motivation and compliance. From a theoretical perspective (RQ2), leaders act as behavioural models (SCT), enhancing coping appraisal and reducing barriers to action (PMT), which motivates employees to adopt secure behaviours. Implication for Framework Design (RQ3): Leadership commitment must be positioned as a foundational driver. Design actions include scheduling executive walk-throughs, integrating leadership performance indicators linked to cybersecurity culture, and ensuring consistent resource commitments.

Theme 5: Recognition, Incentives and Sustained Employee Engagement: In relation to (RQ1), the findings show that recognition and incentives transform cybersecurity from a compliance burden to a valued organisational practice. Additionally, the findings indicate that reinforcement mechanisms maintain attention and normalise secure habits over time. Theoretically (RQ2), recognition functions as reinforcement (SCT), improves coping appraisal and lowers response costs (PMT), supporting durable behavioural change. Implication for Framework Design (RQ3): Gamification and incentives should act as accelerators of behavioural change. Recommended actions include introducing gamified challenges, recognition schemes, and secure-behaviour badges.

Theme 6: Security Champions and Ambassadors: Addressing (RQ1), the findings indicate that security champions translate organisational intent into context-specific practices within departmental realities and act as trusted advocates. Participants viewed champions as essential to bridge strategic priorities and operational realities. From a theoretical perspective (RQ2), security champions enable observational learning and strengthen self-efficacy (SCT), while increasing response efficacy (PMT) through local examples and peer influence. Research Question 3 suggests that security champions must be impetuous change agents. Therefore, the design actions to consider are establishing a departmental champion network, equipping champions with methodical playbooks, and providing champion office hours for peer support.

Collectively, these interpretations demonstrate how the six themes function as interdependent enablers of cybersecurity culture and how SCT and PMT jointly explain their behavioural influence. Subsection 4.5.2 synthesises these themes into an integrated system, providing the conceptual bridge to the preliminary and refined cybersecurity culture framework, which is further presented in Sections 4.6 and 4.7 within this chapter.

4.5.2 Integrated Interpretation of Cybersecurity Culture Enablers

The thematic map in Figure 4-5 illustrates how the six data-driven themes operate as an integrated system rather than standalone elements. Visible leadership commitment and cultural modelling (Theme 4) legitimise cybersecurity as an organisational priority and support other enablers. These leadership actions directly influence continuous and role-specific cybersecurity training (Theme 2), such as executive endorsement, which enhances participation and reinforces the importance of ongoing learning. Policy clarity and effective communication (Theme 1) are like the pillars for leadership that help you see exactly what training outcomes and leadership intent mean for you, through what is expected of you. Furthermore, clear and accessible policies limit misunderstandings, define roles, and facilitate consistent, reliable adherence to security measures.

Cross-organisational collaboration and feedback (Theme 3) help embed culture by promoting shared responsibility and encouraging organisational learning. Prearranged collaboration forums, together with open feedback channels, facilitate knowledge sharing and working together to solve problems. Recognition and awards, as well as continued employee engagement (Theme 5), serve as motivational factors that help maintain focus and strengthen positive habits through gamification and reward mechanisms. These measures make information security not only a matter of compliance but also a good practice in internal operations. Finally, security champions and ambassadors (Theme 6) bridge the gap between strategic priorities and operational realities. Champions act as trusted role models within departments, translating organisational expectations into context-specific practices and promoting peer-led advocacy. Figure 4-5 shows the thematic map with the cybersecurity culture enablers.

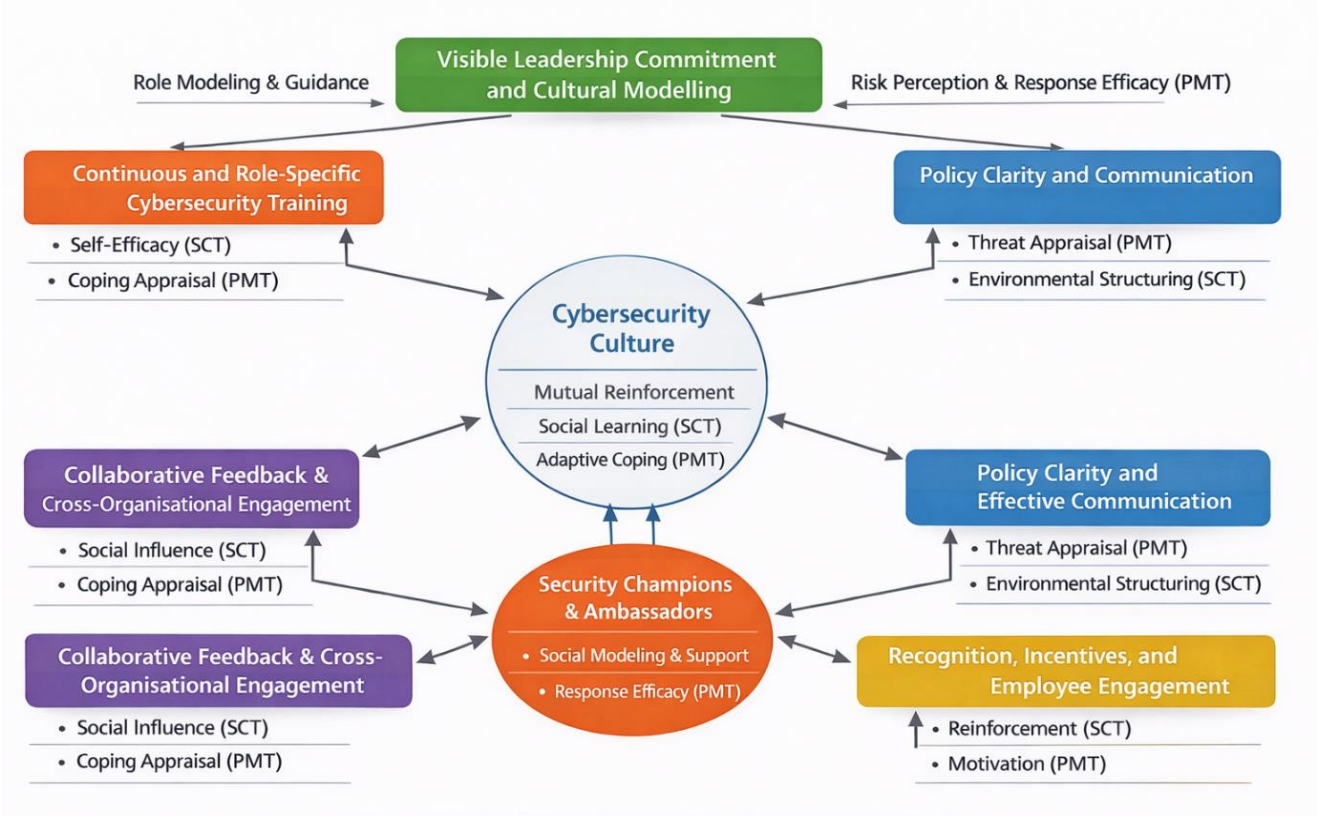


Figure 4-5: Integration Map for Cybersecurity Culture Enablers

Figure 4-5 collectively demonstrated that cybersecurity culture is shaped through the dynamic interaction of strategic, structural, behavioural, and social mechanisms. No single theme is sufficient on its own; their effectiveness is significantly heightened when implemented together, forming a mutually reinforcing system. These enablers create a system in which they help one another achieve sustainable cultural change. This integrated perspective provides a conceptual bridge between the findings and the refined cybersecurity culture framework discussed in further Sections 4.6 and 4.7.

4.5.3 Interpretation of Findings in Relation to the Literature

Research areas identified in this study align strategically with the literature segments discussed in Chapter Two. The similarities were most notable with the topics of leadership, training, policy governance, collaboration, reinforcement mechanisms, and champion models. However, the empirical analysis yielded context-specific names and organising concepts that reflect

participants' lived experiences. For example, the theme of visible leadership commitment and cultural modelling extends beyond generic leadership references by emphasising modelling behaviours and cultural signalling, while recognition, incentives, and sustained employee engagement integrate motivational and reinforcement dynamics that are often treated separately in prior studies. This separation is methodologically appropriate within thematic analysis, which prioritises identifying shared meaning patterns grounded in the dataset rather than replicating existing labels in the literature. This contextual specificity enhances the practical relevance of the findings and ensures that the refined framework is tailored to the case study's organisational and sectoral realities.

4.5.4 Methodological Rigour and Trustworthiness

To ensure methodological rigour and enhance the credibility of the findings, the study adhered to the principles of Reflexive Thematic Analysis (RTA) as articulated by Braun and Clarke. RTA sees the researcher as an active interpreter of meaning rather than a neutral coder, and emphasises transparency, reflexivity, and analytic depth. Throughout the analytic process, decisions, reflections, and interpretive developments were systematically recorded using reflexive memos and a structured audit trail. The reflexive memos documented the researcher’s evolving insights, positionality, and interpretive shifts, supporting continuous critical reflection on how meaning was being constructed. The audit trail provided a transparent chronological record of coding decisions, theme refinements, and analytic justifications, thereby enhancing dependability and traceability.

Themes were reviewed iteratively for internal coherence, conceptual distinction, and alignment with the study questions. This iterative refinement ensured that the final themes reflected meaningful patterns of shared understanding rather than merely summarising topics. In line with the conventions of RTA, participant quotations were selected for their analytical contribution rather than to represent the majority view. The purpose was to illuminate the essence of each theme, substantiate interpretive claims, and demonstrate grounding in participants' lived experiences. When tightly integrated, these measures support the credibility, coherence, and transparency of the analysis, thereby providing a robust empirical foundation

essential to the inception and subsequent development of the refined cybersecurity culture framework presented in the following section.

4.6 Development of the Empirically Informed Cybersecurity Culture Framework

Building on the preliminary conceptual framework presented in Chapter Two through RO1 and RO2, this section explains how the framework was further developed using the empirical findings of the study. RO1 provided the organisational, human and governance requirements, while RO2 defined the core components and characteristics of an effective cybersecurity culture framework. These literature derived elements were then examined against participants' insights and thematic findings to confirm, adapt or extend the framework for Namibia's telecommunications sector. This progression shows how literature-derived components were examined, confirmed, adapted or extended through empirical evidence, consistent with contemporary qualitative case study logic and theory-informed framework development (Khadka & Ullah, 2025; Annamalah et al., 2026). The improved cybersecurity culture framework architecture is presented, grounded in theory to support Chapter Two and the empirical insights in Chapter Four. The framework centres on six main components and highlights the design levers, governance structures, and implementation logic to which each component is connected. Taken together, these provide a workable roadmap for cybersecurity culture in the telecommunications sector.

4.6.1 Foundational Principles of Developing a Framework

Although the preceding sections presented data-driven themes, these are here abstracted into guiding principles to inform the design and operationalisation of the framework. These foundational principles reflect recurring patterns that reflect both theoretical constructs and empirical findings. The development of this framework is guided by the following five principles.

- ◊ **Leadership-Anchored Culture**: Cybersecurity should be elevated as a top strategic priority across the organisation and demonstrated visibly by top management to authorise secure behaviour and indicate ongoing commitment.

- ◊ **Enablement Over Compliance**: Policies, training, and controls must serve to empower employees. These measures are designed to foster a culture in which individuals engage confidently in secure behaviours, rather than simply adhering to procedures or fulfilling compliance requirements.
- ◊ **Learning Loops and Collective Responsibility**: Collaborative efforts and established feedback processes should formalise ongoing shared learning, drive continuous improvement, and reinforce collective accountability for cybersecurity results.
- ◊ **Behavioural Reinforcement and Motivation**: Implementing recognition programmes and incentive schemes is essential to promote positive security behaviours, maintain user engagement, and establish secure practices as standard within the organisation.
- ◊ **Local Advocacy and Translation**: Security champions serve as cultural liaisons within the organisation, translating corporate objectives into actionable, locally relevant solutions and promoting peer engagement.

These principles establish the normative logic of the framework and guide the configuration of its structural components.

4.6.2 Core Components and Design Levers

Operationally, the framework comprises six interconnected components, each supported by design levers derived directly from the empirical themes. Altogether, these components translate the framework principles into actionable organisational mechanisms. Table 4-14 presents an overview of these core components and their associated design levers, illustrating how each component is operationalised within the framework.

Table 4-14: Preliminary Development of Framework Components and Design Levers

Framework Component	**Key Design Levers**	**Rationale (Linked to Theme)**
Governance and Policy Enablement	Plain-language policy packs; named policy owners; quarterly updates	Policy Clarity and Effective Communication
Capability and Learning	Role-based learning pathways; simulations; six-month refresh cycles	Continuous and Role-Specific Cybersecurity Training
Collaboration and Learning Loops	Incident review forums; feedback SLAs; communities of practice	Collaborative Feedback and Cross-Organisational Engagement
Leadership and Cultural Signalling	Executive modelling calendar; leadership KPIs; visible resourcing commitments	Visible Leadership Commitment and Cultural Modelling
Motivation and Reinforcement	Gamified campaigns; recognition tiers; secure-behaviour badges	Recognition, Incentives, and Sustained Employee Engagement
Local Advocacy and Translation	Departmental champion networks, playbooks, and dedicated office hours	Security Champions and Ambassadors

As shown in Table 4-14, the components span strategic, managerial, and behavioural dimensions, reflecting the multi-layered nature of cybersecurity culture within telecommunications organisations. The associated design levers indicate specific organisational practices, such as leadership commitment, targeted training, governance, and reinforcement strategies, that are necessary for effective functioning. This alignment ensures that the framework remains both analytically grounded and practically applicable by connecting abstract principles to concrete organisational actions. This configuration ensures that behavioural, structural, and social mechanisms are addressed in an integrated manner.

