THE PERCEPTION OF MANAGEMENT ON COMPUTER-RELATED CRIME

By

John Roger Fewell

Submitted in accordance with the requirements for the degree of

MASTER OF COMMERCE

In the Department of Accounting

at Vista University

Supervisor : Professor J van Graan

Joint supervisor : Professor R P Voges

Date submitted : June 1995

Place : Port Elizabeth

ACKNOWLEDGEMENTS

This dissertation is dedicated to my wife, Avril E. Fewell, my son, Sean E. Fewell, and my daughter, Gwyneth R. M. Fewell, whose patience, support, and faith in me was never ending and provided the strength for me to complete this work.

Numerous persons have been instrumental in the completion of this work. A special thanks is extended to Professor J van Graan, my supervisor, for his guidance and help, and to Professor R P Voges, my joint supervisor, who together with Professor van Graan spent many hours in reading and commenting on this document. I also wish to thank Jenny Stokes and Jeff Hashick for proof reading this document, Dr P S Coetzee for his invaluable guidance and assistance in the final preparation and presentation of this document, and to Professor P W Cunningham for his advice on the flow and linking up of the topics within the various chapters.

DECLARATION

I declare that "The Perception of Management on Computer-related Crime" is my own work, that all sources used or quoted have been indicated and acknowledged by means of complete references, and that this dissertation was not previously submitted by me for a degree at another university.

Signed 

John Roger Fewell

SUMMARY

THE PERCEPTIONS OF MANAGEMENT ON COMPUTER-RELATED CRIME

This dissertation is concerned with the question of defining what is a computer-related crime and who is responsible for the prevention and detection of such crimes within an organisation.

The nature of computer-related crime and current criminal legislation is examined to formulate a definition of computer-related crime.

Computer-related crime is defined as encompassing :

- the introduction of fraudulent information into a computer system
- the unauthorised use of computer facilities
- the alteration or destruction of information
- the stealing by electronic means of money, financial instruments, property, services, or valuable data.

The survey that was conducted confirmed management perceptions of what comprises such a crime, and also sought to ascertain the extent of any such crime within the sampled organisations.

The survey revealed that management are solely responsible for the detection and prevention of computer-related crime within their organisations, but that they are assisted in this regard by their external auditors.

The survey also revealed that 29,6% of the respondents had experienced at least one incidence of computer-related crime within the last eighteen months, and that substantial amounts of money were involved. The perpetrators ranged from clerks to middle management. Computer-related crime appears to be on the increase with perpetrators not always being prosecuted.

KEY WORDS

computer-related crime
- definition of
- methods
- detection
- prevention
- perceptions of

computer crime
computer fraud
computer abuse
white collar crime
computer criminal legislation

ABSTRACT

THE PERCEPTIONS OF MANAGEMENT ON COMPUTER-RELATED CRIME

This report has sought to determine what is a computer-related crime, what the perceptions of management are on computer-related crime, and the extent and magnitude of any such crimes.

An extensive literature review was performed in order to identify a definition of what is a computer-related crime as well as what constitutes such a crime.

The study also sought to identify what South African legislation is currently available for the prosecution of such crimes and also includes a review of the legal situation pertaining to computer crime in both the United Kingdom and the United States of America.

Based on the literature examined, a control methodology is presented that seeks to assist management in the prevention and detection of computer-related crimes.

To measure the perceptions of management of local organisations, data were collected from a representative sample of such organisations within the Eastern Cape that included manufacturers, retailers, financial institutions, service providers, educational institutions and municipalities. The questionnaire was designed to obtain a definition of computer-related crime as well as what constitutes such a crime in order to support that definition identified within this study. This survey also sought to identify all occurrences of such crimes within the sample population. A third objective of the survey was to determine who management perceive is responsible for the detection and prevention of such crimes.

The findings from this survey supported the definition of a computer-related crime as identified within this study, as well as what constitutes such a crime. The survey identified that management rely on the internal audit department and the data processing department to prevent such crimes, whilst management assisted by the external auditors are responsible for detecting such crimes. The survey also revealed that there is a definite incidence of such crimes within the surveyed geographical region and that very few computer-related crimes are in fact being prosecuted.

The survey revealed that management are solely responsible for the detection and prevention of computer-related crime within their organisations, but they are assisted in this regard by their external auditors.

This study has sought to show that computer-related crime is more than just a technical problem, that it is a problem that involves personnel as well. Management appear not to be treating the subject with the seriousness it deserves even though computer-related crime appears to be on the increase. When such crimes are reported, the perpetrators are usually not prosecuted even though the monetary effects can run into tens and even hundreds of thousands of Rands.

CONTENTS

CONTENTS Page

CONTENTS Page

CONTENTS Page

CONTENTS Page

CONTENTS Page

CONTENTS Page

CHAPTER 1

THE PERCEPTION OF MANAGEMENT ON COMPUTER-RELATED CRIME

1.1 THE RESEARCH PROBLEM

The detection of computer-related type criminal acts has not been definitively defined as being either the task of management or that of the companies' auditors. Who in fact is responsible for detecting such acts ? This discussion has been waged for a number of years : management generally appear to believe that they can rely on their auditors to detect such crime, whereas auditors believe that the detection of such crime is solely the task of management.

The South African Institute of Chartered Accountants in their statement on the auditor's responsibility to detect and report illegal acts, other irregularities and errors identifies :

- "The responsibility for the prevention and detection of illegal acts, other irregularities and errors within the entity rests with management. Management of the entity act in a fiduciary capacity in relation to the property that is under their control and it is their responsibility to ensure that the entity's operations are conducted in accordance with all relevant legal obligations." (South African Institute of Chartered Accountants, 1992; 3).

Dealing with the responsibility of the auditor :

- "The auditor is not responsible for preventing illegal acts, other irregularities and errors." (South African Institute of Chartered Accountants, 1992; 4).
- "Based on this preliminary assessment, the auditor should plan, perform and evaluate the audit work to provide reasonable assurance of detecting illegal acts, other irregularities and errors which are material to the financial information." (South African Institute of Chartered Accountants, 1992; 5).
- The auditor is required to obtain representations from management concerning the absence of illegal acts or other irregularities (South African Institute of Chartered Accountants, 1992; 5).

The various statements issued by the South African Institute of Chartered Accountants tend to limit the liability of auditors to detect errors and fraud, and by implication, the detection of computer-related crime.

The Equity Funding case occurred in America in 1973. This case was largely instrumental for legislation being enacted by :

- o the American Institute of Certified Public Accountants requiring that auditors must express an opinion not only on the books of account but also on the computer systems (American Institute of Certified Public Accountants, 1977).
- o the federal government of the United States of America drawing up legislation defining what comprises a computer-related crime and its associated penalties.

In April of that year the Equity Funding bubble burst. The American public was incredulous as the Equity Funding Corporation of America had been the darling of Wall Street. By January 1, 1973, it had shown the greatest ten year growth of any company in America. The fraud had gone on for a decade, from 1964 to 1973. The extent of the fraud was enormous. At least $143 million in inflated pre-tax earnings and assets. The principal officers were jailed, as were two partners and a manager from that company's auditors. Class action of $ 200 million was brought against the auditors. The main motive had been an obsessive desire to keep the share price as high as possible (Loeffler, 1974; Seidler, Epstein & Epstein, 1977).

Articles relating to computer-related crime which appeared in the local South African press appear in Appendix A and are representative of what is currently being written, both the sensational and the non sensational. These articles identify a potential problem and are symptomatic of a deeper, more complex problem, and are not merely cases of sensationalism in that they blow a minor problem out of all proportion.

1.2 OBJECTIVES

The objectives of this study are :

(1) To ascertain the perceptions of management as to whose function it is to detect computer-related crime.

(2) To determine whether there is a computer-related crime problem within the selected population.

(3) To determine the extent of any computer-related crime.

(4) To provide an analysis of what management perceive is encompassed by the term, computer-related crime, as well as an identification of the predominant aspects of such computer-related crime.

1.3 HYPOTHESES

The hypotheses which will be addressed in this study are :

HO^1 : Management perceive that they are solely responsible for detecting computer-related crime within their organisations.

HO^2 : Management perceive that they are assisted by their auditors in detecting computer-related criminal acts.

HO^3 : Management perceive that they can rely on their auditors to detect computer-related criminal type acts.

1.4 METHODOLOGY

1.4.1 The scope of the study

Management refers to individuals who exercise leadership in an organisation. Managers provide the dynamic force necessary to transform the resources of a business organisation into a productive, operating concern. They are responsible for directing an organisation in the achievement of its objectives. The services of management are necessary in all co-operative endeavours (Longenecker, 1979; 22 - 23). In other words management is the process of planning, leading, controlling and organising the efforts of all the organisations members and other resources to achieve the organisation's goals (Stoner & Freeman, 1992; 6).

For the purpose of this study, the management to be surveyed are the senior managers or owners, where applicable, of those organisations. The sectors in which these organisations operated within include : local government, financial, manufacturing, banking, retail, wholesale and the service industries. In all cases only the local offices of these organisations were surveyed.

1.4.2 The sample

Probability sampling was employed to select 100 organisations randomly to be surveyed for this research. The population from which the 100 random selections were to be made comprised those organisations situated within the Eastern and Southern Cape, and Border regions.

The population comprised those companies registered with the Chamber of Commerce in Port Elizabeth, George and East London as well as the Midland Chamber of Industries in Port Elizabeth, who employed more than 10 employees at the date when the 100 organisations were selected.

The study employed a postal survey. Questionnaires were mailed to respondents with a covering letter explaining the purpose of the study together with a stamped, self addressed, envelope. If fewer than 30% responded then reminders were to be sent out three weeks later to all those respondents who had not yet returned their questionnaires.

1.4.3 The measuring instrument

Data were collected through a mail survey. A structured questionnaire was mailed to all selected respondents. This questionnaire, in Appendix B, was used to measure perceived perceptions on computer-related crime within the selected population. The questionnaire consisted of 13 statements. These structured questions included dichotomous questions, multiple choice questions with single answers, multiple questions with multiple replies, and check-lists.

The questionnaire was structured to measure the perceptions of management with regard to whose function it is to detect computer-related crime (Section A). In Section B, respondents were asked what they considered to be a computer-related criminal act. Section C sought to identify whether management had experienced any cases of computer-related crime within their organisations, as well as the number of instances and their estimated monetary value.

The questionnaire was pretested on a small scale, prior to mailing and the answers tabulated. The objective was to evaluate the suitability of the classification data measures in the questionnaire. In addition, the effectiveness of the formal instructions accompanying the questionnaire were assessed.

1.5 DIVISION OF CHAPTERS

The study is divided into seven chapters as follows :

* Chapter 1 indicates the scope of the study and the methods used. This chapter includes: problem definition and objectives, hypothesis statement, description of the methodology (including the sample procedure and the method of measurement), and a demarcation of the study.