4.6.3 Framework Layers and Structural Logic

The framework adopts a three-tiered layered design to reflect the interdependence between strategic direction, operational implementation, and behavioural reinforcement, as depicted in Figure 4-6. Figure 4-6 visually illustrates the hierarchical yet interconnected structure of the Cybersecurity Culture Framework, demonstrating how a leadership-driven strategy is translated into operational practices and subsequently reinforced through behavioural mechanisms.

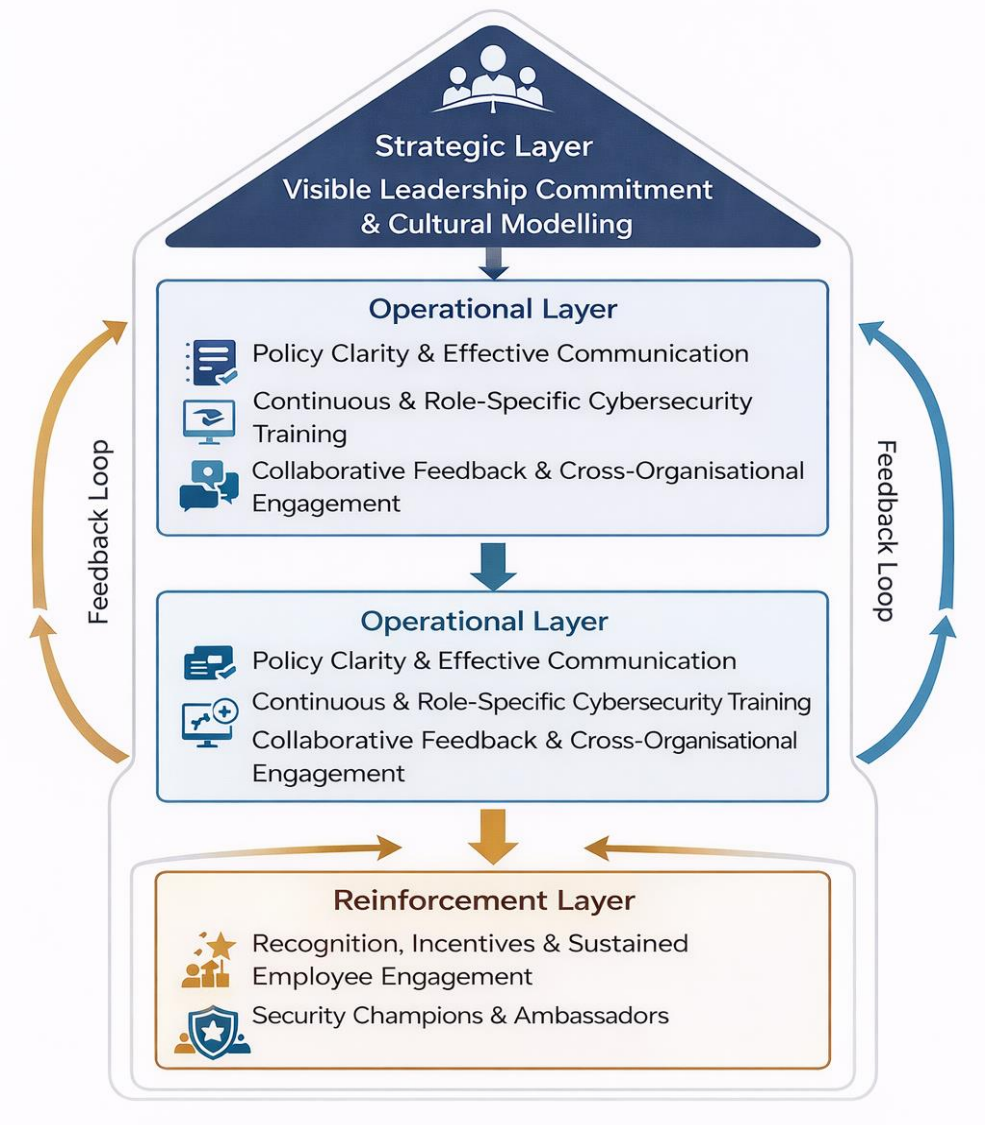


Figure 4-6: Layers of Cybersecurity Culture Framework (Layered Model)

As shown in Figure 4-6, the Strategic Layer forms the foundation of the framework and is anchored in visible leadership commitment, governance structures, and cultural role modelling. This layer establishes organisational priorities, sets expectations for cybersecurity behaviour, and provides oversight mechanisms that guide decision-making across the organisation.

Building on this foundation, the Operational Layer, positioned at the centre of the framework in Figure 4-6, translates strategic intent into actionable practices. This layer comprises policy clarity and effective communication. This includes continuous and role-specific cybersecurity training, collaborative feedback, and cross-organisational engagement. Altogether, these elements operationalise cybersecurity strategy by embedding it into everyday processes and routines.

The Reinforcement Layer, depicted in Figure 4-6 as the uppermost and feedback-oriented layer, ensures the sustainability of cybersecurity culture over time. This layer includes reward and recognition mechanisms, ongoing employee involvement, and the use of security champions and ambassadors. By reinforcing desired behaviours and rewarding positive cybersecurity practices, the reinforcement layer strengthens behavioural consistency, sustains employee engagement and supports the diffusion of cybersecurity culture across departments. This layer also provides feedback loops to the operational and strategic layers, enabling continuous improvement and cultural adaptation.

The development of the empirically informed framework presented in Section 4.6 represents an initial synthesis of literature and empirical findings. To enhance contextual relevance and practical applicability within the telecommunications sector, this framework was further refined through iterative analysis, theme consolidation, and alignment with sector-specific realities. Hence, what follows is a detailed version of the Telecommunications Cybersecurity Culture Framework, incorporating sector-specific adaptations and a high-level implementation roadmap that translates the layered design principles into practical, sustainable organisational practices.

4.7 Refined Telecommunications Cybersecurity Culture Framework

This section presents the Telecommunications Cybersecurity Culture Framework (TCCF), a refined and context-specific framework developed through the integration of empirical findings and relevant literature. The framework is analytically grounded and designed to strengthen cybersecurity culture within telecommunications organisations. The framework is designed for addressing sector-specific operational, regulatory, and organisational realities. It draws on established behavioural theories of Social Cognitive Theory and Protection Motivation Theory. It integrates these theories with insights derived from the empirical analysis to reflect the unique characteristics of the telecommunications sector.

The TCCF explains how leadership, governance structures, employee behaviours, and reinforcement strategies work together to build a positive, sustainable cybersecurity culture. It moves beyond its description by offering a clear, theory-informed guide that supports both academic understanding and practical applications within organisations. Building on the framework presented in Section 4.6, the TCCF incorporates refinements informed by empirical evidence to enhance contextual relevance, scalability, and long-term sustainability, consistent with the study's research objectives (RO1-RO3). Accordingly, the TCCF represents a structured and actionable contribution to advancing cybersecurity culture within the telecommunications sector.

The refined framework presented in this section represents the outcome of the framework development process followed in the study. It builds on the preliminary conceptual framework introduced in Chapter Two and incorporates empirical insights generated through the thematic analysis in Chapter Four. The progression from the Chapter Two preliminary framework to the Chapter Four refined framework demonstrates how literature derived components were reviewed, confirmed, adapted and contextualised using evidence from the Namibian telecommunications case study. This distinction is important because the Chapter Two framework provides the conceptual starting point, whereas the Chapter Four framework represents the study’s developed framework and final contribution, consistent with

contemporary qualitative case study logic and theory-informed framework development (Khadka & Ullah, 2025; Annamalah et al., 2026).

4.7.1 Refined Cybersecurity Culture Framework Structure Overview

Figure 4-7 illustrates the refined Telecommunications Cybersecurity Culture Framework (TCCF). The refined framework is structured around a central cybersecurity culture construct and comprises three interdependent layers, which are the Strategic, Operational, and Reinforcement layers, supported by the feedback loops. This layered design reflects the dynamic, iterative nature of the culture development, highlighting how leadership, organisational systems, and employee behaviours interact to shape and sustain cybersecurity culture.

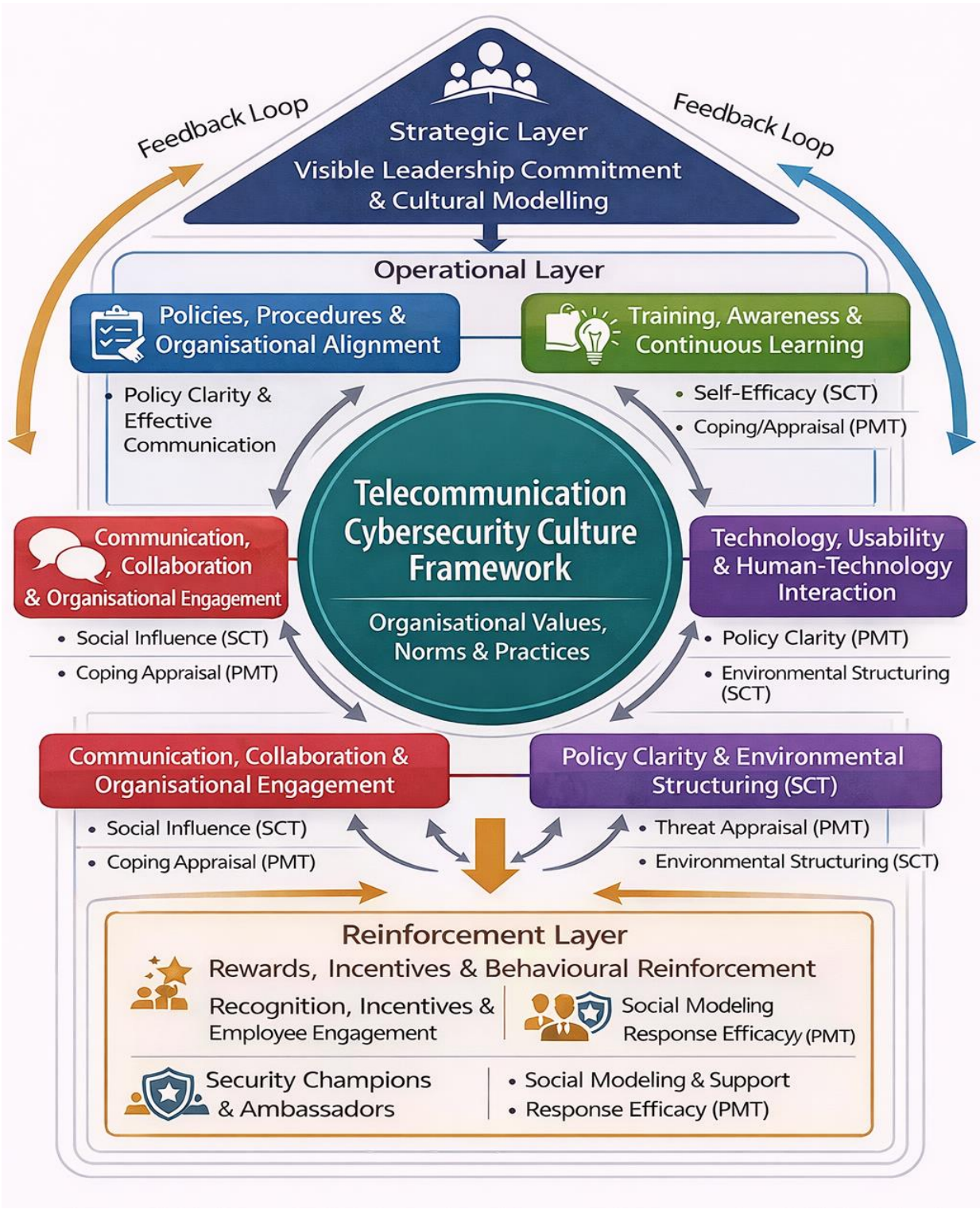


Figure 4-7: Refined Telecommunications Cybersecurity Culture Framework

An explanation of the framework layers in Figure 4.7 is provided below:
The Strategic Layer foregrounds visible leadership commitment and cultural modelling as the primary drivers of governance, accountability, and strategic prioritisation. This layer establishes cybersecurity as an organisational value and provides the structural conditions, such as policies, resources, and expectations, that are necessary for behavioural adoption across the organisation.

The Operational Layer translates strategic intent into actionable practices, day-to-day behaviours, and processes through policy clarity and effective communication, continuous and role-specific cybersecurity training, cross-organisational collaboration, and feedback mechanisms. These components collectively enable knowledge transfer, skill development, and cross-functional engagement, ensuring alignment between organisational objectives and everyday practices.

The Reinforcement Layer highlights the role of security champions, recognition, incentives, and behavioural reinforcement in sustaining cybersecurity culture. These instruments reinforce desired behaviours, enhance motivation, and support cultural diffusion across departments and roles.

The feedback loops depicted in Figure 4-7 illustrate the cyclical and adaptive nature of cultural development. It signifies the dynamic and iterative nature of cybersecurity culture development. Insights from operational practice and employee engagement continuously inform leadership decision-making, while strategic direction is recalibrated in response to emerging risks, organisational learning, and contextual changes.

Finally, the Integration of Behavioural Theories explicitly incorporates principles from Social Cognitive Theory and Protection Motivation Theory, demonstrating how behavioural mechanisms such as social modelling, self-efficacy, threat appraisal, response efficacy, and reinforcement are embedded across the framework layers. These theoretical connections enhance both the explanatory strength and practical value of the framework; they ensure it is grounded in established behavioural science.

Overall, Figure 4-7 alongside the narrative above represents the culmination of the study's theoretical synthesis and empirical validation. It further provides a coherent, context-specific, and operationally meaningful framework for understanding and enhancing cybersecurity culture within the telecommunications sector.

4.7.2 Refined Framework Sector Relevance

The refined TCCF is specifically designed for the telecommunications sector, which operates within a highly complex environment characterised by critical infrastructure dependencies, stringent regulatory obligations, high availability requirements, and extensive human–technology interaction. Telecommunications organisations manage distributed networks, diverse user groups, and interconnected systems, all of which amplify the risk of human-related cybersecurity vulnerabilities. By integrating governance, behavioural, and technological dimensions, the framework addresses sector-specific challenges, including policy complexity, skills gaps, and siloed operational structures. The inclusion of collaborative feedback and security champions is particularly significant in telecommunications contexts, where cross-functional coordination is essential for effective risk mitigation. Consequently, the TCCF offers a contextualised approach that aligns cybersecurity culture initiatives with the operational realities of telecommunications organisations.

The sector is undoubtedly exposed to various challenges, such as providing uninterrupted services, managing complex network infrastructure, and complying with strict regulatory oversight, which have necessitated contextual refinements to the framework. Therefore, the following recommended adaptations include:

- ◊ **Operational Cadence:** Coordinate the timing of training refresh cycles with network maintenance windows and systems release schedules; provide micro-learning modules tailored for shift-based operational staff to reduce service disruption and, at the same time, ensure continuity of learning.

- ◊ **Tooling Integration:** Embedding policy prompts and "how-to" micro-guides in operational systems like ticketing and approval workflows will help reduce response costs and improve compliance.

- ◊ **Regulatory Alignment:** Match policies with telecom-specific standards and regulatory requirements; consider putting up clear Responsible, Accountable, Consulted, and Informed (RACI) matrices to clarify who is accountable for control ownership in network change and incident processes layers.

- ◊ **Incident Learning:** Perform monthly cross-functional post-incident reviews with anonymised case summaries and distribute practice cards to operational teams.

- ◊ **Champion Roles:** Assign cybersecurity champions for each network domain (e.g., core, radio, transport, IT applications, IT infrastructure, etc.); clearly define responsibilities and allocate dedicated time for peer coaching and knowledge sharing.

Building on this sector-specific contextualisation established, the next section presents a high-level implementation roadmap for the TCCF, outlining phased actions, governance structures, and practical steps required to operationalise the framework within telecommunications organisations.

4.7.3 High-Level Framework Implementation Roadmap

The implementation of the TCCF is conceptualised as a phased, iterative process. The first phase focuses on strategic alignment, where leadership commitment is formalised through governance structures, policy endorsement, and resource allocation. The second phase points out operational inclusion, involving the deployment of clear policies, targeted training programs, and collaborative engagement platforms. The final phase concentrates on reinforcement and sustainability, committing recognition and empowering security champions to maintain momentum.

The roadmap is intentionally flexible, allowing organisations to adapt implementation pathways based on maturity, regulatory obligations, and resource availability. This approach ensures that the framework is not only theoretical but also actionable, aligning with principles of organisational change. A 12-month phased plan provides quarterly milestones, each comprising specific activities and measurable results to track progress and enable continuous

improvement. Table 4-15 presents the 12-month phased implementation roadmap, outlining key activities and expected outputs for each quarter. The roadmap provides measurable milestones that enable organisations to track progress, assess behavioural change, and support continuous improvement throughout the implementation process.

Table 4-15: A Phased Implementation Plan

Quarter	Key Activities	Expected Outputs / KPIs
Quarter 1	Conduct baseline culture diagnostic; appoint departmental champions; publish plain-language policy pack	Champions onboarded; policy comprehension >70%
Quarter 2	Launch role-based training paths; implement executive modelling calendar; host first incident-learning forum	Training completion >80%; at least two executive-led sessions
Quarter 3	Roll out gamified security campaign; establish feedback SLAs; initiate cross-domain communities of practice	Participation rate >65%; feedback turnaround <10 days
Quarter 4	Refresh policies; deliver advanced simulation exercises; evaluate framework effectiveness using the culture scorecard	Improved secure behaviour trends; culture maturity score increased

As shown in Table 4-15, the quarterly phases progress from foundational activities, such as baseline culture diagnostics and policy clarification, to more advanced reinforcement mechanisms, including gamified awareness campaigns and simulation exercises. The inclusion of clear outputs and KPIs ensures that each phase remains measurable, outcome-driven, and aligned with telecommunications sector priorities. Overall, this phased approach supports a gradual, sustainable approach to strengthening cybersecurity culture while remaining aligned with organisational needs.

While the proposed roadmap provides a structured and practical pathway for implementation, the successful adoption of the TCCF may be influenced by organisational, behavioural, and contextual risks, which are assessed in the following section.

4.7.4 Potential Implementation Risks and Mitigation Considerations

While the TCCF offers a structured approach to cultivating cybersecurity culture, several implementation risks may arise during adoption. These risks include leadership turnover, employee fatigue from repetitive training, misaligned incentives, and resistance to cultural change. Proactively addressing these risks strengthens the framework's practical credibility and supports informed decision-making during implementation. The key risks and corresponding mitigation strategies identified through the analysis are outlined below. Table 4-16 summarises the key risks and recommended mitigation strategies.

Table 4-16: Implementation Risks and Mitigation Strategies for the TCCF

Risk Category	Risk Description	Potential Impact	Mitigation Strategies
Competing Priorities	Senior leadership attention shifts to other operational pressures, reducing commitment to culture initiatives	Loss of strategic momentum Reduced visibility of cybersecurity priorities Slower adoption across the organisation	Integrate cybersecurity KPIs into executive scorecards Embed culture activities into BAU processes. Formalise leadership accountability
Training Fatigue	Employees disengage due to repetitive, generic, or overly frequent training content.	Decreased participation in awareness activities. Lower knowledge retention. Increased risk behaviour	Develop short, practical learning modules. Rotate gamified challenges. Use scenario-based, role-relevant training.
Fragmented Adoption	Departments adopt cultural practices at different rates, creating inconsistency	Uneven cultural maturity. Weakest departments become risk hotspots. Slower cultural diffusion	Deploy security champions for localised support. Conduct quarterly culture reviews. Provide targeted coaching to lagging units

Table 4-16 summarises the key implementation risks associated with the TCCF, their potential impacts, and the corresponding mitigation strategies. It also provides a clear, structured view of the challenges that may arise during implementation and how to proactively address them.

Addressing these risks and their potential impacts ensures that the TCCF is implemented in a coordinated and resilient manner, supporting sustained cultural transformation across the telecommunications organisation. Building on this risk assessment, the next section evaluates the TCCF's long-term sustainability and adaptive capacity.

4.7.5 Framework Sustainability and Adaptive Capacity

The refined TCCF is designed as a dynamic, adaptive system that evolves as the organisation matures and the technological, regulatory, and threat landscapes change. The embedded feedback loops enable continuous monitoring, learning, and refinement to ensure responsiveness to evolving threats, technologies, and regulatory requirements. Its three-tiered layered structure ensures sustained alignment between leadership intent, organisational processes, and employee behaviour. Strategic direction flows downward, while behavioural insights and operational realities flow upward, creating a cycle of continuous improvement. The sustainability of the TCCF is further strengthened through its integration of behavioural mechanisms drawn from Social Cognitive Theory (e.g., self-efficacy, observational learning, reinforcement) and Protection Motivation Theory (e.g., coping appraisal, response efficacy). The framework promotes sustainable cultural transformation instead of short-term compliance. Hence, these design features position the TCCF not as a static, compliance-driven model, but as a living framework that supports long-term cultural transformation. Its adaptive capacity enables ongoing organisational resilience through repeated assessment, stakeholder involvement, and structured change-management processes.

4.8 Chapter Summary

The chapter represented the analysis of the qualitative data using Braun and Clarke's (2021) six-phase Reflexive Thematic Analysis approach. The analysis identified six data-driven themes: visible leadership commitment and cultural modelling; continuous and role-specific

cybersecurity training; policy clarity and effective communication; collaborative feedback and cross-organisational engagement; recognition, incentives, and sustained employee engagement; and security champions and ambassadors. Each theme was analysed in relation to the research questions and interpreted through the theoretical lenses of Social Cognitive Theory and Protection Motivation Theory. The findings demonstrated that these enablers function as an interdependent system, mutually supporting one another and shaping cybersecurity culture through strategic, structural, behavioural, and social mechanisms.

The chapter further introduced the developed Cybersecurity Culture Framework, followed by the refined empirically informed Telecommunications Cybersecurity Culture Framework (TCCF), a sector-specific, evidence-informed model that incorporates a phased implementation roadmap. The refined framework serves as a practical, theoretically grounded guide for cultivating a cybersecurity culture within telecommunications organisations. Chapter Five builds on these findings to present the study's concluding insights, contributions to knowledge and practice, limitations, and recommendations for future research.

CHAPTER FIVE: CONCLUSION AND RECOMMENDATIONS

This chapter provides the organisation of this chapter is visually represented in Figure 5-1 below.

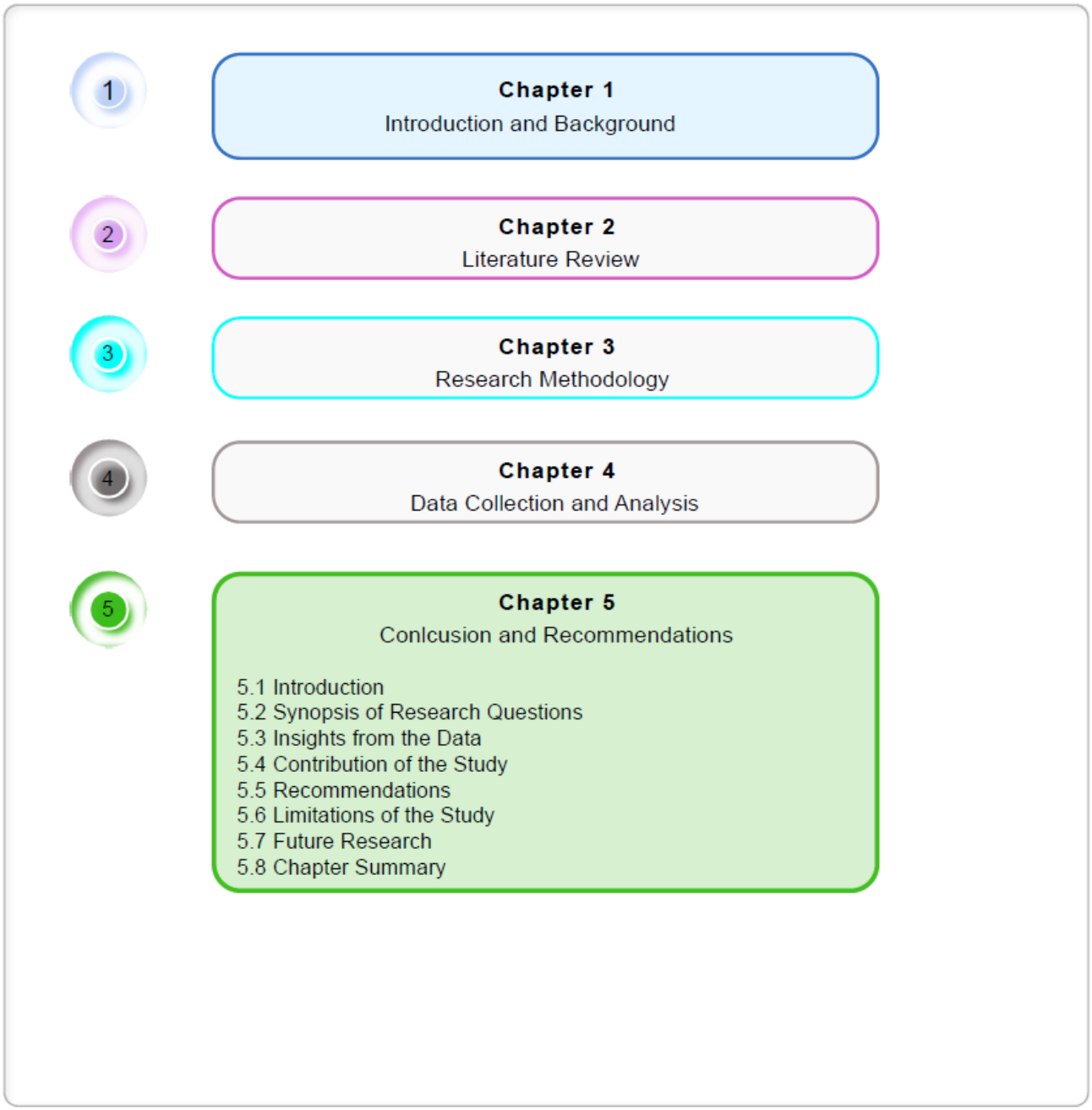


Figure 5-1: Chapter Five Layout

5.1 Introduction

This chapter presents the study's overall conclusions and recommendations. It begins with a synopsis of the research questions and explains how the findings addressed the study's objectives. This is followed by a concise summary of the key results and a discussion of the insights that emerged from the qualitative analysis. The chapter also outlines the study's contributions to both theory and practice, with particular attention to how the findings advance understanding of cybersecurity culture within telecommunications organisations. In addition, recommendations to improve cybersecurity culture are provided, along with reflections on the limitations encountered during the research and suggestions for future inquiry. The chapter concludes with a final summary and closing reflections on the refined framework presented in Chapter Four.