* Chapter 2 deals with the definition of the term computer-related crime and briefly overviews the computer crime legislation within the United States of America. This chapter also briefly discusses the various methods by which a computer-related crime can be perpetrated.

* Chapter 3 presents a brief overview of computer crime legislation within the following countries :
  - o United Kingdom of Great Britain and Wales
  - o Republic of South Africa.

* Chapter 4 presents a proposed model to manage and control computer related crime.

* Chapter 5 deals with the issue of measuring management perceptions on computer-related crime.

* Chapter 6 presents the empirical results as they relate to the perceptions of management on computer-related crime, how management control computer-related crime, and the extent of the problem of computer abuse.

* Chapter 7 presents a summary of the most important findings of the study, and a discussion of the conclusions and recommendations reached.

CHAPTER 2

CLASSIFYING THE CRIME

2.1 INTRODUCTION

Experience has shown that basing the treatment of computer-related crime on computer technology is of value for both the investigative and business communities. Many computer-related crimes can be prosecuted successfully without delving deeply into the technology. Many more of them, however, are sufficiently different from traditional crimes relative to the occupations of perpetrators, environments, modi operandi, forms of assets lost, time scales, and geography to identify the subject as a unique type of crime that warrants explicit capabilities and action.

2.2 THE NATURE OF COMPUTER-RELATED CRIME

Business, economic and white-collar crimes are changing rapidly as computers proliferate into the activities and environments in which these crimes occur (Melamed, 1994).

Computers are engendering a new kind of crime. The traditional categories of criminals have been extended to include computer personnel as well. The methods of committing such crimes are also new, with a new jargon having been developed to identify such automated criminal methods as data diddling, trojan horses, logic bombs, salami techniques, superzapping, piggybacking, scavenging, data leakage, and asynchronous attacks. The forms of many of the targets of computer-related crime are also new. For example, company records are stored and maintained within computers and only printed out when required.

The timing of crimes has also changed. Traditionally, the time of criminal acts could be measured in hours, days, weeks, months and even in years. Today computer crimes are being perpetrated in milliseconds. Thus, automated crime must be considered in terms of a new time scale because of the speed of the execution of instructions within computers.

Geographic constraints do not inhibit perpetration of this new crime. A telephone with a computer terminal attached to it in one part of the world could theoretically be used to engage in a crime in an on-line computer system in any other part of the world (Melamed, 1994).

All these factors must be considered in dealing with the new crime of computer abuse. Unfortunately, however, the business community, constituting all businesses, government agencies, and institutions that use computers for technical and business purposes, is neither adequately prepared to deal with nor sufficiently motivated to report this new kind of crime to the authorities because they do not think they can get a conviction (Melamed, 1994; 1). Although reliable statistics are as yet unavailable to prove this, computer security studies for the business community and interviews with chartered accountants in public practice have indicated that few crimes of this type are ever reported for prosecution (Credo, Aiken & Carter & Michels, 1985). On the one hand, many businessmen complain that even when they do report this crime, prosecutors frequently refuse to accept the cases for a variety of reasons, including their lack of understanding of the technology and their already heavy case loads. On the other hand, prosecutors and investigators indicate that the victim's records and documentation of crimes associated with computers in the business community are inadequate for effective prosecution (Parker, 1985: 12).

2.3 DEFINITION OF COMPUTER-RELATED CRIME

Computers have been involved in most types of crime, including fraud, theft, larceny, embezzlement, bribery, burglary, sabotage, espionage, conspiracy, extortion, and kidnapping (Parker, 1985: 12). It has generally been thought of as a crime that occurs inside computers (Parker, 1985: 12). This narrow definition has recently broadened as the proliferation of computers into most societal functions proceeds at an increasing pace. The public media have added to the confusion through sensationalised, distorted, often incorrect reporting by journalists and their sources who do not sufficiently understand the technology.

Computer-related crime is not well understood and no consensus on its definition exists. One definition is that it is a form of white-collar crime committed inside a computer system; another definition is that it is the use of a computer as an instrument of a business crime (Parker, 1985: 12). A practical application of the former definition would be the making of unauthorised changes to a computer program to transfer funds from inactive accounts into a favoured account and then 'legitimately' withdrawing the funds.

The definition of a computer-related crime should be based on the problem that needs to be solved. The problem addressed is two fold; how to reduce the incidence of any type of crime in which a knowledge of computer technology is needed to understand the intentional acts that result in losses and how to successfully prosecute the perpetrators of such acts (Parker, 1985: 12). Whereas this is now predominantly a white-collar crime, both the justice and business communities must be prepared to deal with any illegal acts based on an understanding of computer technology.

The broadest definition for computer crime is therefore called for. The term "crime" is used here to mean "alleged crime" because no harmful or antisocial act is a crime until a court declares it so by convicting a party for violating a law (Parker, 1985: 24). Three terms have been used to describe the subject: "computer abuse", "computer crime", and "computer-related crime" (Parker, Nycum & Oura, 1973: 18). Organisations can improve the security of their computers based on the range of intentional acts that have been identified (Parker, 1985: 32).

Computer abuse is any intentional act involving a computer where one or more perpetrators made or could have made gain and one or more victims suffered or could have suffered a loss (Parker, et al., 1973: 18).

Computer crime is a common term used to identify illegal computer abuse; however, it implies direct involvement of computers in committing a crime. Therefore, the term computer-related crime conveys the broader meaning of any illegal act for which knowledge of computer technology is essential for successful prosecution (Parker, et al., 1973: 18). This definition is based on the scope and nature of the particular problem being addressed. The crimes and alleged crimes may involve computers not only actively but also passively. By passively is understood to mean when usable evidence of the act resides in computer stored form. The victims and potential victims include all organisations and persons who use or are affected by computers and data communication systems, as well as those people for whom data is stored and processed using computers.

Computer-related crime goes far beyond business, white-collar, or economic crime. Computer-related crime could therefore also include violent crime that destroy computers or their content or jeopardises human life and well-being because they are dependent on the correct functioning of computers controlling sensitive processes.

Computer fraud is recognised as being a potentially serious threat for most organisations using computer systems. Computer fraud involves the use of computer facilities in deception or the

concealment of loss. Such deception or loss results from the unauthorised removal or diversion of assets or the unauthorised disclosure of confidential information leading to financial loss. On the other hand, computer crime involves malicious damage, improper or vexatious use of computer facilities and theft of computer time (South African Institute of Chartered Accountants, 1989: 2).

Computers play four roles in crime: (Bureau of Justice Statistics, 1984: 3).

- Object Cases include destruction of computers or of data or programs contained in computers or supportive facilities and resources such as air conditioning equipment and electrical power, that allow computers to function.
- Subject A computer can be the site or environment of a crime or the course of or reason for unique forms and kinds of assets.
- Instrument Some types and methods of crime are complex enough to require the use of a computer as a tool or instrument. A computer can be used actively such as in automatically scanning telephone lines to make unauthorised use of a telephone system. It could also be used passively, for example, to simulate a general ledger in the planning and control of a continuing financial fraud.
- Symbol A computer can be used as a symbol for intimidation or deception. This could involve the false advertising of non-existent services, such as in dating bureaux.

All known and reported cases of computer-related crime involve one or more of these four roles.

What comprises a computer-related crime is not always clearly understood. If a computer is stolen it is simply a case of theft as no knowledge of computer technology was necessary. However, where the crime requires a knowledge of computer technology to determine the value of the article taken, the nature of the possible damage done, or the intended use by the thief, then this would be considered to be a computer-related crime.

2.4 A CLASSIFICATION OF COMPUTER-RELATED CRIME

A classification of computer-related crime is based on a variety of lists and models from several sources to produce standards for categorisation. The classification goes beyond white-collar crimes, because as stated above, computers have been used to assist in committing such crimes as robbery, larceny, extortion, espionage and sabotage.

Senator Abraham Ribicoff's Senate Bill (S240) to amend Title 18 of the U.S. Criminal Code is an omnibus crime bill making crimes of unauthorised acts in, around, and with computer and telecommunication systems. He identifies four main categories of computer-related crime: (Ribicoff, 1979).

- the introduction of fraudulent records or data into a computer system
- unauthorised use of computer-related facilities
- the alteration or destruction of information or files
- the stealing, whether by electronic means or otherwise of money, financial instruments, property, services, or valuable data.

An analysis of the JUTASTAT service revealed that there is currently no specific legislation in South Africa that deals specifically with computer crime. There is specific legislation that permits the keeping of records with the aid of a computer which is discussed in Chapter 3. The United States criminal legislation as it relates to computer-related crime, could form a very comprehensive basis for similar legislation in South Africa.

A computer abuse study has identified categories in several dimensions: (Parker, 1979: 12).

- categorised by type of loss: physical damage and destruction from vandalism, intellectual property, direct financial gain and use of services
- categorised by the role played by computers: object of attack, unique environment and forms of assets produced, instrument, and symbol
- categorised by type of act relative to data, computer programs, and services: modification, destruction, disclosure, and use of services
- categorised by type of crime: fraud, theft, robbery, larceny, arson, embezzlement, extortion, conspiracy, sabotage and espionage
- categorised by modi operandi: physical attacks, false data entry, superzapping, impersonation, wire tapping, piggybacking, social engineering, scavenging, Trojan horse attacks, trap door use, asynchronous attacks, salami techniques, data leakage, logic bombs, simulation, and viruses.

These classifications can be developed into a set of complete, detailed descriptions and models of computer-related crime. This study categorised computer-related crime by modi operandi which is discussed further within the context of paragraph 2.5.

A number of publications on computer-related crime have been produced. Among them are: "Operational Guide to White-Collar Crime Enforcement on the Investigation of Computer Crime" (Becker, 1978); "Manual for Prosecution of Computer-Related Crime" (Miller, 1978); "Computer

Fraud and Counter Measures" (Kraus & MacGaham, 1979); "Computer Crime Investigation Manual" (Schabeck, 1979); "Computer Security Management" (Parker,1981); "How to Prevent Computer Crime" (Bequai,1983); "Data Theft" (Cornwall, 1987); and "Approaching Zero, Data Crime and the Computer Underworld" (Clough & Mungo, 1993).

2.5 COMPUTER-RELATED CRIME METHODS

In the study of computer-related crime a thorough understanding is essential of the various methods of using computer technology to perpetrate such a crime.

This section describes 12 computer-related crime methods in which computers play a key role. Most technologically sophisticated computer-related crimes will use one or more of these 12 methods. A special jargon has been developed for describing these 12 computer-related crime methods. These methods result in one of the following acts being perpetrated against other computer services, computer equipment, computer programs or data:

- modification
- destruction
- disclosure
- unauthorised use of
- denial of use of.

These acts may range over many known types of crime.