5.2 Synopsis of Research Questions

This section revisits how the study addressed the main research question and its three sub-questions, demonstrating the alignment between the research problem identified in Chapter One (Section 1.5), the theoretical foundations established in Chapter Two, the methodological approach outlined in Chapter Three, the qualitative findings presented in Chapter Four, and the integrative interpretation provided in Chapter Five.

As highlighted in Chapter One, human-related vulnerabilities and limited cybersecurity awareness within Namibia's telecommunications organisations significantly heighten the risk of security breaches and undermine organisational resilience. To address this problem, the study aimed to develop and refine a cybersecurity culture framework tailored to the telecommunications sector, leading to the overarching main research question:

How can a cybersecurity culture be improved to address human-related vulnerabilities, strengthen organisational resilience, and enhance cybersecurity awareness within Namibia's telecommunications sector?

To answer this overarching question, the subsections below summarise how each supporting sub-question was answered.

5.2.1 Research Question 1

What organisational, human, and governance requirements are necessary for an effective cybersecurity culture framework within the telecommunications sector?

The literature review in Chapter Two (Sections 2.6 (2.6.1) identified leadership commitment, governance structures, employee capability, and communication systems as foundational requirements for cybersecurity culture. The empirical findings presented in Chapter Four (Section 4.5) confirmed and expanded these requirements. Participants emphasised that:

- ◊ Visible leadership commitment is essential for signalling cybersecurity priorities and promoting accountability.
- ◊ Employee awareness and engagement are driven by practical training opportunities, and accessible communication channels also shape day-to-day security behaviour.
- ◊ Reinforcement mechanisms, including recognition, feedback, and shared learning, are necessary to maintain motivation and embed secure practices.

These elements represent the organisational, human, and governance requirements for an effective cybersecurity culture framework. Collectively, these findings demonstrate that leadership commitment, continuous awareness, and behavioural reinforcement constitute core organisational, human, and governance requirements for an effective cybersecurity culture framework within the telecommunications sector.

5.2.2 Research Question 2

What core components and characteristics define an effective cybersecurity culture framework suitable for Namibia's telecommunications sector?

Theoretical insights from Social Cognitive Theory (Chapter 2, Section 2.3.1) and Protection Motivation Theory (Section 2.3.2) guided the identification of the framework's behavioural components. SCT informed elements, such as leadership modelling, observational learning, and reinforcement, while PMT informed aspects of threat appraisal, response efficacy, coping appraisal, and self-efficacy.

The literature reviewed in Chapter Two (Sections 2.6.1–2.6.6) further emphasised the importance of role-specific training, policy clarity, and collaborative feedback mechanisms. These theoretical and empirical insights were integrated during the framework conceptualisation phase in Chapter Four (Section 4.5), defining the core characteristics needed for a context-appropriate cybersecurity culture framework in the telecommunications sector.

5.2.3 Research Question 3

How to develop a cybersecurity culture framework for Namibia's telecommunications sector?

In answering RQ3, the study demonstrates that the refined cybersecurity culture framework was developed by integrating the RO1 derived organisational, human and governance requirements with the RO2 derived core components and characteristics and then contextualising these elements through the empirical findings presented in Chapter Four. This confirms that the framework was developed progressively rather than introduced as a standalone output.

The refined framework presented in this section represents the outcome of the framework development process followed in the study. It builds on the preliminary conceptual framework introduced in Chapter Two and incorporates the empirical insights generated through the thematic analysis in Chapter Four. The progression from the preliminary conceptual framework to the refined empirically informed framework demonstrates how literature derived components were reviewed, confirmed, refined and presented using evidence from the Namibian telecommunications case study organisation. This distinction is important because the Chapter Two framework provides the conceptual starting point, whereas the Chapter Four framework represents the study's developed framework and final contribution.

The framework was finally developed through iterative integration of empirical insights in Chapter Four (Section 4.7), yielding the Telecommunications Cybersecurity Culture Framework (TCCF). The refined framework comprises three interdependent layers, each reflecting a distinct but complementary dimension of cybersecurity culture:

- ◊ Strategic Layer: embedded leadership commitment, governance structures, and policy direction to establish cybersecurity as an organisational priority.
- ◊ Operational Layer: translates strategic intent into practice through continuous awareness initiatives, clear communication, and role-specific capability development.
- ◊ Reinforcement Layer: sustains desired behaviours through recognition programmes, feedback mechanisms, continuous improvement, and the use of departmental security champions.

In addition to these three layers, the refinement incorporated two cross-cutting features that strengthen the framework's adaptability and behavioural grounding as depicted in Figure 4-7.

- ◊ Feedback Loops: The feedback loops represent the cyclical and adaptive nature of cybersecurity culture development. Insights from operational practice and employee engagement continuously inform leadership decision-making, while strategic direction is adjusted in response to emerging risks, organisational learning, and contextual changes.
- ◊ Integration of Behavioural Theories: The framework embeds behavioural mechanisms from Social Cognitive Theory and Protection Motivation Theory, incorporating elements such as social modelling, self-efficacy, threat appraisal, response efficacy, and reinforcement across all layers. This theoretical grounding enhances the development of the framework's explanatory strength and practical relevance.

Overall, the refinement process produced an experientially validated, context-specific, and theoretically informed cybersecurity culture framework that directly responds to the organisational realities of telecommunications providers in Namibia.

Across all three sub-questions, the study demonstrated a coherent progression from problem definition (Chapter One) to conceptual grounding (Chapter Two), methodological execution (Chapter Three), empirical analysis (Chapter Four), and interpretive integration (Chapter Five). The research questions were comprehensively addressed, culminating in a refined, sector-

specific cybersecurity culture framework that meaningfully supports organisational resilience in Namibia’s telecommunications sector.

5.3 Summary of Findings

This section consolidates the study's key findings presented in Chapter Four. Rather than re-analysing the data, it provides a thematic overview of the key factors shaping cybersecurity culture in the telecommunications sector. The findings are organised around six interconnected themes, which informed the development of the refined Telecommunications Cybersecurity Culture Framework (TCCF).

1. Visible Leadership Commitment and Cultural Modelling

The findings indicate that leadership visibility, role modelling, and prioritisation of cybersecurity are central to shaping organisational norms and expectations related to secure behaviour.

2. Continuous and Role-Specific Cybersecurity Training

Cybersecurity awareness and competence depend on ongoing, role-relevant training that extends beyond generic awareness initiatives. In addition to general awareness programmes, scenario-based, more interactive training is provided to enhance confidence.

3. Policy Clarity and Effective Communication

The study revealed that policy effectiveness is influenced by clarity, accessibility, and the presence of two-way communication mechanisms that support understanding and application.

4. Collaborative Feedback and Cross-Organisational Engagement

The findings highlight the importance of structured collaboration and feedback mechanisms in promoting shared responsibility and organisational learning.

5. Recognition, Incentives, and Sustained Employee Engagement

Employee engagement with cybersecurity initiatives was associated with the presence of reinforcement mechanisms, including recognition, incentives, and participatory activities.

6. Security Champions and Ambassadors

The appointment of departmental security champions emerged as a practical mechanism for embedding cybersecurity practices within operational contexts and bridging strategic and operational priorities.

These findings demonstrate that cybersecurity culture within telecommunications organisations is shaped by the interaction of strategic leadership, operational enablement, and behavioural reinforcement. These themes provided the empirical foundation for developing TCCF and informed the conclusions and recommendations presented in the subsequent sections of this chapter.

5.3 Insights from the Data

The thematic analysis provided a deep understanding of the organising, behavioural, and structural elements that shape the cybersecurity culture of the telecommunications sector. The results showed that cybersecurity culture is not the result of isolated interventions or one-off initiatives. Rather, it is a systemic, integrated approach that strategically blends leadership through clear governance structures and behavioural reinforcement mechanisms.

The study highlighted that leadership commitment, which reflects the organisation's priority and, in turn, informs security practices, is the most effective form of cultural transformation. In addition, policy clarity requires leadership engagement to ensure that the security guidelines are accessible, understandable, and consistently communicated across all levels of the organisation. It was noted that continuous, role-specific training is a key factor in helping employees become confident and competent. Therefore, an organisation can implement security principles in real-world situations.

The analysis also highlighted the importance of collaboration, with structured feedback loops and cross-functional communication fostering shared responsibility and collective learning. Additionally, behaviour modification techniques, such as reward schemes and gamified campaigns, were identified as critical tools for sustaining motivation and embedding safe behaviours into regular habits. Finally, security champions and ambassadors were considered an effective means of aligning corporate goals with working standards, ensuring that cultural

ideals are translated into appropriate working behaviours at the team level. Such understanding guided the development and continuous optimisation of the Telecommunications Cybersecurity Culture Framework (TCCF), which was ultimately defined as an instrument to identify and mitigate human factors, build organisational resilience, and foster sustainable cultural change through a layered, adaptive approach.

5.4 Contribution of the Study

This section emphasises and discusses these contributions, which are of great value within the framework of the study objectives. This highly informative work extends the existing theoretical groundwork and practical domains by deepening the understanding of internal culture in cybersecurity within the telecommunications industry and by providing companies with a tool to realise their strategies based on the research findings. In addition to the development of the Telecommunications Cybersecurity Culture Framework, the study generated two scholarly outputs in Springer conference proceedings, thereby extending its academic contribution to the wider discourse on cybersecurity culture in telecommunications organisations.

5.4.1 Theoretical Contributions

1. Integration of Behavioural Theories into Cybersecurity Culture Research

This research is grounded in Social Cognitive Theory (SCT) and Protection Motivation Theory (PMT). It applies these theories to cybersecurity culture. The study theoretically substantiates cultural interventions primarily by explaining how constructs such as self-efficacy, observational learning, coping appraisal, and response efficacy influence the performance of safe behaviours.

2. Contextualisation of Cybersecurity Culture in Telecommunications

Most studies appear to focus primarily on the financial sector, with only a few addressing corporate businesses at large. This study adds value by defining cybersecurity culture within the telecommunications industry. Thus, it addresses sector-specific aspects, including the complexity of network infrastructure, regulatory compliance requirements, and the need to ensure continuous operations.

3. Development of a Multi-Layered Framework

The Telecommunications Cybersecurity Culture Framework (TCCF) uses a metaphor of three-layered designs: strategic, operational, and reinforcement to describe the interdependence of leadership, policy, training, collaboration, and behavioural reinforcement. This layered approach advances theoretical understanding of how cultural components interact to produce sustainable change.

5.4.2 Practical Contributions

1. Actionable Framework for Organisations

The TCCF is basically a hands-on plan to help telecommunications companies integrate cybersecurity culture. Leadership modelling, role-specific training, policy clarity, collaborative feedback, recognition, and champion networks are elements that provide practical solutions to human-related security threats.

2. Sector-Specific Adaptations

The framework incorporates contextual adaptations, such as operational cadence alignment, tooling integration, and domain-specific champion roles, thereby maintaining its operational relevance in the unique realities of telecoms organisations.

3. Implementation Roadmap and Risk Mitigation

The study provides a 12-month implementation roadmap, measurable KPIs, and identifies potential risks and their corresponding mitigation strategies. This makes the framework more applicable to real-life situations and helps organisations plan and track their cultural transformation initiatives.

By bridging theoretical insights with empirical evidence, this study advances scholarly understanding of cybersecurity culture and provides a sector-specific, evidence-based framework that organisations can adopt to strengthen resilience and enhance cybersecurity awareness.

5.5 Recommendations

Based on the study's findings and the refined Telecommunications Cybersecurity Culture Framework (TCCF) presented in Chapter Four, several recommendations are proposed to strengthen cybersecurity culture within telecommunications organisations. The current recommendations are structured according to the six components of the framework and are intended to address human-related vulnerabilities, support the organisation in building resilience, and enable effective behavioural change.

- ◊ **Leadership:** Organisations should embed cybersecurity into their strategic priorities by incorporating cybersecurity-related Key Performance Indicators (KPIs) into executive scorecards. This will ensure accountability and sustained leadership focus. Senior leaders must also actively model secure behaviours by participating in awareness initiatives and demonstrating compliance with security protocols. Visible leadership engagement signals organisational commitment and sets the tone for cultural transformation.

- ◊ **Training:** Provide ongoing, role-specific cybersecurity training to build employee confidence and skills. Use scenario-based sessions, phishing simulations, and real case studies. Update training every six months to address new threats.

- ◊ **Policy:** Cybersecurity policies should be simplified and written in clear, accessible language to improve understanding across all organisational levels. One major step could be introducing additional communication channels for interaction. For example, digital platforms can be used to share policy updates and FAQs, facilitating two-way communication. Policies should be reviewed quarterly to ensure they align with the latest operational and regulatory requirements.

- ◊ **Collaboration:** To promote shared responsibility in cybersecurity, organisations should establish structured collaboration methods. For example, they might host incident-learning forums where employees openly discuss lessons learned and exchange best practices. Additionally, a company could design and implement three-month Feedback

Service Level Agreements (SLAs) to ensure prompt responses to any employee security concerns, ultimately fostering greater trust and accountability within the organisation.

- ◊ **Motivation:** To sustain engagement, organisations should use gamified security campaigns, leaderboards, and recognition programmes. Linking incentives to performance appraisals can encourage lasting secure behaviours.

- ◊ **Champions:** Departmental security champions should be appointed to act as peer advocates and cultural influencers. They say that champions must have well-organised playbooks and clear role outlines to support them in leading secure practices. Precious time must be set aside for champions to provide coaching and support colleagues, ensuring advocacy is their everyday focus.

Generally, these suggestions should be viewed as an integrated strategy rather than isolated measures. Thus, a holistic approach enables leadership, training, policy clarity, collaboration, motivation, and advocacy to synergise to embed a culture of cybersecurity across the entire organisation. Consistent with Georgiadou et al. (2020), it is advisable for organisations to conduct a gap analysis, in consultation with key stakeholders, to assess readiness and awareness before implementing large-scale interventions. Here, these guidelines are provided as actionable help for organisations planning to integrate cybersecurity awareness and responsibility into their culture.

5.6 Limitations of the Study

Although the study provides valuable insights into the telecommunications sector's cybersecurity culture, several limitations should be noted. These limitations do not diminish the importance of the results but emphasise the points at which one should be careful when interpreting the data and where future studies may continue the journey. The first limitation is the study's scope, which was confined to a single telecommunications organisation in Namibia. Although the case study methodology enabled an in-depth exploration of the firm's operations and culture, it limits the generalisability of the results to other firms or industries. The results

are limited to this geographic area and may not reflect all practices in the telecommunications sector.

The second limitation is the sample size and the data collection method. The research used a qualitative sampling approach and recruited 25 participants from managerial, IT, and non-IT staff. This provided an in-depth understanding; however, given the small sample size, the results should be interpreted more as guidance than as a full study. Also, semi-structured interviews may have introduced a self-reporting bias, as responses could have been influenced by organisational norms or social desirability. The lack of quantitative validation is another shortcoming. The use of thematic analysis was appropriate for studying perceptions and experiences, but without statistical tests, it would be impossible to generalise the findings or establish causal links between the identified factors and the behavioural outcomes.

Lastly, the research captures a specific moment in time; the organisational culture is revealed only for a three-month period. In fact, cybersecurity culture is continually influenced by changes in technology, regulations, and internal developments, such as the reorganisation of the company, and it evolves accordingly. Continued research may reveal not only cultural factors but also differences in intervention sustainability over time. To sum up, the key limitations are that one should be very careful when generalising the results beyond the case study context. In addition, they identify potential areas of research in which the developed framework can be tested and extended through a larger sample, a broader range of methods, and a longer observation period.

5.7 Future Research

Although this study sheds light on the cybersecurity culture in the telecommunications sector, future researchers can take various directions to expand the contribution of their work. One way to broaden their study is to examine multiple telecommunications organisations rather than just one, or to explore different industrial sectors. This will make the findings more widely applicable and allow for a comparative study of cultural practices. Furthermore, future researchers might consider using experimental designs to test the components of the

Telecommunications Cybersecurity Culture Framework (TCCF). The survey or structural equation modelling could be used as a statistical tool to provide empirical evidence of the relationships between framework types and behavioural outcomes, thereby complementing the qualitative understanding gained in this study.

In addition, it would be helpful to continue studying cybersecurity culture over time using a longitudinal research approach. An organisation's culture is not static; it changes in response to technological developments, regulatory changes, and restructuring. Observing cultural changes over the long term would improve understanding of the framework's effectiveness and flexibility. Furthermore, future research can focus on examining the influence of emerging technologies such as Artificial Intelligence (AI)-driven security solutions, automation, and cloud-based services on organisational cybersecurity culture. By examining how these technological advances affect employees and operations, researchers can ensure that cultural frameworks remain relevant and responsive to the rapidly evolving technological landscape. Understanding these impacts is essential for organisations to adapt and maintain effective cybersecurity practices as they adopt new tools and services.

Ultimately, successive works may extend human factors investigation to broader, more diverse areas such as diversity, gender inclusivity, and generational differences. These aspects may reveal ways to develop more inclusive, targeted strategies that promote a strong cybersecurity culture and build organisational resilience. In conclusion, there are advantages if future research expands the empirical base, quantitatively validates theoretical constructs, and investigates continually changing technological and behavioural scenarios. The first change will be the development of more detailed cybersecurity culture models, and the second will be their continuous support for organisations in developing security cultures that are both adaptive and sustainable over time.

5.8 Chapter Summary

This chapter synthesised the study's main findings and demonstrated how the research objectives were met. The chapter provided a comprehensive discussion of how each research

question was systematically addressed through the study's findings. The responses to these questions were developed by closely examining the results obtained and integrating relevant theoretical frameworks. This approach ensured the analysis was informed not only by empirical data but also by established theory, thereby strengthening the validity of the conclusions. By combining practical evidence with academic perspectives, the study provided a comprehensive understanding of the issues under investigation. The summary of the findings focused on six major issues: leadership commitment; visible, continuous training for staff in their roles; clear policies; collaborative engagement; recognition mechanisms; and security champions, which together influence cybersecurity culture in the telecommunications sector.

The first key finding of the data analysis was that cybersecurity culture is shaped by a combination of strategic leadership, operational enablement, and behavioural reinforcement. This understanding led to the creation of the Telecommunications Cybersecurity Culture Framework (TCCF), which reflects changes informed by sector-specific insights and considerations, and provides a clear, practical roadmap for implementation. Moreover, the chapter provided a summary of the study at both theoretical and practical levels, emphasising the integration of behavioural theories, such as Social Cognitive Theory (SCT) and Protection Motivation Theory (PMT), into cultural design and the facilitation of viable organisational strategies. The next paragraph presented recommendations to support TCCF integration, followed by an acknowledgement of the current study's limitations and areas for future research, including broader sampling, quantitative validation, and longitudinal studies.

In essence, this chapter connected the direct observations with the revamped framework and paved the way for the final chapter, which will synthesise the study's findings and examine its theoretical, practical, and future research implications.

REFERENCES

African Union. 2019. *Convention of the African Union on cybersecurity and personal data protection (Malabo Convention)*. Available at: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection [Accessed: 26 January 2026].

Ahmed, S.F., Sakib, M., Afrin, S., Jannat, R., Taher, S.B. & Kabir, M. 2024. Toward a secure 5G-enabled Internet of Things: A survey on requirements, privacy, security, challenges, and opportunities. *IEEE Access*, *12*, pp.13126–13151. Available at: https://doi.org/10.1109/ACCESS.2024.3352508

Alavi, M., Nikou, S. & Kim, S. 2021. The governance of 5G infrastructure: Between path dependency and risk-based approaches. *Journal of Cybersecurity*, *7*(1), tyab017. Available at: https://doi.org/10.1093/cybsec/tyab017

Alshaikh, M. 2020. Developing a cybersecurity culture to influence employee behaviour: A practice perspective. *Computers & Security*, *98,* 102003. doi.org/10.1016/j.cose.2020.102003

Alsharnouby, M., Al-Dubai, A. & Wills, G. 2024. Gamification in cybersecurity education: A systematic literature review and research agenda. *Journal of Applied Research in Higher Education*, *17*(4), pp.1162–1180. Available at: https://doi.org/10.1108/JARHE-02-2024-0072

Amutenya, J. & Botha, R.A. 2019. A cybersecurity framework for Namibia: Current state and the way forward. *Southern Africa Telecommunication Networks and Applications Conference (SATNAC)*. Available at: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID4332733_code5274849.pdf?abstractid=4332733&mirid=1 [Accessed: 20 January 2026].

Annamalah, S., Abdullah, S.A.K., Anthonysamy, L. & Ahmed, S. 2026. Case study research in qualitative inquiry: A structured guide to design, data collection and analysis. *Qualitative Research Journal*, ahead-of-print. Available At: https://doi.org/10.1108/QRJ-11-2025-0429

Aurigemma, S., Leonard, L. & Panko, R. 2021. Gamifying cybersecurity training: An empirical study of effectiveness. *Journal of Cybersecurity*, *7*(1), taab006. Available at: https://doi.org/10.1093/cybsec/taab006

Ayyagari, S. & Maru, S. 2022. Cybersecurity culture: Building resilient organisations in the digital age. *International Journal of Cybersecurity*, *12*(2), pp. 212–228.

Baltes, B. & Rees, M. 2023. Challenges in establishing cybersecurity culture: Insights from the telecommunications industry. *Cybersecurity Review*, *11*(3), pp. 47–59.

Bandura, A. 2023. *Social cognitive theory: an agentic perspective on human nature*. 2nd edition. New York: Wiley. Available at: https://www.wiley.com/en-us/Social+Cognitive+Theory%3A+An+Agentic+Perspective+on+Human+Nature-p-00388489 [Accessed: 20 January 2026].

Bell, E., Bryman, A. & Harley, B. 2022. *Business research methods*. 6th edition. Oxford: Oxford University Press.

Bouke, M.A., Abdullah, A., Alshatebi, S.H., El Atigh, H. & Cengiz, K. 2023. *African Union Convention on cyber security and personal data protection: Challenges and future directions.* arXiv preprint. Available at: https://arxiv.org/abs/2307.01966 [Accessed: 20 January 2026].

Braun, V. & Clarke, V. 2021. *Thematic analysis: A practical guide*. London: SAGE Publications. Available at: https://doi.org/10.4135/9781529732452

Chang, L. & Coppel, N. 2020. Building cyber security awareness in a developing country: Lessons from Myanmar. *Computers & Security, 97*, Article 101959. Available at: https://doi.org/10.1016/j.cose.2020.101959

Charalambous, G., Piki, A. & Stavrou, G. 2025. *Redesigning cybersecurity awareness-raising and training programs: Insights from professionals*. Available at: https://knowledge.lancashire.ac.uk/id/eprint/56654/ [Accessed: 21 January 2026].

CIS (Centre for Internet Security). 2021. *CIS Controls v8*. Available at: https://www.cisecurity.org/controls [Accessed: 15 January 2026].

CISA (Cybersecurity and Infrastructure Security Agency). 2022. *Best practices in cybersecurity awareness and training*. CISA Central. Available at: https://www.cisa.gov/cybersecurity-awareness-training [Accessed: 10 January 2026].

Collis, J. & Hussey, R. 2021. *Business research: A practical guide for undergraduate and postgraduate students*. 5th edition. London: Macmillan Education.

Corradini, I. 2020. Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology. *Studies in Systems, Decision and Control.* Springer, Cham, Switzerland. Available at: https://doi.org/10.1007/978-3-030-43999-6

Cram, W. A., Proudfoot, J. G. & D'Arcy, J. 2020. Maximizing employee compliance with cybersecurity policies. *MIS Quarterly Executive*, *19*(3), Article 5. Available at: https://aisel.aisnet.org/misqe/vol19/iss3/5/ [Accessed: 11 January 2026].

Creswell, J.W. & Creswell, J.D. 2018. *Research design: Qualitative, quantitative and mixed methods approaches*. 5th edition. Thousand Oaks, CA: SAGE Publications.

Creswell, J.W. & Poth, C.N. 2018. *Qualitative inquiry and research design: Choosing among five approaches*. 4th edition. Thousand Oaks, CA: SAGE Publications.

Da Veiga, A., Astakhova, L.V., Botha, A. & Herselman, M. 2020. Defining organisational information security culture — Perspectives from academia and industry. *Computers & Security*, *92*, Article 101713. Available at: https://doi.org/10.1016/j.cose.2020.101713

Delso-Vicente, A.T., Díaz-Marcos, L., Aguado-Tevar, O. & García de Blanes-Sebastián, M. 2025. Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity*. Future Business Journal, 11*(28). Available at: https://doi.org/10.1186/s43093-025-00452-7

Delso-Vicente, J., Sutton, A., Tompson, L., Sidebottom, A. & Cleland, B. 2025. Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Computers & Security*, 148, Article 104110. Available at: https://doi.org/10.1016/j.cose.2024.104110

Di Nocera, F., Tempestini, G. & Orsini, M. 2023. Usable security: A systematic literature review. *Information, 14*(12), p.641. Available at: https://doi.org/10.3390/info14120641

ENISA (European Union Agency for Cybersecurity). 2020. *Cybersecurity culture in organisations*. Athens: ENISA. Available at: https://www.enisa.europa.eu/publications/cybersecurity-culture-in-organisations [Accessed: 10 January 2026].

ENISA (European Union Agency for Cybersecurity). 2021. *ENISA threat landscape 2021*. Athens: ENISA. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 [Accessed: 5 January 2026].

ENISA (European Union Agency for Cybersecurity). 2023. *ENISA threat landscape 2023*. Athens: ENISA. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 [Accessed: 10 January 2026].

Fallatah, W., Furnell, S. & Wagner, C. 2026. Towards a usability-focused security culture framework. *Journal of Cybersecurity and Privacy*, 6(1), Article 34. Available at: https://doi.org/10.3390/jcp6010034

Fezzey, T., Batchelor, J. H., Burch, G. F., & Reid, R. (2023). Cybersecurity continuity risks: lessons learned from the COVID-19 pandemic. *Journal of Cybersecurity Education*, *Research and Practice, 2*, Article 4. doi: 10.32727/8.2023.3. Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2022/iss2/4

Fusch, P.I., Fusch, G.E. & Ness, L.R. 2018. Denzin's paradigm shift: Revisiting triangulation in qualitative research. *Journal of Social Change*, *10*(1), pp. 19–32. Available at: https://doi.org/10.5590/JOSC.2018.10.1.02

Fusch, P.I., Ness, L.R. & Booker, J.M. 2018. The role of data saturation in qualitative research. *The Qualitative Report*, *23*(8), pp. 1929–1937.