2.5.1 Data Diddling

This is the simplest, and most common method used in computer-related crime. It involves changing data before or during their input to computers. The changing can be done by anybody associated with or having access to the processes of creating, recording, transporting, encoding, examining, checking, converting, and transforming data that ultimately enter a computer (Bureau of Justice Statistics, 1984: 10). Examples include the forging or counterfeiting of documents; exchanging valid computer tapes or disks with prepared replacements; source entry violations; and neutralising or avoiding manual controls (Parker, 1981: 229 - 230; Cornwall, 1987: 199;).

Data is normally protected by manual methods, and once data is in the computer, it can be automatically validated and verified. Manual controls require specific roles for trusted people

with separation of responsibilities or dual responsibilities that force collusion in order to perpetrate fraudulent acts. Batch control totals are manually calculated and then compared in the computer with matching computer-produced batch control totals. Batch control totals are prepared from data batched into smaller groups and then added together to produce a sum that is the control total. Another common control is the use of check digits or characters imbedded in the data based on various characteristics of each field of data (e.g. odd or even number indicators or hash totals). Sequence numbers and time of arrival can be associated with data and checked to ensure that data has not been removed or reordered. Large volumes of data can be checked by using utility or special-purpose programs in a computer.

Evidence of data diddling is discovered by data that does not correctly represent such data as found at sources, or lacks equality with redundant or duplicate data, does not match earlier forms of data by reversing the manual processes that have been carried out, control totals or check digits that do not agree nor meet validation and verification tests within the computer. (Parker, 1981: 229 - 230; Bureau of Justice Statistics, 1984: 10; Cornwall, 1987: 199).

2.5.2 Trojan Horse

The Trojan horse method is the covert placement of computer instructions in a program so that the computer will perform unauthorised functions but usually still will allow the program to perform its intended purposes (Bureau of Justice Statistics, 1984: 11). This is the most common method in computer program-based frauds and sabotage. Instructions may be placed in production computer programs so that they will be executed in the protected or restricted domain of the program and have access to all of the data files that are assigned for exclusive use of that program. Programs are usually constructed loosely enough to allow space to be found or created for inserting the required instructions (Parker, 1981: 230 - 234; Bequai, 1983: 23 - 24; Cornwall, 1987: 203 - 204; Clough & Mungo, 1993: 100 - 101).

The only practical method of preventing and detecting Trojan horse methods is to examine every line of code prior to it being compiled into machine readable code. There is no practical method to detect such a trojan horse if the perpetrator is sufficiently clever to insert the trojan horse directly into the machine readable code. A typical business application program can consist of thousands of computer instructions and data. The Trojan horse can also be concealed among the millions of instructions in the operating system and utility programs. It lies in wait for the execution of the target application program, inserts the extra instructions into it for a few milliseconds of execution time, and then removes them with no remaining evidence. The

computer logs would show the target program being run but not the insertion of the extra code during the actual run time as this would be completed during the normal loading and unloading routines. Even if it is discovered, there is no indication of who may have done it except to narrow the search to those programmers who have the necessary skills, knowledge, and access among employees, former employees, contract programmers, consultants, or employees of the computer or software suppliers (Parker, 1981: 230 - 234; Bequai, 1983: 23 - 24; Cornwall, 1987: 203 -204; Clough & Mungo, 1993: 100 - 101).

2.5.3 Salami Technique

An automated form of crime involving the theft of small amounts of assets from a large number of sources is identified as a salami technique (taking small slices without noticeably reducing the whole) (Parker, 1985: 33). For example, in a banking system, the demand deposit accounting system for cheque accounts could be changed (using the Trojan horse method) to randomly reduce a few hundred accounts by 10 cents or 15 cents by transferring the money to a predetermined account, where it can be legitimately withdrawn through normal methods. No accounting controls are violated because the money is not removed from the accounting system, merely rearranged within the clients records so that the total of the clients records still agree to the accounting records. The success of the fraud is based on the idea that each cheque account customer looses so little that it is of little consequence to the customer. Many variations are possible. The assets may be an inventory of products, computer services and facilities, or money (Kraus & MacGaham, 1979: 15 -16; Parker, 1981: 234 - 238; Cornwall, 1987: 201).

One salami method in a financial system is known as the "round down" fraud. The round down fraud requires a computer system application where large numbers of financial accounts are processed. The processing must involve the multiplication of Rand amounts by numbers - such as in interest rate calculations. This arithmetic results in products that contain fractions of a cent. The round down fraud has been known for many years and does not require a computer to carry it out. A computer would make it a lot easier to perpetrate (Parker, 1981: 234 - 238).

2.5.4 Superzapping

Superzapping derives its name from Superzap, a macro/utility program used in most IBM computer centres as a systems tool (Bureau of Justice Statistics, 1984: 17). Any computer

centre that has a secure computer needs a "break glass in case of emergency" type computer program that will bypass all controls in order to modify or disclose any of the contents of the computer. Computers sometimes stop, malfunction or enter a state that cannot be overcome by normal recovery or restart procedures. Computers also perform unexpectedly and need attention that normal access methods do not allow. In such cases, a special access program is needed. This is similar in one way to a master key to be used if all other keys are lost or are locked in the safe they were meant to open (Parker, 1981: 238 - 240; Cornwall, 1987: 199; Clough & Mungo, 1993: 65).

Utility programs such as Superzap are powerful and dangerous tools in the wrong hands. They are normally used only by systems programmers who maintain the computer operating system. These utilities should be kept secure from unauthorised use. However, they are often placed in program libraries where they can be used by any programmer or operator who knows of their presence, how to use them and the necessary password to access them (Parker, 1981: 238 - 240).

2.5.5 Trap Doors

In the development of large applications and computer operating systems, it is the practice of programmers to insert debugging aids that provide breaks in the code for insertion of additional code and intermediate output capabilities. The design of computer operating systems attempts to prevent both access to them and the insertion of code or modification of such code. Consequently, system programmers will sometimes insert code that allows a compromise of these requirements during the debugging phases of implementation and later when the system is being maintained and improved. These facilities are referred to as trap doors (Bureau of Justice Statistics, 1984: 19). Normally, trap doors are eliminated in the final editing but sometimes they are overlooked or purposely left in to facilitate ease of making further access and modification. In addition, some unscrupulous programmers may purposely introduce trap doors in order that they can compromise the computer at a later date. Designers of large complex programs may also introduce trap doors inadvertently through weakness' in design logic (Bureau of Justice Statistics, 1984: 19). Trap doors may also be introduced in the electronic circuitry of computers. For example, not all of the combinations of codes may be assigned to instructions found in the computer and documented in the programming manuals. When these unspecified commands are used, the circuitry may cause the execution of unanticipated combinations of functions that allow the computer system to be compromised (Parker, 1981: 240 -242; Bequai, 1983: 24; Cornwall, 1987: 203).

During the use and maintenance of computer programs and computer circuitry, ingenious programmers invariably discover some of these weakness' and take full advantage of them for both useful and also for innocuous purposes. However, these trap doors may also be used for unauthorised, malicious purposes as well. Functions that can be performed by computer programs and computers that are not in the specifications are often referred to as negative specifications. It is difficult enough for designers and implementers to make programs and computers function according to specifications and to prove that they perform according to those specifications. Similarly, it is difficult to prove that a computer system does not perform functions that were not specified (Parker, 1981: 240 -242; Cornwall, 1987: 203).

Research is continuing on a high-priority basis to develop methods of proving the correctness of computer programs and computers according to complete and consistent specifications (IBM, 1992; 26 - 27). There is no simple method currently available for proving the correctness or otherwise of commercially available computers and computer programs. Therefore, trap doors will continue to exist, and there is never any guarantee that they have all been found nor corrected (Parker, 1981: 240 -242; Cornwall, 1987: 203).

2.5.6 Logic Bombs

A logic bomb is a computer program executed at appropriate or periodic times in a computer system that determines conditions or states of the computer that facilitate the perpetration of an unauthorised, malicious act (Bureau of Justice Statistics, 1984: 21). For example, in one case, secret computer instructions were inserted (a Trojan horse) in the computer operating system where they were executed periodically. The instructions would test the year, date and time of day clock in the computer so that on a specified day of the year 2 years later at 3.00 p.m. the time bomb, a type of logic bomb, would go off. The logic bomb would then display a confession by the programmer on all of the 300 computer terminals that were on-line at that time. This message would appear for a few seconds on the screens. The logic bomb would then cause the entire computer system to crash. This was timed so that the perpetrator would be geographically a long distance from the computer and its users (Parker, 1976: 53). In another case, a payroll system programmer put a logic bomb in the personnel system so that if his name was ever removed from the personnel file, indicating termination of employment, a secret code would cause the entire personnel file to be erased (Parker, 1976: 53; Parker, 1981: 242 - 243; Cornwall, 1987: 206).

A logic bomb can be programmed to trigger an act based on any specified condition or data that may occur or be introduced. Logic bombs are usually placed in the computer system using the Trojan horse technique (Parker, 1981: 243).

2.5.7 Asynchronous Attacks

Asynchronous attack techniques take advantage of the asynchronous functioning of a computer operating system (Bureau of Justice Statistics, 1984: 21). The majority of computer operating systems function asynchronously based on the services that must be performed for the various computer programs presently in memory waiting to be executed. For example, several jobs may simultaneously call for output reports to be printed. The operating system actually stores these requests and, as resources become available, performs them in the order in which resources are available to fit that request or according to an overriding priority schedule. Therefore, rather than executing requests in the order they are received, the system performs them asynchronously based on available resources. There are highly sophisticated methods of confusing the operating system to allow it to violate the isolation of one job from another (Parker, 1981: 243 - 244).

2.5.8 Scavenging

Scavenging can be defined as a method of obtaining information that may be left in or around a computer system after the execution of a job (Bureau of Justice Statistics, 1984: 23). A simple example of physical scavenging might be the searching of rubbish bins for copies of discarded computer listings or carbon paper from multiple-part forms. More technical and sophisticated methods of scavenging can be done by searching for residual data left in disc storage within the computer after the job has been executed (Parker, 1981: 245 - 246).

For example, most computer operating systems do not erase buffer storage areas used for the temporary storage of input or output data, nor do they erase magnetic disk or magnetic tape storage media. The reason for this is the excessive computer time that would be required to do so. Therefore, new data is simply written over the old data. It is possible for the next job to be executed to first read the old data before over-writing it with the new data (Parker, 1981: 246; Bureau of Justice Statistics, 1984: 23).

2.5.9 Data Leakage

A number of known computer-related crimes involved the removal of data from computer systems or computer facilities (Lampson, 1977: 34). The removal of data presents the most dangerous exposure to the perpetrator. His technical act may be well hidden in the computer; however, to convert it to economic gain, he must get the data out of the computer system. Output reports are subject to examination by computer operators and other data processing personnel. Several techniques can be used to leak data from a computer system. The perpetrators may be able to hide the sensitive data in otherwise innocuous looking output reports. This could be done by adding to blocks of data (Parker, 1981: 246 - 247).

In more sophisticated ways the data could be interspersed with otherwise innocuous data. An even more sophisticated method might be to encode data to look like something different than it is. For example, a computer listing may be formatted so that the secret data is in the form of different lengths or printer lines, number of words or numbers per line, locations of punctuation, and use of code words that can be interspersed and converted into meaningful data. Theoretically data can be obtained by causing a printer to print and skip lines in a pattern where the noise of the printer, recorded with a cassette tape recorder, might be played back at slow speed to produce a pattern translatable into binary information. These are rather exotic methods of data leakage. (Parker, 1981: 246 -247; Bureau of Justice Statistics, 1984: 24).

2.5.10 Piggybacking and Impersonation

Piggybacking and impersonation can be done either physically or electronically. Physical piggybacking is a method for gaining access to controlled access areas controlled by either electronically or mechanically locked doors. For example, an individual usually with his hands full of computer-related objects such as tape reels stands by the locked door, when an authorised individual arrives and opens the door, the piggybacker simply goes in after or along with him. Turnstyles or a stationed guard are the usual methods of preventing this type of unauthorised access. The turnstyle allows passage of only one individual with a metal key, an electronic or magnetic card key, or combination lock activation. A "mantrap" could be installed which is a double-doored closet through which only one person at a time can move with one key action. Success of this method of piggybacking is dependent upon the quality of the access control mechanism as well as the alertness of authorised persons in resisting co-operation with the perpetrator (Parker, 1981: 247 - 249; Bequai, 1983: 24; Bureau of Justice Statistics, 1984: 25; Cornwall, 1987: 201).

Electronic piggybacking can take place in an on-line computer system where individuals are using terminals, and identification is verified automatically by the computer system. When a terminal has been activated, the computer authorises access, usually on the basis of a key, secret password, or other passing of required information (protocol). Compromise of the computer can take place when a hidden computer terminal is connected to the same line and used when the legitimate user is not using his terminal. The computer will not be able to differentiate or recognise the two terminals, but senses only one terminal and one authorised user. Piggybacking can also be accomplished when the user does not sign off when his task on the terminal has been completed thus leaving the terminal in an active state or leaving the computer in a state where it assumes that the user is still active (Bureau of Justice Statistics, 1984: 23).

Impersonation is the process by which one person assumes the identity of another. Physical access to computers or computer terminals and electronic access through terminals to a computer require positive identification of an authorised user. The verification of identification is based on some combinations of something the user knows, such as a secret password; something the user is -.i.e., a physiological characteristic, such as finger print, hand geometry, or voice; and something the user possesses, such as a magnetic stripe card or metal key. Anybody with the correct combination of identification characteristics can impersonate another individual (Parker, 1981: 248 - 249; Bequai, 1983: 24; Bureau of Justice Statistics, 1984: 25; Cornwall, 1987: 201).

2.5.11 Wire Tapping

The potential for wire tapping grows rapidly as more computers are connected to communication facilities and increasing amounts of electronically stored assets are transported from computer to computer over communication circuits. Wire tapping has not become popular as far as it is known because of the many easier ways to obtain or modify data.

Wire tapping equipment is relatively cheap and can be imported from the USA (Bureau of Justice Statistics, 1984: 28). Recording and printing of data can usually be done more directly and easily through the computer system or by impersonation through terminals. The perpetrator usually will not know when the particular data he is interested in will be sent. Therefore, he must collect relatively large amounts of data and search for the specific items of interest. Identification and isolation of the communications circuit can also pose a problem for the

perpetrator. Interception of microwave and satellite communications represents even greater difficulty because of the complexity and cost of the equipment to perform such an operation. In addition, to further complicate matters, there might be active detection facilities built into the communications network (Parker, 1981: 249 -250; Bequai, 1983: 22).

The best method of protecting data is encryption or secret coding of the data using an encryption key. New, powerful products are now on the market to provide encryption. It is anticipated that most data which is valuable will be routinely encrypted within the next few years. This will probably greatly reduce the threat of wire tapping.

2.5.12 Simulation and Modelling

A computer can be used as either a tool or as an instrument in a crime. The computer can be used for planning or to control the crime. Complex white- collar crime often requires the use of a computer because of its sophistication. An existing process can be simulated on a computer or a planned method could be modelled to determine its possible success (Parker, 1981: 259 - 251; Bureau of Justice Statistics, 1984: 28; Cornwall, 1987: 203).

In one case involving a million dollar manual embezzlement, an accountant owned his own service bureau and simulated his company's accounting and general ledger system on his computer. He was able to input correct data and modified data to determine the effects of the embezzlement on the general ledger. He also had the capability to run the simulation in the reverse direction by inputting to the computer the general ledger data he wished to have. He then ran the system in reverse to determine the false accounts payable and accounts receivable entries required that would result in the required general ledger output (Parker, 1976: 74).

The use of a computer for simulation and modelling normally requires extensive amounts of computer time and computer program development.

2.6 CONCLUSION

A study of computer-related crime requires that the term computer crime be defined and what in fact constitutes a computer crime. This chapter has discussed the concept of computer-related crime as well as its constituent parts.

In order to gain the necessary background to computer crime, the nature of computer-related crime was firstly briefly discussed. This led to the definition that computer crime is an intentional act involving a computer where one or more perpetrators made or could have made a gain and one or more victims may have or could have suffered a loss. The nature of what actually comprises such a crime was then discussed.

Having defined the basic concepts, the development of American computer abuse legislation was then briefly discussed.

In any study of computer-related crime the methods of perpetrating such acts must be defined. This study defined twelve computer-related crime methods in which computers play a key role.

Computer-related crime is defined in the present literature. Many definitions are possible because of the extensive nature or field covered. The best definition - "the intentional act involving a computer where one or more perpetrators made, or could have made, gain and one or more victims suffered, or could have, suffered loss".

The 12 methods discussed cover the major "forms" of the crime.

CHAPTER 3

COMPUTER-RELATED CRIMINAL LEGISLATION

3.1 INTRODUCTION

This chapter continues the discussion by tracing computer-related criminal legislation within the United States of America, the United Kingdom of Great Britain as well as that within the Republic of South Africa. The economy of these two countries has had a major impact upon our economy and it is considered fitting that a brief study of computer-related criminal legislation be conducted as it pertains to these two countries prior to discussing the South African situation.

A historical overview of the American and United Kingdom computer crime legislation is necessary, as these two countries have had more experience in dealing with computer-related crimes.

3.2 COMPUTER ABUSE LEGISLATION IN THE UNITED STATES OF AMERICA

Computer abuse started with the emergence of computer technology in the late 1940's. As the number of people in the computer field began to increase, the facet of human nature of doing harm to society for personal gain took hold as it does with any segment of the human population; the problem of crime became especially acute as computer technology proliferated into sensitive areas in society. This occurred first in military systems and then in engineering, science, and finally business applications (Bureau of Justice Statistics, 1984: 6).

There is limited published material available on computer crime in South Africa. The information that there is, is very brief. Consequently, to study computer-related crime, the very detailed and explicit cases as reported in the United States are referred to in support of statements made within this study.

The first recorded computer abuse occurred in the United States of America in 1958 (Parker, et al., 1973: 23). The first United States federally prosecuted computer-related crime, identified as

such, was the alteration of bank records by computer in Minneapolis, in the United States of America, in 1966 (Parker, et al., 1973: 23).

Pursuit of the study of computer-related crime and computer abuse has been controversial. In 1970, a number of researchers concluded that the problem was merely a small part of the effect of technology on society and was not worthy of specific, explicit research (Bureau of Justice Statistics, 1984: 6). The increase in substantial losses associated with intentional acts involving computers prove the fallacy of this view. The explicit identification of computer-related crime as a subject for research and development of preventative measures in criminal justice suffered a similar fate in the mid-1970's (Bureau of Justice Statistics, 1984: 6). Researchers argued that computers should not be the focus in a study of various types of crime (Bureau of Justice Statistics, 1984: 6). They believed the involvement of computers should be subordinate to the study of each specific type of crime, both manual and automated (Bureau of Justice Statistics, 1984: 6).

The formal study of computer abuse was started in the United States of America in 1971. In 1973 the first national conference on computer abuse produced a comprehensive report (Parker, et al., 1973: 24). Since then, many reports, papers, journal articles, and books have been published describing research to date.

The interest of the criminal justice community in the United States of America began in response to increasing numbers of cases and action by criminal justice organisations, including the Federal Bureau of Investigation (FBI) Academy, Criminal Justice Conferences on white-collar and organised crime, National District Attorneys Association Economic Crime Project, local FBI offices, and the National College of District Attorneys. In 1976, the FBI established for its agents a 4-week training course in investigation of computer-related crime and another for other agencies in 1978 (Bureau of Justice Statistics, 1984: 7).

In 1976, as a result of the increasing frequency of computer-related crime cases and the inadequacy of federal criminal law to deal with it, Senator Abraham Ribicoff and his U.S. Senate Government Affairs Committee started a research project on computer-related crime. This committee produced two reports on its research (U.S. Senate Committee on Government Operations, 1976; 1977). Senator Ribicoff introduced the first Federal Systems Protection Act Bill in June 1977. As the result of U.S. Justice Department comments and hearings in June 1978, the Federal Systems Protection Act Bill, was introduced. This Bill was revised and a new bill, S240, was introduced into Congress. All the American states have computer-related crime laws based on the Ribicoff bill (U.S. Senate Subcommittee on Criminal Law and Procedures,

1978). This federal act has been subsequently amended as required by its subsequent use in prosecutions of computer-related crimes. The U.S.A. has comprehensive legislation on computer-related crime.

3.3 COMPUTER ABUSE LEGISLATION IN THE UNITED KINGDOM

3.3.1 INTRODUCTION

With the universal use of computers throughout Government and industry within the United Kingdom, there has naturally been an associated change in the law. Today the legal framework under which a company operates has been modified by many statutes which take account of the use of computers in offices, factories and for the keeping of records generally. This chapter examines a number of United Kingdom Acts that address computer-related criminal prosecutions.

3.3.2 THE COPYRIGHT (COMPUTER SOFTWARE) AMENDMENT ACT 1985

This new Act has made two changes in the law. It has put beyond doubt the question of whether a computer program was a literary work within the meaning of the Copyright Act 1956. This new Act has said that it is, and what is more, it has said so retroactively - something that is very unusual for any Act. However, the view amongst all lawyers in the field is that this statement has not changed the law since, although the point has never been argued to the point of a final hearing, they were all certain that computer programs were protected under the 1956 Act (Wong & Farquhar, 1987).

The second main change brought about by the amendment has been the increase in criminal penalties for software piracy. The Copyright Act 1956 not only created civil rights in copyright works but also created certain criminal offences based on the same facts. These criminal offences were little used because the maximum fine was only £50. However, an amendment to the Act to deal with video and record piracy was put through Parliament which increased the maximum fines to several thousand pounds. At the same time an organisation called the Federation Against Copyright Theft (FACT) was set up to supply information to the police and bring prosecutions under the new amendment. FACT came into existence at a key time because the video boom had turned the UK into the world video pirate centre. Organised crime

from the States and the Far East was beginning to get involved and Scotland Yard was very keen to nip the matter in the bud (Wong & Farquhar, 1987).