Government of the Republic of Namibia. 1996. *Manual of Guidelines for Common Minimum Standards of Protective Security Measures for Government Ministries/Public Offices and Agencies of the Republic of Namibia*. Windhoek, Government of the Republic of Namibia.

Granić, A. & Marangunić, N. 2024. Technology acceptance model: a review of two decades of study and research. *Educational Information Technologies, 29*,1–25. Available at: https://link.springer.com/article/10.1007/s10639-023-12154-0 [Accessed: 26 January 2026].

GSMA Intelligence. 2024. *5G momentum continues with 1.6 billion connections worldwide, rising to 5.5 billion by 2030*. Available at: https://www.gsma.com/newsroom/press-release/5g-momentum-continues-with-1-6-billion-connections-worldwide-rising-to-5-5-billion-by-2030-according-to-gsma-intelligence/ [Accessed: 27 January 2026].

GSMA. 2024. *Global mobile trends 2024*. London: GSMA. Available at: https://kigen.com/wp-content/uploads/2024/02/GSMA-Global-Mobile-Trends-2024.pdf [Accessed: 27 January 2026].

Gunawan, J. 2022. Understanding trustworthiness in qualitative research. *Belitung Nursing Journal*, *8*(1), pp. 1–3. Available at: https://doi.org/10.33546/bnj.4

Hamidi, M.S. & Singh, B. 2025. *Cyber security challenges in developing countries: A special reference to Afghanistan*. *International Journal of Information Security Engineering*, 3(1), pp.1–6. Available at: https://journals.stmjournals.com/ijise/article=2025/view=201690 [Accessed: 27 January 2026].

Hammersley, M. & Atkinson, P. 2019. *Ethnography: Principles in practice*. 4th edition. London: Routledge. Available at: https://doi.org/10.4324/9781315146027

Hanus, B.T. & Wu, Y. 2021. Building a cybersecurity culture through communication: Exploring influencing factors. *Behaviour & Information Technology*, 40(3), pp. 232–244. Available at: https://doi.org/10.1080/0144929X.2020.1723616

Haney, J.M., Cunningham, C. I.V. & Furman, S.M. (2023). *Towards integrating human-centered cybersecurity research into practice: practitioner survey insights*. In *Proceedings of the USENIX Workshop on Cybersecurity*, 2023, pp. 1–15.

Hennink, M. & Kaiser, B.N. 2022. Sample size sufficiency for a quality qualitative study. *The Qualitative Report*, *27*(1), pp. 52–58. doi:10.46743/2160-3715/2022.5063

International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). 2022. ISO/IEC 27001 2022: *Information security, cybersecurity and privacy protection – Information security management systems — Requirements.* Geneva: ISO Available at: https://www.iso.org/standard/82875.html [Accessed: 8 January 2026].

Khadka, K. & Ullah, A.B. 2025. Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security*, 24, Article 119. Available at: https://doi.org/10.1007/s10207-025-01032-0

Krippendorff, K. 2022. *Content analysis: An introduction to its methodology*. 4th edition. Thousand Oaks, CA: SAGE Publications. Available at: https://doi.org/10.4135/9781071878781

Kritzinger, E., Da Veiga, A. & van Staden, W. 2023. Measuring organizational information security awareness in South Africa. *Information Security Journal: A Global Perspective, 32*(2), pp. 120–133. doi: 10.1080/19393555.2022.2077265.

Kumar, R. 2019. *Research methodology: A step-by-step guide for beginners*. 5th edition. London: SAGE Publications.

Lemieux, R. 2025. *Five steps leadership can take to enable organisational cyber resilience through culture.* DVMS Institute. Available at: https://dvmsinstitute.com/2024/08/15/top-five-things-organizations-need-to-do-to-manage-organizational-cyber-risk/ [Accessed: 16 January 2026].

Liu, Y., Tian, L., Li, C. & Wu, Y. 2024. Analysing the competitiveness and strategies of Chinese mobile network operators in the 5G era. *Telecommunications Policy*, *48*(2), Article 102652.

MacQueen, J.R. 2020. *The flow of organizational culture: New thinking and theory for better understanding and process*. Cham: Palgrave Macmillan. Available at: https://doi.org/10.1007/978-3-030-25685-2.

Mali, S. 2024. Assessing the effectiveness of multi-factor authentication in cloud-based big data environments. *Internet of Things and Cloud Computing*, 12(2), pp.17–27. Available at: https://doi.org/10.11648/j.iotcc.20241202.11

Mataruse, R.T. 2020. *The role of leadership in cybersecurity culture within the South African financial services.* Master's dissertation. University of the Witwatersrand. Available at: https://wiredspace.wits.ac.za/items/eab5fc88-4200-4e89-8a4c-5f29d2d1aa67 [Accessed: 16 January 2026].

Maynard, S.B., McGill, T.J. & Wang, X. 2022. The role of context in information security policy compliance: A review of the literature*. Computers & Security, 112*, 102520. Available at: https://doi.org/10.1016/j.cose.2021.102520

MICT (Ministry of Information and Communication Technology). 2022. *National cybersecurity strategy and awareness creation plan 2022-2027*. Windhoek: MICT. Available at: https://www.mict.gov.na [Accessed: 7 January 2026].

Nam-CSIRT (Namibia Computer Security Incident Response Team). 2024. *Namibia cybersecurity landscape report*. Windhoek: CSIRT. Available at: https://nam-csirt.na/download/overview-of-the-namibian-cyber-landscape-report-october-2024/ [Accessed: 14 January 2026].

Nam-CSIRT (Namibia Computer Security Incident Response Team). 2025. *Cybersecurity bi-annual statistics report 2025*. Windhoek: CSIRT. Available at: https://nam-csirt.na/download/cybersecurity-bi-annual-statistics-report-2025/ [Accessed: 15 January 2026].

Namibia Communications Authority. 2021. *Annual report 2020/21*. Windhoek: Namibia Communications Authority.

National Cyber Security Index. 2023. *Namibia: National Cyber Security Index country profile*. Available at: https://ncsi.ega.ee/country/na/ [Accessed: 14 July 2026].

Nawa, E.L.T., Chitauro, M. & Bhunu Shava, F.B. 2022. *Developing a cybersecurity framework for the Namibian banking institutions. Proceedings of the International Conference on Information Systems and Emerging Technologies (ICISET), 16pp*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4332733 [Accessed: 10 January 2026].

New Era. 2024. Telecom hit by massive cyberattack … over 400 000 files leaked. *New Era*, 16 December. Available at: https://neweralive.na/telecom-hit-by-massive-cyberattack-over-400-000-files-leaked/ [Accessed: 14 July 2026].

NIST (National Institute of Standards and Technology). 2022. *Framework for improving critical infrastructure cybersecurity*. Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://www.nist.gov/cyberframework [Accessed: 10 January 2026].

NIST (National Institute of Standards and Technology). 2024. *Cybersecurity Framework 2.0*. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://www.nist.gov/cyberframework [Accessed: 10 January 2026].

Nkosi, M. 2024. *NETSCOUT Reveals Rising DDoS Threats in Southern Africa*. *IT News Africa*. Available at: https://www.itnewsafrica.com/2024/10/netscout-reveals-rising-ddos-threats-in-southern-africa/ [Accessed: 17 January 2026].

Ogbanufe, O. & Ge, L. (2023). A comparative evaluation of behavioral security motives: protection, intrinsic, and identity motivations. *Computers & Security, 128*, 103136. Available at: https://doi.org/10.1016/j.cose.2023.103136

Ogunjinmi, O.F. 2025. Cybersecurity in telecommunications: Defending networks against emerging threats. *World Journal of Advanced Engineering Technology and Sciences*, *14*(3), pp. 410–424. Available at: https://doi.org/10.30574/wjaets.2025.14.3.0138

Ritchie, J., Lewis, J. McNaughton, N.C. & Ormston, R. 2013. *Qualitative research practice: A guide for social science students and researchers*. 2nd edition. London: SAGE Publications.

SADC (Southern African Development Community). 2022. *Cybersecurity strategy for SADC member states*. Gaborone: SADC.

Sadiku, M.N.O., Adekunte, P.A. & Sadiku, J.O. 2024. Cybersecurity in telecommunications. *International Journal of Trend in Scientific Research and Development*, *8*(6), pp. 493–502. Available at: https://www.ijtsrd.com/papers/ijtsrd71623.pdf [Accessed: 26 January 2026].

Saldaña, J. 2022. *The coding manual for qualitative researchers*. 4th edition. London: SAGE Publications.

Saunders, M., Lewis, P. & Thornhill, A. 2023. *Research methods for business students*. 9th edition. Harlow: Pearson Education Limited.

Silverman, D. 2021. *Qualitative research*. 5th edition. London: SAGE Publications.

Stahl, N.A. & King, J.R. 2021. Expanding approaches for research: Understanding and using trustworthiness in qualitative research. *Journal of Developmental Education*. Available at: https://www.scirp.org/reference/referencespapers?referenceid=3766115 [Accessed: 20 January 2026].

Tejay, G.P. & Winkfield, M. 2025. Does the leadership approach matter? Examining the behavioural influences of leaders on employee information security compliance. *Information Systems Frontiers*. Available at: https://doi.org/10.1007/s10796-025-10592-4

Timcke, S., Gaffley, M. & Rens, A. 2023. *The centrality of cybersecurity to socioeconomic development policy. African Journal of Information and Communication*, *32*, 1–20. Available at: https://doi.org/10.23962/ajic.i32.16949

The Brief. 2024. Govt steps in to assist Telecom Namibia address cyber-attack fallout. *The Brief*, 15 December. Available at: https://thebrief.com.na/2024/12/govt-steps-in-to-assist-telecom-namibia-address-cyber-attack-fallout/ [Accessed: 14 July 2026].

The Brief. 2025a. Paratus Namibia hit by cyberattack. *The Brief*, 19 February. Available at: https://thebrief.com.na/2025/02/paratus-namibia-hit-by-cyberattack/ [Accessed: 14 July 2026].

The Brief. 2025b. 84GB of data compromised in Paratus ransomware attack. *The Brief*, 21 February. Available at: https://thebrief.com.na/2025/02/84gb-of-data-compromised-in-paratus-ransomware-attack/ [Accessed: 14 July 2026].

The Namibian. 2024. Telecom aware of 626.3 GB breach of customers' data. *The Namibian*, 14 December. Available at: https://www.namibian.com.na/telecom-aware-of-626-3-gb-breach-of-customers-data/ [Accessed: 14 July 2026].

Triplett, W.J. 2022. Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, 2(3), pp. 573–586. Available at: https://doi.org/10.3390/jcp2030029.

Uchendu, B, Janczewski, L. & Zhang, X. 2021. Cybersecurity culture: A systematic literature review. *IEEE Access, 9*,10659–10681. doi:10.1109/ACCESS.2021.3050212

Uchendu, B., Nurse, J.R.C., Bada, M. & Furnell, S. 2021. Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109,* 102387.

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., & Jansen, J. 2020. Risk perceptions of cyber-security and precautionary behaviour*. Computers in Human Behavior*, 75, 547–559. Available at: https://doi.org/10.1016/j.cose.2019.101651

Van Staden, M. & Van Niekerk, J. 2023. A framework for the cultivation of a cybersecurity culture in small and medium enterprises*. Information & Computer Security, 31*(2), pp. 185–204. doi:10.1108/ICS-05-2022-0091

Waiganjo, I. N. & Valungameka, E. 2023. An assessment of cybersecurity awareness level in Namibia: Case study of Windhoek. In *Proceedings of the International Conference on Information Systems and Emerging Technologies (ICISET)*, SSRN, pp. 1–12. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4654473 [Accessed: 10 January 2026].

Waiganjo, I.N., Osakwe, J. & Azeta, A. (2025). Impediments to cybersecurity policy implementation in organisations: Case study of Windhoek, Namibia. *International Journal of Research and Scientific Innovation*, *11*(10), pp. 540–546. DOI:10.51244/IJRSI.2024.1110046

Waiganjo, I.N., Osakwe, J. & Azeta, A. 2025. Cybersecurity in Namibia: Challenges, strategies and prospects. *Global Journal of Engineering and Technology Advances*, *22*(3), pp. 1–8. Available at: https://doi.org/10.30574/gjeta.2025.22.3.0048

Wang, X. et al. 2022. Leadership and cybersecurity culture: Empirical insights. *Journal of Cybersecurity Practice*, *4*(2), pp. 45–62.

Willie, M. M. (2023). The role of organizational culture in cybersecurity: Building a security-first Culture. *Journal of Research*, *Innovation and Technologies, Volume II*, *2*(4), 179-198. Available at: https://doi.org/10.57017/jorit.v2.2(4).05

Yin, R.K. 2018. *Case study research and applications: Design and methods*. 6th edition. Thousand Oaks: SAGE Publications.

Zhang, Y, Liu, J & Xu, S 2022. Quantifying the impact of human factors on cybersecurity: a social-technical perspective. *IEEE Transactions on Dependable and Secure Computing, 19*(5), pp. 3421–3435. Available at: https://doi:10.1109/TDSC.2021.3114561

LIST OF APPENDICES

Appendix A: Ethics Clearance Certificate

UNISA university of south africa

UNISA COLLEGE OF SCIENCE, ENGINEERING AND TRECHNOLOGY'S (CSET) ETHICS REVIEW COMMITTEE

Date 08/10/2025 (Amended)

ERC Reference # :2021/CSET/SOC/059
Name : Ms EN Endjala
Student #: 45163464
Staff #:

Dear Ms EN Endjala

Decision: Ethics Approval from 08/10/2025 to 08/10/2028

Researcher(s):

Ms EN Endjala, 45163464@mylife.unisa.ac.za, +264 81 203 3595

Supervisor (s):

Dr H Abdullah, abdulh@unisa.ac.za, +27 11 670 9100

Dr M Mujinga, mujinm@unisa.ac.za, +27 11 471 3154

Working title of research:

Developing a Cybersecurity Culture Framework: A Case Study of Namibia's Telecommunications Sector

Qualification:

Thank you for the application for research ethics clearance by the Unisa College of Science, Engineering and Technology's (CSET) Ethics Review Committee for the above-mentioned research. Ethics approval is granted for a period of 3 years, from 08/10/2025 to 08/10/2028.

The low-risk application was reviewed by the College of Science, Engineering and Technology School of Computing_ERC on 18/11/2021 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment.

Open Rubric

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

This application relates to an amendment request of the manual application that was originally applied for and approved prior to 2023 where after the Online Research Ethics System was implemented in CSET. This amendment request relates to change of the student working title of the research previously: ***"Beyond training and awareness: Exploring cultivation and promoting and effective cyber security risk culture programme in organisations" to the amended: "Developing a Cybersecurity Culture Framework: A Case Study of Namibia's Telecommunications Sector".***

The proposed research may now commence with the provisions that:

1. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
2. Any adverse circumstance arising during the undertaking of the research study that may affect the ethical integrity of the study, including those involving research participants, third parties or juristic persons, must be reported in writing to the School of Computing (SOC) Research Ethics Committee without delay.
3. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
4. *Any changes that may affect study-related risks to research participants, juristic or third persons, must be reported in writing to the SOC_ERC, accompanied by a progress report.*
5. *The researcher will ensure that the research study complies with all applicable national legislation, professional codes of conduct, institutional guidelines, and scientific standards relevant to the specific field of study. Where applicable, adherence to the following South African legislation is essential: the Protection of Personal Information Act (No. 4 of 2013), the Children's Act (No. 38 of 2005), and the National Health Act (No. 61 of 2003).*
6. *Future use of this research data is permitted only in de-identified form and only for secondary research with objectives similar to those of the original study. Any secondary use involving identifiable human data will require additional ethics clearance.*
7. *No field work activities may continue after the expiry date 08/10/2028. Submission of a completed research ethics progress report will constitute an application for renewal, for Ethics Research Committee approval.*
8. *The SOC_ERC may require the submission of regular progress reports on an annual basis, in alignment with Section 7.2 of the Unisa Policy on Research Ethics (2024).*

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Additional Conditions

1. Disclosure of data to third parties is prohibited without explicit consent from the research participants and Unisa.
2. Research data must be stored in compliance with the university's research data management policy for a period of up to 15 years.
3. When publishing the results, the researcher must take appropriate precautions to safeguard the confidentiality and privacy of the research participants, juristic persons, third parties, and the university, in accordance with institutional policies and ethical standards.
4. Adherence to the National Statement on Ethical Research and Publication Practices, specifically Principle 7 on Social Awareness, must be ensured. This principle states: 'Researchers and institutions must be sensitive to the potential impact of their research on society, marginal groups, or individuals, and must consider these when weighing the benefits of the research against any harmful effects, with a view to minimising or avoiding the latter where possible.' The University of South Africa (Unisa) accepts no liability for any failure to comply with this principle.".

Yours sincerely,

Signature

Prof L. Motsi

Chair of College of Science, Engineering and Technology_[School of Computing/Engineering/Science]_ERC

E-mail:motsil@unisa.ac.za

Signature

Prof I. Naidoo

Executive Dean/ By delegation from the Executive Dean of the College of Science, Engineering and Technology

E-mail: naidoi@unisa.ac.za

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Appendix B: Research Permission Letter

UNISA university of south africa

PERMISSION LETTER

Request for permission to conduct research at Mobile Telecommunication Limited (MTC)

"Beyond training and awareness: Cultivating an effective cyber security risk culture programme in organisations".

16 July 2021

Mr Raymond Cloete
MTC Head Office, Olympia
Ground Floor, Human Capital Department
Telephone number: +264612802770 and email rcloete@mtc.com.na

Dear Mr Cloete

I, Esther Ndspewa Endjala, am doing research with Dr Hanifa Abdullah, a senior lecturer, in the Department of Information Systems towards a degree in Master of Science at the University of South Africa. We are inviting MTC to participate in a study entitled: Beyond training and awareness - Cultivating an effective cyber security risk culture programme in organisations.

The aim of the study is to identify what factors impact the cultivation of cybersecurity culture in organisations. The study is also expected to collect relevant information that will enable the researcher to evaluate what is considered as barriers of cultivating and promoting an effective cybersecurity culture in the workplace.

Your company has been selected as the study institution and the research will be conducted in the context of a telecommunication organisation. The company has vast experience in the industry and has over two million active subscribers that use the telecommunications infrastructures, products, and services. This requires effective security controls, since the telecommunication industry is highly regulated due to the critical infrastructure it operates; the massive customers information processed and stored.

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

The study will entail to establish an understanding on how to promote an effective cyber security risk culture through security awareness programmes at the organisational level, as well as providing guidance to organisations to empower their employees to promptly recognise and acts against costly data breaches and regulators non-compliance issues that are faced by industries.

Potential risks to be considered during this research are anonymity, confidentiality, and informed consent. On the condition of the participant, anonymity means withholding the identities of the participants and using disguise names to protect the participants' privacy. Obtain participants' permission involved in the research and protect their privacy. A consent letter will be prepared for each participant to partake in the research study voluntarily. Data collection will only be gathered after the approval of ethical clearance has been obtained from the UNISA Ethical Committee. Captured or recorded data will be stored for a minimum period of five years, after which it will be destroyed through shredding or formatting.

Feedback procedure will contribute towards the body of knowledge and literature on cyber security field and provide new opportunities for future research work on cyber security culture across organisations of different types and sizes. Policymakers and decision-makers will make use of the research findings and recommendations thereof for the development, implementation, and promotion of cyber security culture initiative in organisations.

Yours sincerely

Esther Ndapewa Endjala
Senior IT Auditor

mtc HR
P.O.BOX 23051 • Windhoek • Namibia
Tel: +264-61 280 2418 • Fax: +264-61 280 2028
Bus. Reg. No.94/458 • VAT Reg. No.0069874-015
Physical Address:
Cnr. Mose Tjitendero & [illegible]

C. R. Cloete

Manager: Rem & Ben
+264 811002049

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Appendix C: Letter of Consent to Participants

UNISA university of south africa

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.

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 the recording of the interview discussion as data collection techniques to be used for this study. I am also aware that cross border data transfer between the researcher and supervisor will be do when required during the study.

I have received a signed copy of the informed consent agreement.

Participant Name & Surname..... (please print)

Participant Signature..... .Date.....

Researcher's Name & Surname: Esther Ndapewa Endjala

Researcher's signature:  Date: 25 October 2021

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Appendix D: Participant's Information Sheet

UNISA university of south africa

PARTICIPANT INFORMATION SHEET

Ethics clearance reference number:
Research permission reference number (delete if not applicable):

25 October 2021

Title: Beyond training and awareness: Cultivating an effective cyber security risk culture programme in organisations

Dear Prospective Participant

Student research project (Dissertation)

My name is Esther Ndapewa Endjala, and I am doing research with Dr Hanifa Abdullah, a senior lecturer in the Department of Information Systems towards a Master of Science degree, at the University of South Africa. We are inviting you to participate in a study entitled: Beyond training and awareness: Cultivating an effective cyber security risk culture programme in organisations.

WHAT IS THE PURPOSE OF THE STUDY?

I am conducting this research to find out what is required to cultivate and promote an effective cyber safety culture programme for an organisation. This study is expected to collect important information that will enable the investigation of the key obstacles that influence the cultivation and promotion of cyber security cultural programme within the organisation and determine the factors that need to be addressed to propose a structured cyber security cultural programme at organisational level.

WHY AM I BEING INVITED TO PARTICIPATE?

You were selected to participate in this research as a staff member of the Mobile Telecommunication Limited, and for your experience in working experience in this environment. Fifty-five (55) participants will be participating in the research.

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Appendix E: Unified Interview Guide

Participant Unique ID: _____ Date: _____ Time: _____

I am currently engaged in research for my Master of Science in Computing at the University of South Africa (UNISA). My study focuses on developing a cybersecurity culture framework to enhance security awareness, mitigate human-related vulnerabilities and strengthen daily resilience. This interview aims to gather your valuable insights on this subject. Please rest assured that all information you provide will be handled with the utmost confidentiality.	
SECTION A: Demographic Information (all participants)	
	Participant Gender (Male/Female)
	Age group (21-30, 31-40, 41-50, 51+)
	Role within the organisation (IT staff, non-IT staff, or Management)
	Highest qualification (Diploma/Degree/Master's/PhD)
	Number of years in the organisation (3-5, 6-10, 10+)
SECTION B: Interview Questions	
1. Can you describe your understanding of the cybersecurity culture within your organisation and how it affects your day-to-day work?	
2. How are cybersecurity policies, practices and expectations communicated within your department or across the organisation?	
3. What challenges or barriers do you experience (or observe) when it comes to following or promoting secure practices?	
4. What activities or initiatives are in place to raise cybersecurity awareness or encourage secure behaviour?	
5. What suggestions or best practices would you recommend strengthening the cybersecurity culture in your organisation?	
6. Is there anything else you'd like to share about how cybersecurity could be improved in your workplace?	
Thank you for participating in this interview	

Appendix F: Codebook for Empirical Themes Analysis

Integrated Codebook for Cybersecurity Culture Development in Namibia's Telecommunications Sector

Code Name	Definition	Illustrative Quotations (with pseudonyms)	Participant Group(s)	Frequency (n)	Linked Theme
1. Policy Awareness	Understanding and familiarity with organisational cybersecurity policies.	*"I know about the security policy, but it needs to be updated." (7_NIT)*	IT, Non-IT	18	Policy Clarity and Effective Communication
2. Policy Clarity	The degree to which employees find cybersecurity policies clear and applicable.	*"The policy still talks about floppy disks—it's outdated." (7_NIT)*	Non-IT	9	Policy Clarity and Effective Communication
3. Communication Gaps	Lack of clear communication channels between IT and other departments.	*"IT doesn't tell us about updates or incidents." (3_NIT)*	Non-IT, Management	14	Policy Clarity and Effective Communication
4. Accessibility of Policies	Ease of accessing and understanding cybersecurity documents.	*"Policies exist, but not everyone knows where to find them." (6_MGT)*	IT, Management	8	Policy Clarity and Effective Communication
5. Awareness Messages	Routine reminders or pop-ups that reinforce secure practices.	*"We could use login pop-up reminders about security." (22_MGT)*	Management	5	Policy Clarity and Effective Communication
6. Incident Communication	Reporting and feedback on cybersecurity incidents.	*"We only hear about incidents when something major happens." (19_MGT)*	IT, Management	12	Policy Clarity and Effective Communication
7. Management Visibility	The degree to which leaders are visibly engaged in security matters.	*"Executives should be more visible in promoting cybersecurity." (24_MGT)*	Management	10	Visible Leadership Commitment and Cultural Modelling
8. Top-Down Advocacy	Leadership-driven promotion of cybersecurity awareness and action.	*"Cybersecurity culture should be driven from the top down." (18_MGT)*	Management	12	Visible Leadership Commitment and Cultural Modelling
9. Leadership Role Modelling	Leaders demonstrating expected cybersecurity behaviour.	*"Top management should walk the talk." (20_NIT)*	Non-IT, Management	8	Visible Leadership Commitment and Cultural Modelling
10. Accountability Framework	Leadership enforces compliance and responsibility.	*"Cybersecurity should be in performance appraisals." (2_ITP)*	IT, Management	9	Visible Leadership Commitment and Cultural Modelling
11. Continuous Awareness Training	Regularly scheduled training sessions for employees.	*"We have weekly online sessions on the*	IT, Non-IT	22	Continuous and Role-Specific

		KnowBe4 platform." (6_ITP)			Cybersecurity Training
12. Role-Specific Training	Tailored training for departmental or role relevance.	*"Training should be department specific." (11_NIT)*	Non-IT, Management	10	Continuous and Role-Specific Cybersecurity Training
13. Practical Training	Training involving real scenarios or simulations.	*"We need more practical examples in training." (21_MGT)*	IT, Management	11	Continuous and Role-Specific Cybersecurity Training
14. Training Accessibility	Employees' ability to access cybersecurity training materials.	*"We should make training mobile to reach everyone." (22_MGT)*	Management	7	Continuous and Role-Specific Cybersecurity Training
15. Onboarding Integration	Inclusion of cybersecurity in the new employee onboarding.	*"Cybersecurity should be part of new employee orientation." (5_ITP)*	IT	8	Continuous and Role-Specific Cybersecurity Training
16. Knowledge Retention	Long-term understanding and recall of training materials.	*"People forget after training; we need reminders." (9_NIT)*	Non-IT	6	Continuous and Role-Specific Cybersecurity Training
17. Awareness Campaigns	Organised efforts to raise awareness through posters, emails, etc.	*"There are posters, but people hardly pay attention." (5_MGT)*	IT, Management	10	Continuous and Role-Specific Cybersecurity Training
18. Feedback Mechanisms	Platforms for employees to express cybersecurity concerns.	*"There are channels for reporting concerns." (10_NIT)*	Non-IT, Management	14	Collaborative Feedback and Cross-Organisational Engagement
19. Cross-Department Collaboration	Cooperation among IT, HR, and other departments.	*"When IT and HR work together, things improve." (6_MGT)*	IT, Management	11	Collaborative Feedback and Cross-Organisational Engagement
20. Employee Voice	Inclusion of employees' input in security decisions.	*"We should involve employees in developing security policies." (18_MGT)*	Management	7	Collaborative Feedback and Cross-Organisational Engagement
21. Interdepartmental Workshops	Interactive meetings to share knowledge between teams.	*"Workshops with other departments helped align understanding." (3_ITP)*	IT, Non-IT	8	Collaborative Feedback and Cross-Organisational Engagement