FACT was very successful and a lot of video piracy was stamped out. However, just as FACT was getting into its stride, the home computer boom took off. Pundits pointed out the similarities between cassette tapes and small program tapes and indicated that organised crime could move into this area. Further discussion with major computer manufacturers lead to the establishment of the Federation Against Software Theft or FAST, which is the organisation which steered the new computer copyright amendment through Parliament (Wong & Farquhar, 1987).

However, the thrust of FAST is not just against piracy of home computer games. One company that was closely involved in the establishment of FAST is Digital Equipment (DEC). DEC, like most major hardware manufacturers, see their future earnings growth in software rather than hardware. DEC has been particularly concerned about unauthorised copying of their operating systems on the PDP 11 series - mainly RSX 11. Litigation against Darkcrest in which DEC allege such piracy so weakened Darkcrest that it went into receivership. It is well known that DEC has been able to get several tens of thousands of pounds out of many software houses without recourse to litigation merely by saying that they are sending their investigators round to do a special audit (Wong & Farquhar, 1987).

3.3.3 COMPUTER EVIDENCE ACT 1986

On 1 January 1986 the Government brought into effect all of the provisions of the Police and Criminal Evidence Act 1984. The Act, which dealt mainly with police powers of detention and questioning, also contained a section of particular interest to computer users since it marked a major change in the law on admissibility of evidence from computer records in criminal cases

Evidence may be defined as any material which tends to persuade the court of the truth or probability of some fact asserted before it. A great deal of evidence which would be capable of having this persuasive effect has not been admitted by the courts for reasons which have their roots in the history of the development of the United Kingdom legal system. Automatically generated evidence from computers has, until this Act, sometimes been considered to be inadmissible (Wong & Farquhar, 1987).

However, prior to the new Act the matter was far from settled. Very few cases actually came before the courts where either party contested the admissibility of computer generated evidence. Partly this has been because of the way criminal cases are argued in court. In most trials one party tenders the evidence and the other party instantly raises objections to its admissibility or remains silent. Spotting whether evidence is admissible or not can thus be a split-second decision. In the case of computer produced evidence lawyers who could have objected to the admissibility of the evidence have not so objected because they have not known enough about the technology to say why the evidence is not admissible (Wong & Farquhar, 1987).

The new Act, in theory, changes this position. First it deals with the problem of evidence derived from documentary records which were admissible under the Criminal Evidence Act 1965 and automatically produced computer records which were not. Many personal balances with major building societies which are recorded on computers can today be considered to be made up of documentary records (withdrawals and payments is recorded in the building society book) and automatically generated records (withdrawals from building society cash dispensers). Under the 1965 Act it could be argued that any building society balances which contained automatically generated records was not within the class of admissible documents and had to be excluded from consideration by the court in criminal cases. The new Act changes this position and establishes a system whereby computer produced documents of this kind can be admitted provided they are accompanied by a certificate signed by a person in authority covering certain matters. Most of these are set out in section 69 of the Act (Wong & Farquhar, 1987).

"69. (1) In many proceedings a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown

a) That there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer;

b) that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents; and

c) that any relevant conditions specified in rules of court under subsection (2) below are satisfied.

(2) Provision may be made by rules of court requiring that in any proceedings where it is desired to give a statement in evidence by virtue of this section such

information concerning the statement as may be required by the rules shall be provided in such form and at such times as may be so required.".

In the case of accounting records produced by a computer, audit controls on the use of the computer and access to the records produced using it will be relevant in considering whether there are reasonable grounds for saying that there may have been improper use of the computer.

Additionally the term "improper use" in the clause could also refer to compliance with good data processing practices.

At first the requirement under the Act "that at all material times the computer was working properly" looks very hard to prove. In fact because of the certification procedure a very doubtful computer system can be given an air of respectability if nobody chooses to look too hard at the person who is making the certificate. (Wong & Farquhar, 1987). Under Part II of Schedule 3 of the Act supplementary provisions to Section 69 set out the content of the certificate exhibiting the printout.

"8. In any proceedings where it is desired to give a statement in evidence in accordance with section 69 above a certificate

a) identifying the document containing the statement and describing the manner in which it was produced;

b) giving such particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer;

c) dealing with any of the matters mentioned in subsection (1) of section 69 above; and

d) purporting to be signed by a person occupying a responsible position in relation to the operation of the computer

shall be evidence of anything stated in it; and for the purpose of this paragraph it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it."

It will be obvious that "a person occupying a responsible position in relation to the operation of the computer" will be an entirely different type of person in different companies and in different data processing environments. In a very small business the person may be the sole trader himself or his bookkeeper. In a medium sized firm using a minicomputer the person would be the system manager of the system. In a large mainframe operation the person will be the data processing manager or possibly the computer operations director for the company. Each of these will have varying degrees of technical knowledge. Some will be using the computer as a mere tool and will not be capable of saying on a basis of knowledge whether the computer was working correctly or not. Others will be very familiar with the correct operation of their large computer systems and will know, for example, when and how to study the console log to determine whether at the material time the computer was emitting signs that would indicate it was not working properly. System managers who will have done the system generation on their system will know how their system has been configured, what error logging facilities have been enabled, should know whether the programs were loaded in order specified by the manufacturer and whether any additional programs co-resident in memory have been put on the system which could compete with each other and interact in unspecified ways.

However, the Act does take account of the fact that lawyers may wish to cross-examine the deponent to such a statement.

"9. Notwithstanding paragraph 8 above, a court may require oral evidence to be given of anything of which evidence could be given by a certificate under that paragraph."

It is thought that now that the Act is in force there will be frequent applications to cross-examine deponents and, initially at least, courts will look on such applications favourably in almost all cases (Wong & Farquhar, 1987). The making of false statements in such a certificate is a criminal offence as set out in paragraph 10 of the Schedule.

"10. Any person who in a certificate tended under paragraph 8 above in a magistrates' court, the Crown Court or the Court of Appeal makes a statement which he knows to be false or does not believe to be true shall be guilty of an offence and liable

a) on convicting on indictment to imprisonment for a term not exceeding two years or to a fine or to both;

b) on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum (as defined in section 74 of the Criminal Justice Act 1982) or to both."

The prescribed fine is £2 000 or such sum as is for the time being substituted therefore by an order in force under the Magistrates' Courts Act 1980. The Criminal Penalties Order 1984, permits the Secretary of State to substitute by order such sum as appears to him to be justified if it appears to him that there has been a change in the value of money since the prescribed fine was specified.

The Act has some interesting provisions regarding the weight to be attached to evidence from a computer. It clearly implies that less weight should be given to information recorded not at the time of the event but long after the event. This is similar to the rule under the present law which allows witnesses to refresh their memories by looking at notices made contemporaneously but not at notes made long after the event. This clause was put into the Act after Professor Smith of Nottingham University pointed out in a letter to the Times that without such a clause computer produced records would be in a better position than records produced by manual means (Wong & Farquhar, 1987: 44). Additionally the Act suggests that less weight should be given to computer evidence where the person concerned with the supply of the information had an incentive to fabricate it. This provision reflects the constant fear in the common law of perjury, fabrication and attempts to abuse or pervert the course of justice.

"11. In estimating the right, if any, to be attached to a statement regard shall be had to all the circumstances from which any incongruence can reasonably be drawn as to the accuracy or otherwise of the statement and, in particular

a) to the question whether or not the information which the information contained in the statement reproduces or is derived from was supplied to the relevant computer or recorded for the purpose of being supplied to it, contemporaneously with the occurrence or existence of the facts dealt with in that information; and

b) to the question whether or not any person concerned with the supply of information to that computer, or with the operation of that computer or any equipment by means of which the document containing the statement was produced by it, had any incentive to conceal or misrepresent the facts.

12. For the purposes of paragraph 11 above information shall be taken to be supplied to a computer whether it is supplied directly or (with or without human intervention) by means of any appropriate equipment."

However, these clauses do not appear to deal with the situation where a data processing manager is charged with a crime the key evidence of which will be the information recorded on the computer which he is responsible for. Because he is the person in authority it would seem to be the case that he should depose to the certificate since anyone else who so deposed could not do so with knowledge (Wong & Farquhar, 1987).

3.3.4 COMPUTER MISUSE ACT 1990

Unauthorised access to computer material

A person who causes a computer to perform any function with intent to secure access to any program or data held in any computer, and the access he intends to secure is unauthorised, and he knows at any time that is the case, is guilty of an offence. This person is liable on summary conviction to imprisonment for a term not exceeding six months or to the prescribed fine not exceeding £2 000 (subject to the comment mentioned under point 3.3.3 above regarding the powers of the Secretary of State to change such fine) or both.

The Act contains no definition of the term "computer".

"Hacking" is now covered by the new offences created by this Act.

Section 1(2). Intent need not be directed at any particular program or data, a program or data of any particular kind, or a program or data held in any particular computer.

Section 17(2). Held in any computer includes - where the person alters or erases the program or data, copies or moves it to another storage medium or to a different location in the storage medium where it is held, uses it, or has it output from the computer in which it is held.

Section 17(6). Provides guidance on the interpretation of "any program or data held in a computer".

Section 17(5). Access is unauthorised if the person is not himself entitled to control access of the kind in question to the program or data, and he does not have consent to such access by him from any person so entitled.

Section 1(1) (3). The Act does not require the use of one computer to gain unauthorised access to another.

It is immaterial, except as otherwise provided, whether any act or event proof of which is required for conviction of the offence occurred in the home country concerned (section 4(6): defined as England, Wales, Scotland, and Northern Ireland), or whether the accused was in the home country concerned at the time of the of the act or event. However, at least one significant link with domestic jurisdiction must exist in the circumstance of the case for the offence to be committed (section 8). It is also immaterial for guilt whether or not the accused was a British citizen at the time the offence was committed (section 9(1)).

Section 5(2). For the purpose of the offence, where either the accused, or the computer concerned, was in the jurisdiction at the time of the offence.

A search warrant may be issued by a circuit judge where there are reasonable grounds for believing that an offence under this section has been or is about to be committed (section 14(1)), and the section creating the offence is deemed to have effect without prejudice to any enactment relating to power of inspection, search or seizure (section 10). The circuit judge is satisfied that there are reasonable grounds for believing that an offence of unauthorised access to computer material has been or is about to be committed in any premises, and evidence is in those premises. Rules for the jurisdiction of magistrates' courts in respect of offences under this section, and time limits for their prosecution, are also specified (section 11).