22. Feedback Loop	Mechanism ensuring employee concerns are addressed.	*"Employees give feedback, but responses are slow." (25_MGT)*	Non-IT, Management	6	Collaborative Feedback and Cross-Organisational Engagement
23. Resistance to Change	Employee reluctance to adopt new cybersecurity practices.	*"Some employees resist participating in training." (16_NIT)*	Non-IT, Management	9	Policy Clarity and Effective Communication
24. Departmental Silos	Limited cooperation across departments regarding cybersecurity.	*"Each department works in isolation." (8_ITP)*	IT, Management	7	Collaborative Feedback and Cross-Organisational Engagement
25. Communication Transparency	Open sharing of cybersecurity status and incidents.	*"We need regular security status updates." (25_MGT)*	Management	5	Policy Clarity and Effective Communication
26. Employee Complacency	Overconfidence leads to careless security behaviour.	*"People click on links without checking." (6_ITP)*	IT	11	Continuous and Role-Specific Cybersecurity Training
27. Management Commitment	Leadership's dedication to promoting a security culture.	*"Cybersecurity only comes up when something goes wrong." (19_MGT)*	Management	9	Visible Leadership Commitment and Cultural Modelling
28. Practical Learning	Learning through simulations and experiential exercises.	*"Simulated phishing helps us see real threats." (3_ITP)*	IT	6	Continuous and Role-Specific Cybersecurity Training
29. Incentive Systems	Rewards for positive cybersecurity behaviour.	*"Reward employees who complete their training." (6_ITP)*	IT, Management	8	Recognition, Incentives, and Sustained Engagement
30. Gamification Techniques	Use of game-like features to engage employees.	*"Gamified learning makes it more exciting." (17_NIT)*	Non-IT, Management	7	Recognition, Incentives, and Sustained Engagement
31. Peer Recognition	Informal appreciation among colleagues for secure practices.	*"We should recognise security-conscious teams." (18_MGT)*	Management	5	Recognition, Incentives, and Sustained Engagement
32. Performance Appraisal Link	Integration of cybersecurity performance in staff evaluations.	*"Include security in performance KPIs." (2_ITP)*	IT, Management	9	Recognition, Incentives, and Sustained Engagement
33. Continuous Reinforcement	Ongoing reinforcement of secure behaviour through recognition.	*"Appreciation helps people stay engaged." (10_NIT)*	Non-IT	7	Recognition, Incentives,

					and Sustained Engagement
34. Learning from Incidents	Use of real cases for organisational learning.	*"We should communicate lessons from incidents." (4_ITP)*	IT	8	Policy Clarity and Effective Communication
35. Limited Resources	Lack of sufficient tools, time, or funding.	*"We need more support from management to upgrade systems." (1_ITP)*	IT	10	Visible Leadership Commitment and Cultural Modelling
36. Resource Allocation	Management's role in providing sufficient cybersecurity resources.	*"Management allocates budgets after incidents." (6_MGT)*	Management	6	Visible Leadership Commitment and Cultural Modelling
37. Cybersecurity Ownership	Employees' sense of responsibility for cybersecurity.	*"Every employee must take responsibility." (18_MGT)*	All	15	Visible Leadership Commitment and Cultural Modelling
38. Shared Responsibility	Collective ownership of cybersecurity culture.	*"It's everyone's responsibility, not just IT." (19_MGT)*	Non-IT, Management	10	Collaborative Feedback and Cross-Organisational Engagement
39. Role Clarity	Clear understanding of cybersecurity roles.	*"People don't know what's expected of them." (12_NIT)*	Non-IT	8	Policy Clarity and Effective Communication
40. Leadership Training	Capacity building for leaders on cybersecurity advocacy.	*"Managers need more cyber leadership training." (20_MGT)*	Management	6	Visible Leadership Commitment and Cultural Modelling
41. Compliance Monitoring	Mechanisms to ensure adherence to security protocols.	*"Some staff don't complete the mandatory awareness program." (7_ITP)*	IT, Management	9	Continuous and Role-Specific Cybersecurity Training
42. Behavioural Reinforcement	Reinforcing desired cybersecurity behaviour.	*"Positive feedback motivates staff to do better." (6_NIT)*	Non-IT, Management	7	Recognition, Incentives, and Sustained Engagement
43. Transparency Culture	Encouraging openness in discussing security weaknesses.	*"We need transparency when breaches happen." (24_MGT)*	Management	6	Collaborative Feedback and Cross-Organisational Engagement
44. Practical Scenarios	Real-world examples integrated in awareness programs.	*"We should include practical case studies." (21_MGT)*	Management	5	Continuous and Role-Specific

					Cybersecurity Training
45. Mutual Accountability	Shared oversight of cybersecurity behaviour.	*"Everyone should hold each other accountable." (20_MGT)*	All	8	Visible Leadership Commitment and Cultural Modelling
46. Digital Literacy	General technological understanding supporting security compliance.	*"Some employees still lack basic digital skills." (14_NIT)*	Non-IT	7	Continuous and Role-Specific Cybersecurity Training
47. Cyber Fatigue	Declining engagement from repetitive training.	*"People lose interest when training feels the same." (9_NIT)*	Non-IT	4	Continuous and Role-Specific Cybersecurity Training
48. Incident Reporting Culture	Willingness to report security breaches.	*"Sometimes we just fix it ourselves instead of reporting." (2_ITP)*	IT	8	Policy Clarity and Effective Communication
49. Top Management Endorsement	Formal approval and visibility of executives in initiatives.	*"The CEO should drive security initiatives." (25_MGT)*	Management	6	Visible Leadership Commitment and Cultural Modelling
50. Positive Reinforcement	Reward-based encouragement for cybersecurity practices.	*"Rewarding effort encourages participation." (13_NIT)*	Non-IT, IT	6	Recognition, Incentives, and Sustained Engagement
51. Accountability in Practice	Leadership follows through with cybersecurity responsibilities.	*"We need leaders to be accountable for breaches." (23_MGT)*	Management	6	Visible Leadership Commitment and Cultural Modelling
52. Internal Benchmarking	Comparing cybersecurity practices across departments.	*"We can learn from teams doing better." (8_ITP)*	IT	4	Recognition, Incentives, and Sustained Engagement
53. Continuous Learning	Ongoing self-directed improvement on security topics.	*"Cybersecurity is always evolving; learning shouldn't stop." (1_ITP)*	IT, Management	10	Continuous and Role-Specific Cybersecurity Training
54. Inclusivity in Culture	Involving all levels of staff in cybersecurity programs.	*"Inclusivity should start from top-down." (18_MGT)*	Management	7	Security Champions and Ambassadors
55. Cultural Ambassadors	Staff who advocate for cybersecurity in their teams.	*"We need people who act as champions in each department." (11_NIT)*	Non-IT, Management	9	Security Champions and Ambassadors

56. Peer Influence	Encouraging colleagues to model and adopt secure behaviour.	*"When peers advocate, others follow easily." (5_ITP)*	IT, Non-IT	6	Security Champions and Ambassadors
57. Security Advocacy Networks	Structured ambassador programs across departments.	*"Cyber-heroes could help drive awareness." (22_MGT)*	Management	5	Security Champions and Ambassadors
58. Embedded Learning	Integrating cybersecurity awareness in daily tasks.	*"Make security part of what we do every day." (17_NIT)*	Non-IT	5	Security Champions and Ambassadors
59. Behaviour Modelling	Employees modelling correct security behaviour.	*"Colleagues learn from those who take it seriously." (15_NIT)*	Non-IT	6	Security Champions and Ambassadors
60. Empowerment through Knowledge	Enabling employees to feel capable of preventing threats.	*"Training gives us confidence to spot phishing." (2_ITP)*	IT, Non-IT	7	Security Champions and Ambassadors
61. Collective Learning	Learning through shared discussion and teamwork.	*"Discussions after training help us learn more." (13_NIT)*	Non-IT	6	Collaborative Feedback and Cross-Organisational Engagement
62. Cultural Reinforcement	Continuous reinforcement of cybersecurity values.	*"We need to keep reminding people about good practices." (3_ITP)*	IT	8	Recognition, Incentives, and Sustained Engagement
63. Employee Motivation	Intrinsic and extrinsic drivers of cybersecurity behaviour.	*"Motivation drops when effort isn't recognised." (5_NIT)*	Non-IT, Management	6	Recognition, Incentives, and Sustained Engagement
64. Continuous Feedback	Mechanisms for iterative improvement based on employee feedback.	*"We rarely hear back after giving feedback." (25_MGT)*	Management	4	Collaborative Feedback and Cross-Organisational Engagement
65. Resilience Building	Developing adaptability and alertness against threats.	*"We must stay ready for new types of attacks." (1_ITP)*	IT	6	Security Champions and Ambassadors
66. Leadership Endorsement of Champions	Executive support for ambassador programmes.	*"Management should formally appoint security champions." (18_MGT)*	Management	4	Security Champions and Ambassadors
67. Continuous Evaluation	Regular assessment of training impact.	*"We should track how training improves behaviour." (22_MGT)*	Management	5	Continuous and Role-Specific Cybersecurity Training

68. Sector Benchmarking	Comparing practices with other telecom companies.	*"We should learn from how other telecoms handle awareness." (25_MGT)*	Management	3	Recognition, Incentives, and Sustained Engagement
69. Positive Cultural Norms	Shared values that support cybersecurity practices.	*"Security is becoming part of who we are." (6_ITP)*	All	5	Security Champions and Ambassadors
70. Departmental Accountability	Managers ensure their teams follow policies.	*"Each manager must monitor compliance." (23_MGT)*	Management	4	Visible Leadership Commitment and Cultural Modelling
71. Reporting Confidence	Employees' willingness to report without fear.	*"We can report freely; no one is punished." (11_NIT)*	Non-IT	5	Collaborative Feedback and Cross-Organisational Engagement
72. Sustained Engagement	Long-term involvement of employees in security initiatives.	*"We must keep engagement alive beyond the campaigns." (20_NIT)*	All	8	Recognition, Incentives, and Sustained Engagement

Appendix G: Thematic Analysis from codes to categories to the themes

Initial Codes (Extracted from Data)	Categories	Final Theme	Illustrative Participant Evidence
Leadership visibility in security initiatives; Executive advocacy; Resource allocation for cybersecurity; Management leading by example	Leadership modelling and commitment	Theme 1: Leadership Commitment and Support	*"Executives should be more visible in these efforts."* (21_MGT) *"Top management, including the CTO, should advocate change."* (24_MGT)
Lack of regular training; One-off awareness sessions; Role-specific knowledge gaps; Interactive learning approaches	Continuous and contextualised training	Theme 2: Regular Security Awareness and Role-Specific Training	*"We haven't had any training this year."* (9_NIT) *"Gamification could make learning more engaging."* (2_ITP; 19_MGT)
Outdated policies; Poor policy communication; Limited employee awareness of policies; Inconsistent enforcement	Policy clarity and communication effectiveness	Theme 3: Policy Reviews and Communication	*"Policies exist, but most staff don't really read or understand them."* (15_NIT) *"Policy updates are not always communicated clearly."* (6_ITP)
Limited cross-departmental engagement; Minimal feedback loops; Siloed security responsibilities; Lack of consultation	Organisational collaboration and feedback	Theme 4: Collaboration and Feedback Mechanisms	*"Cybersecurity feels like an IT issue rather than a shared responsibility."* (11_NIT) *"There is little feedback after reporting incidents."* (8_ITP)
Lack of incentives; Low motivation for compliance; Interest in gamification; Recognition for secure behaviour	Motivation and behavioural reinforcement	Theme 5: Gamified Security Practices, Recognition and Incentives	*"There is no reward for doing the right thing when it comes to security."* (17_NIT) *"Incentives would motivate staff to take security seriously."* (20_MGT)
Informal security advocates; Peer influence; Trusted security contacts; Knowledge sharing champions	Distributed security leadership	Theme 6: Security Champions and Ambassadors	*"People listen more to colleagues they trust than policies."* (5_ITP) *"Having security champions in departments would help."* (22_MGT)

Appendix H: Language Editor's Certificate

ACET Consultancy
Anenyasha Communication, Editing, and Training
Box 50453 Bachbrecht, Windhoek, Namibia
Cell: +264814218613
Email: mlambons@yahoo.co.uk

06 February 2026

To Whom It May Concern

LANGUAGE EDITING – ESTHER NDAPEWA ENDJALA

This letter serves to confirm that a research report titled **DEVELOPING A CYBERSECURITY CULTURE FRAMEWORK: A CASE STUDY OF THE TELECOMMUNICATIONS SECTOR IN NAMIBIA** was submitted to me for language editing.

The research document was professionally edited, and track changes and suggestions were made in the document. The research content or the author's intentions were not altered during the editing process, and the author has the authority to accept or reject my suggestions.

Yours faithfully

PROF. (DR) NELSON MLAMBO
PhD in English
M.A. in Intercultural Communication
M.A. in English
B. A. Special Honours in English – First class
B. A. English & Linguistics