Unauthorised access with intent to commit further offences

A person who commits an offence of unauthorised access (section 1) with intent to commit an offence for which the sentence is fixed by law or for which a person may be sentenced to a term of five years imprisonment (section 2(2), or with intent to facilitate the commission of such an offence, is guilty of an offence and liable, on conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the prescribed amount mentioned above, or to both and on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both (section 2(1) and 2(5). It is immaterial whether the further offence is to be committed on the same occasion as the unauthorised access or on some future occasion

(section 2(3)), and a person may be guilty of this offence even though the facts are such that the commission of the further offence is impossible (section 2(4).

Provisions concerning jurisdiction are similar to those for the offence of unauthorised access, with the exception that no significant link need exist for the commission of that offence to be established in proceedings for this offence (section 4(3), 4(4)).

A person who is found not guilty of this offence may be nevertheless be convicted on the lessor charge of unauthorised access if he could have been found guilty of that offence within the time limits applicable to such proceedings (section 12).

Unauthorised modification of computer material

A person who does any act which causes an unauthorised modification of the contents of any computer, and at the time when he does the act has the requisite intent and the requisite knowledge (section 3(4): knowledge that any modification he intends to cause is unauthorised), is guilty of an offence and liable, on conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the prescribed limit or to both and, on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both (section 3(1), (7)). A modification of the contents of a computer does not constitute an offence under the Criminal Damage Act 1971 unless its effect is to impair the computer's physical condition (section 3(6)).

> Section 17(8). Modification is "unauthorised" if the person whose act causes it is not entitled to determine whether the modification should be made, and he does not have the consent to the modification from any person who is so entitled.
>
> Section 17(7). Modification includes the alteration or erasure of any program or data held in the computer concerned, or addition to the contents of any program or data.
>
> Section 3(2). Intent is defined as to cause a modification of a computer and thereby impair the operation of any computer, prevent or hinder access to any program or data, or impair the operation of any such program or the reliability of any such data.
>
> Section 3(3). Intent need not be directed at any particular computer, any particular program or data or a program or data of any particular kind, or any particular modification or a modification of any particular kind.

It is immaterial, except as otherwise provided, whether any act or event proof of which is required for conviction of the offence occurred in the home country (section 4(6)) concerned, or whether the accused was in the home country concerned at the time of the act or event (section 4(1). However, at least one significant link with domestic jurisdiction must exist in the circumstances of the case for the offence to be committed (sections 4(2) and 8). It is also immaterial for guilt whether or not the accused was a British citizen at the time the offence was committed (section 9(1)).

A person who is found not guilty of this offence, or any attempt to commit such an offence, may nevertheless be convicted on the lessor charge of unauthorised access if he could have been found guilty of that offence within the time limits applicable to such proceedings (section 12).

3.3.5 CONCLUSION

As in the United States of America, there is legislation dealing specifically with computer-related criminal activities. The Computer Misuse Act, together with the Compute Evidence Act and the Copyright Act enable successful prosecutions against perpetrators of computer-related criminal activities. Punishment of wrong doers can result in either a fine or imprisonment of up to five years, or both. Perpetrators of such criminal-related crimes can expect the full force of the law to be used in the prosecution of their activities.

3.4 COMPUTER ABUSE LEGISLATION IN THE REPUBLIC OF SOUTH AFRICA

3.4.1 INTRODUCTION

This section deals specifically with the computer abuse situation in South Africa and briefly discusses the legal implications of computer abuse as well as what the situation is regarding the statutory law.

An analysis of the JUTASTAT service revealed that there is no legislation dealing specifically with computer crime. South Africa does not have a set of comprehensive laws similar to that in the United Kingdom of Great Britain and the United States of America that deal specifically with computer-related criminal acts.

There is no definition of what comprises a computer-related crime nor the penalties to be imposed on such crimes.

3.4.2 THE LEGAL IMPLICATIONS OF COMPUTER ABUSE

3.4.2.1 COMPUTERS AND THE LAW

Because of the recent development of computers, our laws seldom expressly touch on problems relating to computers. Furthermore, there are a limited number of reported cases relating to computer abuse (Credo, 1985: South African Institute of Chartered Accountants, 1989).

3.4.2.2 CRIME IN COMMON LAW

Criminal law is that branch of national law which proscribes certain forms of human conduct as crimes and provides for the punishment of these persons who unlawfully and with a guilty mind commit a crime. The sources of criminal law are based on the moral, legal, and social convictions of the community. These convictions and the values which underlie them are expressed in the formal sources of the criminal law, which are legislation, judicial decisions, and authoritative treatises. The purpose of the criminal law is to define socially intolerable conduct, and to hold conduct within limits which are reasonably acceptable from the society's point of view (Burchell, Milton, Burchell, 1982: 1 - 10).

A crime may be defined as conduct which common or statute law prohibits and expressly or compliedly subjects to a punishment which is remissible by the State alone and which the offender cannot lawfully avoid by his own act once he has been convicted (Burchell, Milton, Burchell, 1982: 82 - 92).

3.4.2.3 THE CRIME OF THEFT

Theft consists in an unlawful contrectatio with intent to steal of a thing capable of being stolen. The essential elements are :

- contrectatio, the removal of assumption of control
- unlawful
- intent to steal
  - o the intention must be to deprive the owner or possessor permanently of the full benefits of his ownership
  - o an intention to gain is not necessary
  - o an intention to prejudice the owner or possessor is not required
  - o the accused must not believe that the owner or possessor, acting within his rights, would permit the contrectatio
- property capable of being stolen (Milton, 1990: 602 - 603).

With intent to steal meant that there had to be intent to deprive the owner PERMANENTLY of the WHOLE BENEFIT of his ownership. The meaning has been extended by statute to include unauthorised borrowing, or unauthorised removal of property with the intention of using it without the consent of the owner. However, unauthorised use without physical removal or without removal from the control of the rightful owner would not constitute theft, although it may in some instances represent trespass (Milton, 1990: 606 -626).

Property falls into two groups :

- property absolutely incapable of being stolen, and
- property relatively incapable, either because of its nature or because of the relationship between it and the accused.

Property must have a physical existence and may not be an incorporeal or an idea or a design (Milton, 1990: 627 - 628).

Property incapable of being stolen :

- immovables cannot be stolen, but that part of an immovable which is separated from it can be (for example, trees and crops)
- only corporeal movable things are capable of being stolen
- things which are common to all, but capable of ownership by no one in particular (for example, air in its natural environment)
- things whose ownership vests in the State, for the benefit of all (such as the sea shore)
- abandoned property cannot be stolen

- wild animals cannot be stolen even if they are running on private property unless they have been captured and are still under control
- an owner cannot steal his own property, unless he intends to deprive someone else who has a special interest in it
- property taken by consent (Milton, 1990: 627 -630).

Special categories of property susceptible to theft :

- jointly owned property
- trust money and property
- 'special property or interest' in that property (Milton, 1990: 630 - 642).

This would appear to create a problem in terms of our definition of computer abuse. Theft of a computer, or a magnetic tape or disk, would clearly be a common law crime. But frequently, incorporeals such as software, programs and data have a value as high as the hardware and even sometimes many times greater, yet they are not legally recognised as 'property'. Thus if a program, or confidential data, is physically removed in printed form, the only theft would be theft of the paper on which they appeared. Similarly, if the programs or data were copied onto tapes or disks belonging to the accused or if they were transmitted via a communication line to another site, there would be no theft. In each of these instances the essential element of contrectatio - the intent to steal (that is to permanently deprive the owner of the full benefits of ownership, and property capable of being stolen) - are lacking. However, the situation has been addressed by an amendment to the Copyright Act in 1992 where it can be proven that the firm has copyright on such program. If an employee of a firm diverted the activities of the programming team and, without authority, used them to write programs for his own use, on an outside computer, it seems that this would not constitute theft. Services are not property, and thus cannot be stolen (Milton, 1990).

3.4.2.4 THE CRIME OF MALICIOUS DAMAGE

Malicious injury to property consists in unlawfully and intentionally damaging the property of another. The essential elements are

- property
  - o the thing directly damaged or destroyed must be corporeal. Where physical damage is done, the complainant need not be the owner of the article, all he need have is a special property or interest in it analogous to that which is required in theft. Incorporeal

rights are always invaded when corporeal things are unlawfully damaged. If one owns the property, one may destroy it providing no one else has an interest in it.

- damaging
  - o this incorporates two separate elements : causation and damage
    . For there to be a casual link there must be a duty to act.
    . Damage arises where one meddles with the property in such a way that it is destroyed or lost or permanently damaged, or damaged with the result that it reasonably requires repair, whether this costs the owner money or labour, or in such a way that it its use is permanently or temporarily interfered with, whether this happens because a constituent part is displaced, removed or broken.
- unlawfully, and
  - o the damage may be excused by statute, or by the law of property, or by some defence such as obedience to orders, self defence, or defence of property.
  - o the onus of proving that the accused acted unlawfully remains on the State throughout.
- intent
  - o the intent that is required has two aspects :
    . intention to do the act and cause the damage
    . lack of bona fide belief that the act is lawful
    Even if the person intends to cause the damage and acts unlawfully, he will escape liability if he bona fide believes that he is legally entitled to cause that damage (Milton, 1990: 820 - 828).

From this it would appear that deliberate physical damage to a tape or disk is a crime, whereas the erasure or alteration of magnetic encodings on tapes or disks is not a crime. The destruction of the written copies of programs is a crime only insofar as the destruction of the paper is concerned.

3.4.2.5 THE CRIME OF FRAUD

Fraud consists in unlawfully making, with intent to defraud, a misrepresentation which causes actual prejudice or which is potentially prejudicial to another. The essential elements are :

- unlawfully
- making a misrepresentation, either by words and/or conduct
- intent to defraud which may be actual or legal. This establishes that negligence, no matter how gross, cannot constitute fraud.

- causing (The charge sheet must allege a casual link between the misrepresentation and the prejudice, actual or potential.)
- prejudice (The prejudice need not be proprietary, and the potential prejudice suffices : actual prejudice is not required.) (Milton, 1990: 755 - 778).

Fraud therefore consists of 'deliberate misrepresentation of facts' resulting in loss to the victim. This misrepresentation might be by means of the written or spoken word and would include the falsification of business records (Milton, 1990: 755 - 778).

Probably, the falsification of records by means of suppression or insertion of data into a computer system would constitute fraud. The perpetration of fraud by means of tampering with a program does not in itself constitute 'misrepresentation of facts' and thus might not constitute fraud.

3.4.2.6 CRIME vs DELICT

Delict differs from crime in that it is not public wrong punishable by the State, but a civil wrong, resulting in an actionable right by the party suffering loss, giving rise to a claim for pecuniary compensation for harm suffered, or an interdict to refrain a person from taking a specified action. It is an infringement of another persons interests that is wrongful irrespective of any prior contractual undertaking to refrain from it, though there may also be one. It entitles the injured party to claim compensation in civil proceedings, although criminal proceedings aimed at punishing the wrongdoer may also ensue. A single act may give rise to both delictual and criminal liability. Many crimes may also be delicts, but whereas the crime is punishable by the State, the delict is the basis for civil action by the victim. The existence of concurrent contractual liability is no bar to an action in delict, provided that the requirements of delictual liability are also satisfied. Although one may have an action for breach of contract, i.e. ex-facie the document upon which one sues, the claim is still based on damages which one would have suffered, particularly pecuniary. The action would still be classified as a delict - a wrong committed ex-facie the contract (Boberg, 1989: 1 -5).

Delictual liability is generally based upon fault. There is no warrant, however, for excluding instances of no-fault liability from its ambit, for the essential character of the law of delicit is that it compensates for unlawfully inflicted injury, not that it usually requires fault before doing so. The fault requirement limits delictual liability. The availability of an ordinary civil action for damages is so strong a traditional feature of the law of delicit that a statutory scheme for

providing compensation upon an administrative basis falls outside its scope (Boberg, 1989: 16 - 17).

The basis of delictual liability is the Aquilian action. The Aquilian action is a general action and the two specific groups of actions are :

- o the actio aquilia
- o the actio injuriarum

both of which are Aquilian actions. The lex aquilia provides a general remedy for wrongs to interests of substance, and the actio injururiarum provides a general remedy for wrongs to interests of personality. Both actions require that the defendant should have been at fault. In the actio aquilia action either intention or negligence suffices, but in the actio injuriarum only intention will find liability. A further difference lies in the nature of the harm for which redress is provided. In the actio aquilia action there must be patrimonial loss - pecuniary or financial damage - and damages are awarded to compensate the plaintiff for the loss only, but in the actio injuriarum there is no such requirement, and sentimental damages are awarded as a solatium to assuage the plaintiff's injured feelings. Where both kinds of loss arise from a single act there is no need to bring separate actions, for redress under both heads may be obtained in a single action though intention must be alleged and proved to support a claim for sentimental damages. These two basic types of delict can be summarised as an injury to personality, such as slander or 'crimen injuria', and wrongful action to property or persons (Boberg, 1989: 18).

'Fault' in this context means either 'dolus' (wrongful intent) or 'culpa' (negligence) (Boberg, 1989: 268).

Compensation in the form of a solatium may also be recovered for pain and suffering and other non-patrimonial elements of loss associated with bodily injuries (Boberg, 1989: 18 - 19).

Liability under an Aquilian action is based on

- a wrongful act or omission;
- fault which may be either intentional or negligence;
- causation, which must not be to remote;
- resulting in patrimonial loss;

on the part of the defendant's wrongful and culpable conduct.

Whereas the liability under an actio injuriarum is based on :

- a wrongful act or omission;

- fault must be confined to intention;
- causation, which must not be to remote;
- resulting in an infringement of an interest of personality.

on the part of the defendant's wrongful and culpable conduct (Boberg, 1989: 24 - 25).

Under this section are included :

- the concept of wrongfulness : duty and right
- negligent statements
- pure economic loss caused negligently
- unlawful competition
- trespass
- nervous or emotional shock
- products liability
- abuse of right
- omissions (Boberg, 1989: 24 - 25).

As can be seen, a delict does not necessarily result from any explicit contractual relationship, but may cause, as its reasonable consequence, an injury to another person. In our context 'theft' of confidential data or malicious erasure of programs or files, although possibly not crimes, may be actionable as delicts. Trespass is also a delict; this is defined as wrongful disturbance of another persons possession, in respect of either immovable or moveable property (Boberg, 1989: 170). It is not clear whether this could be extended to cover incorporeals, but it would certainly cover unauthorised use of a computer. However, it should be noted that someone who has permission to use something, but exceeds the scope of his authority, has not committed trespass.

In law, every person is duty bound to refrain from doing that which he knows will involve the violation of another's legal right. Every person is also under a duty to refrain from wilfully perverting the truth with intent to deceive. Thus fraud, in addition to being a crime, is also a delict (Boberg, 1989: 211).

3.4.2.6.1 REMEDIES AND LIMITS THEREON

Civil suit MUST be brought by or on behalf of the aggrieved party, unlike the situation in a crime, where suit is usually brought by the State.

The plaintiff must prove that the act caused pecuniary loss, capable of assessment (Boberg, 1989: 24 - 25). This is not always easy, for example, how does one put a monetary value on the loss occasioned by confidential data falling into the hands of a competitor?

The Court, if the delict is proved, may award monetary damages. It may also order restitution or interdict the perpetrator from continuing to perpetrate the specific misdeeds. Where the case involves property, these damages will be limited to the loss in value of the property, and loss of use thereof or the loss of profits directly resulting from the delict. (Note that if a property needs to be repaired, the cost of such repair is not the amount of damages which will be awarded; it may happen that the damages awarded in respect of loss of value/use may be less than the cost of repair) (Boberg, 1989: 530, 622 - 623).

Clearly, a victim would only consider bringing an action for delict where there is a realistic chance of recovering damages, and costs, from the perpetrator. Where the damage cannot be defined in sums measurable in monetary terms, no case is possible, and where the perpetrator is a man of straw or where he has already spent his gains, a case would be fruitless and would merely result in the added burden of legal costs. However, victims also sue out of spite, for revenge, or to get even with the perpetrator, even when there is no realistic chance of recovering the damages awarded.

3.4.3 STATUTORY LAW

3.4.3.1 THE COMPUTER EVIDENCE ACT NO. 57 OF 1983

This Act relates only to civil cases and not to criminal matters.

In any action involving computer-related crime, there is a necessity to ensure that the computer printouts presented as evidence, are in fact admissible.

This Computer Evidence Act deals specifically with those procedures that are required to be completed in order that an authenticating affidavit can be prepared to accompany a computer print-out presented as evidence in a court case. The Act refers to the authenticating affidavit which must accompany a computer print-out if it is to be admissible as evidence in civil proceedings.

This Act defines a computer as any device capable of :

- o processing data received by it, in terms of supplied mathematical or logical rules
- o storing data before or after such processing
- o producing information from such processing of that data.

The Act defines an authenticated computer print-out as a computer print-out accompanied by an authenticating affidavit.

By an authenticating affidavit is meant the affidavit which authenticates a such computer print-out.

The procedure specified for the preparation of such an authenticating affidavit for a computer printout would require ;

- o identifying the computer printout in question
- o if it is a copy of a computer printout then it must be confirmed as being a true copy of such printout
- o must explain in general terms the extent and sources of the data and the instructions supplied to the computer to produce this printout, as well as the purpose and effect of the processing by that computer
- o certify that the computer was correctly supplied with data and instructions which were appropriate and adequate to produce the required printout.

The person (defined as the deponent) involved must certify that there is no reason to doubt or suspect the truth or reliability of the information recorded on the printout.

This person to certify that such information as given being to the best of that persons knowledge and belief.

The person signing this affidavit must be qualified to do so in terms of his knowledge on the subject as well as his examination of the print-out.

He must verify all records and facts, or state the extent to which he was unable to do so.

Printouts prepared by a public institution in the normal course of their activities do not require to be certified by the deponent.

The Act states that such authenticated computer print-outs shall be admissible as evidence of a fact recorded in it, when direct oral evidence would be admissible.

The evidential weight of such authenticated computer print-outs shall have that evidential weight which the court in the circumstances attaches to it.

The Act provides for penalties for false or misleading information in such an affidavit. Provision is made for a fine not exceeding R 4 000,00, or imprisonment not exceeding two years, or both.

A potential problem may be that few deponents to the authenticating affidavit may, in reality, have adequate knowledge of the complete functioning of that particular computer system in question, and it may also be difficult to detect errors in computer operation when there has been a malfunction caused by a variation in current or an unsuitable environment.

3.4.3.2 THE COPYRIGHT ACT NO. 98 OF 1978

The Copyright Act was silent on the subject of computers until July 1992.

Previously the particular wording of the Act, together with the accumulated case history in the area of copyright, left room for debate as to what the attitude of the Courts might be. This was resolved, after a fashion, in the 1981 Northern Office Micro Computers case (Northern Office Micro Computers (Pty) Ltd and Others v Rosenstein, 1981). Here the judge held the view that computer programs are in fact eligible for copyright.

Justice Marais, in the Northern Office Micro Computer case, ruled that a computer program was in fact eligible for copyright as a literary work, that a computer printout of the program code satisfies the requirement that it be reduced to written or other material form, and further that computer instructions on floppy disks may perhaps meet the requirements of having been 'recorded'.

The Copyright Act Amendment Act No. 125 of 1992 specifically made provision for computer programs to be eligible for copyright as a separate category of work. This amendment came into effect on 10 July 1992.

Section 2(1) lists those categories of work which, if ORIGINAL, shall be eligible for copyright :

a) literary works
b) musical works
c) artistic works
d) cinematograph films
e) sound recordings
f) broadcasts
g) programme-carrying signals
h) published editions
i) computer programs.

The term 'works' is defined in Section 1. The definition of 'literary work' includes, irrespective of literary quality and in whatever mode or form expressed:

a) novels, stories, and political works
b) dramatic works, stage directions, cinematograph film scenarios and broadcasting scripts
c) textbooks, treatises, histories, biographies, essays and articles
d) encyclopaedias and dictionaries
e) letters, reports and memoranda
f) lectures, addresses and sermons; and
g) written tables and compilations

but shall not include a computer program.

The Act defines a 'computer program' as meaning a set of instructions, fixed or stored in any manner and which, when used directly or indirectly in a computer, directs its operation to bring about a result.

Nature of the copyright in computer programs

Section 11B states that copyright in a computer program vests the exclusive right to do or authorise the doing of any of the following acts in the Republic :

a) reproducing the computer program in any manner or form
b) publishing the computer program if it was hitherto unpublished
c) reproducing or publishing an adaptation of the program
d) making an adaptation of the computer program
e) letting, or offering or exposing for hire by way of trade, directly or indirectly, a copy of the computer program.

Section 19B provides that the copyright in a computer program shall not be infringed by a person who is in lawful possession of that computer program, or an authorised copy thereof if :

a) copies are made to the extent reasonably necessary for back-up purposes
b) a copy so made is intended exclusively for personal or private purposes, and
c) such copy is destroyed when the possession of the computer program in question, or authorised copy thereof, ceases to be lawful.

Duration of the Copyright

Section 3 (2) provides that the term of copyright in respect of computer programs will be fifty years from the end of the year in which the work is lawfully made available to the public, or failing this, fifty years from the end of the year in which the work is made.

Moral Right

Section 20 of the Copyright Act provides that notwithstanding the transfer of the copyright in a computer program, the author shall have the right to claim authorship in the work and to object to any distortion, mutilation or other modification of the work where such action is or would be prejudicial to the honour or reputation of the author.

Ownership of the copyright

Section 21 (c) states that where the author is employed in terms of a contract of service or apprenticeship, the employer shall own the copyright, otherwise it is the author who owns the copyright.

Copyright Protection - Unauthorised Reproduction

Copyright in an eligible work under the Copyright Act does not confer absolute protection for the work but only protection against copying.

Marking

In terms of Section 26 of the Copyright Act, an advantage in making a computer program with the name of the author is that such person shall, unless the contrary is proved, be presumed to be the author of the work.

Infringement of Copyright

Section 23 defines infringement of copyright as follows:

"1. Copyright shall be infringed by any person, not being the owner of the copyright, who, without the licence of such owner, does or causes any other person to do, in the Republic, any act which the owner has the exclusive rights to do or to authorise.

2. Without derogating from the generality of subsection (1), copyright shall be infringed by any person who, without the licence of the owner of the copyright and at a time when copyright subsists in a work -

a) imports an article into the Republic for a purpose other than for his private and domestic use;

b) sells, lets, or by the way of trade offers or exposes for sale or hire in the Republic any article; or

c) distributes in the Republic any article for the purposes of trade, or for any other purpose, to such an extent that the owner of the copyright in question is prejudicially affected; d) acquires an article relating to a computer program in the Republic

if to his knowledge the making of that article constituted an infringement of that copyright or would have constituted such an infringement if the article had been made in the Republic.".

Judicial proceedings can be instituted to obtain relief in respect of infringement of copyright.

Section 24 provides that infringements of copyright shall be actionable at the suit of the owner of the copyright. Such owner can obtain relief by way of damages, interdict, delivery of the infringing copies used or intended to be used. This section proceeds to define how damages can be determined.

The onus of proof in judicial proceedings is outlined in Section 26. The person presumed to be the author:

- in a work of joint authorship, is each author
- where the author is anonymous or pseudonymous and is commonly known, then by that name, otherwise

if the name of the publisher appears on the program and it is still within the fifty year period, then it is the publisher.

Where the author is dead, then that program shall be presumed to be an original work, unless the contrary can be proved.

Penalties for infringement

The law deals firmly with persons infringing copyright. A person convicted of an offence shall be liable, in the case of a first conviction, to a fine not exceeding R 5 000 or a jail sentence not exceeding three years, or both, for each article to which the offence relates. A second offender is liable to a fine of up to R10 000 or a jail sentence not exceeding five years, or both, per article to which the offence relates.

In addition, the Act gives the copyright owner various civil rights, such as relief by interdict, monetary damages, and recovery of costs.

SUMMARY

This Act offers to the owners of original computer programs protection from unauthorised copying and use of their programs.

3.4.3.3 THE CORRUPTION ACT NO. 94 OF 1992

The Prevention of Corruption Act No. 6 of 1958 was repealed in 1992 and replaced by the Corruption Act No. 94. This Act came into effect on 3 July 1992.
This Act does not expressly cover computers, programs or data, but nevertheless could include many of these in its ambit.

It covers a wide range of persons in a position of implied or express trust, including employees, agents, trustees, etc.

It prohibits the acceptance, agreement to accept or attempt to accept any gift, consideration, inducement or reward for dealing improperly with the affairs of the principal. It similarly prohibits the giving or offering of any such gift, consideration, inducement or reward.

Section 1 states that any person shall be guilty of an offence :

- who corruptly gives or offers to give any benefit of whatever nature which is not legally due to any person, defined as upon whom :
  - any power has been conferred
  - charged with any duty by virtue of any employment
  - holding of any office
  - any relationship of agency
  - any relationship by law
  - anyone else
    - with the intention to influence such person to commit or omit to do any act in relation to such power or duty
    - inducing such person to :
      - act in excess of such powers, or
      - to neglect such duty

      in terms of their assigned powers or duties for reward. It is interesting to note that the reference to "anyone else" does not apply to this paragraph.
- such person is defined as upon whom :
  - any power has been conferred
  - charged with any duty by virtue of any employment
  - holding of any office
  - any relationship of agency
  - any relationship by law

  who corruptly receives, obtains, agrees to receive, or attempts to obtain any benefit of whatever nature which is not legally due from any person, either for himself or anyone else, with the intention :
  - that he should commit or omit to do any act in relation to such power or duty
  - to be rewarded for having committed or omitted to do any act which constitutes an excess of such powers, or neglect of such duties as assigned above

  whether the giver or offeror of the benefit has the intention to reward such person, or not.

Section 3 states that the penalty for committing an offence shall be any penalty within the punitive jurisdiction of the court concerned. Court is defined as any magistrate's or regional court and any provincial or local division of the Supreme Court.

This is a very far-reaching Act. It seems to cover any form of bribery, 'kickback', etc. It could also cover unauthorised personal use of computers, programs, data and people if a false

accounting of the usage of these resources is given to the principal. It is also probable that most types of fraud might be covered insofar as they would usually, but not necessarily, include the giving of a false receipt, account or document.

3.4.3.4 THE PATENTS ACT NO. 57 OF 1978

Section 25 (1) states that a patent may be granted for any new invention which involves an inventive step and which is capable of being used or applied in trade, industry or agriculture.

Section 25 (2) states that a program for a computer, or the presentation of information, is not regarded as an invention for the purposes of the Patents Act.

3.4.3.5 SUMMARY OF LEGISLATION REFERRING TO THE USE OF A COMPUTER

To complete this study on South African legislation, the following summary has been prepared of those Acts that have a reference to a computer. An analysis of the JUTASTAT service revealed that there are no acts referring to computer crime.

Agricultural Research Act No. 86 of 1990

Section 4 Functions, powers and duties of Agricultural Research Council.

(o) (i) May produce and sell reports and computer programmes.

Bills of Exchange Act 34 of 1964

Section 95 Signature

(2) The name of an authorised signatory printed on a post office warrant-voucher or cheque will be accepted as having been signed by such person.

Basic Conditions of Employment Act 3 of 1983

Section 32 Evidence.

(4) Any statement or entry contained in any book or document kept by an employer obtained by the use of a computer shall be admissible as evidence.

Criminal Procedures Act 51 of 1977

Chapter 24 Evidence.

Section 236 Proof of entries in accounting records and documentation.

(5) and 236A (6)

A document can be prepared by and maintained by a computer.

Deeds Registries Act 47 of 1937

Section 3 Duties of registrar.

(1) (y) Registers may be kept on a computer.

Defence Act 44 of 1957

Section 66B Ballot.

(6) An electronic computer can be used to take a ballot.

Diamonds Act 56 of 1986

Section (1) Definitions

"Register" includes a computer print-out.

Documentary Evidence from Countries in Africa Act 62 of 1993

Section 1 Definitions

"Documents" include computer print-outs. Information can be recorded or stored in a computer.

Drugs and Drug Trafficking Act 140 of 1992

Section 1 Definitions

"Record" includes any information contained in a computer or reproduced by a computer print-out.

Energy Act 42 of 1987

Section 1 Definitions

"Record" includes a computer print-out.

Financial Markets Control Act 55 of 1989

Section 1 Definitions

Computer printout accepted as a "record".

Geoscience Act 100 of 1993

Section 5 Functions of Council.

(1) (g) The council may produce and sell computer programs in the course of its research.

Machinery and Occupational Safety Act 6 of 1983

Section 31 Proof of certain facts.

(3) A computer can be used to prepare the documents to be kept by an employer.

Minerals Act 50 of 1991

Section 1 Definitions

"Record" includes information contained in or on a computer print-out, tape, disc or any other computer medium.

Section 53 Proof of certain facts.

(1) Information contained in a computer storage medium is admissible as evidence.

Mineral Technology Act 30 of 1989

Section (4) Functions, powers and duties of Mintek.

(1) (d) (i) Mintek may produce and sell computer programmes as an end product of its research, development and technology transfer.

Natural Scientific Professions Act 106 of 1993

Section 3 Constitution of council and appointment of members.

(1) (vii) One person will be nominated to the council by the South African Mathematical Society after consultation with the South African Institute of Computer Scientists.

Nuclear Energy Act 131 of 1993

Section 6 Functions of AEC.

(2) (i) The Atomic Energy Corporation may purchase, produce and sell computer programs in order to create and utilise viable business opportunities in commerce and industry.

Post Office Act 44 of 1958

Section 2B (1) (j) General powers of the postmaster-general.

May render computer services to the medical aid established for the employees of the department.

Public Service Act 111 of 1984

Section 3 Commission for administration.

(f) (iv) Can utilise a computer to promote efficiency and economies.

Public Service Labour Relations Act 1994

Section 20 Essential services.

(1) (e) Key-point computer services are defined as essential services for a community.

Road Traffic Act 29 of 1989.

Section 144 Duplicate of document or token.

(1) (a) A computer can be used to produce a certificate, license, token, or other document.

Regulations in terms of the Deeds Registry Act 47 of 1993

Schedule of fees Section 4

(a) A fee may be charged for each enquiry requiring a computer print-out.

(f) A fee may be charged where an enquiry requires an off-line computer print-out.

Sectional Titles Act 95 of 1986

Section 12 Registration of sectional plans and opening of sectional title register.

(1) (c) The register can be kept on a computer.

Short Process and Mediation in Certain Civil Cases Act 103 of 1991

Section 3 Mediation proceedings.

(iii) (bb) Information can be contained in computer printouts, tapes or discs or any other computer storage media.

Space Act 84 of 1993

Section 1 Definitions

"Technological assets" includes computer software.

Stamp Duties Act 77 of 1968

Section 24 Policies of insurance.

(10) (a) The insurer can use a computer to calculate the duty payable on a policy of insurance.

(c) A computer can be used to record the value of the stamp duty payable on a policy.

(10) Provision is made to use a computer process to print the stamp required for that policy.

(11) (a) A computer can be used to record the total amount of stamp duty to be paid to the receiver of revenue.

Statistics Act 66 of 1976

Section 1 Definitions

A computer print-out is accepted as a "document".

Value Added Tax Act 89 of 1991

Section 55 Records

(1) The books of account required to be kept by a vendor can be kept on a computer. The required records can be printed out from this computer.

(4) The Commissioner can authorise the retention of computer tape records of documents in lieu of the originals.

3.4.4 CONCLUDING REMARKS

No where in our legal structure is the applicability to computer-related criminal activities specifically defined other than in the Copyright Act. The balance of probability is that the law can be stretched to fit computer technology. At other times the balance of probability is that the law does NOT encompass computer technology, as with the common law of malicious damage. The Computer Evidence Act is valuable legislation, in that it details the process to be followed for authenticating computer printouts for presentation as evidence in civil cases.

CHAPTER 4

CONTROL METHODOLOGY TO PREVENT AND DETECT COMPUTER-RELATED CRIME

4.1 INTRODUCTION

In the broadest sense, every manager is responsible for overseeing controls to ensure that the organisation's assets are protected. Information is a critical asset, an organisation's lifeblood. The computer systems program is the heart that pumps information throughout the organisation. The organisation must be able to rely on these systems for accurate and timely information - the basis for all business decisions. Over the years, computer usage has expanded greatly, and the technologies that deliver this increased computing power have grown more complex. The trend to on-line terminal access and a diverse user community means that better methods of protecting these systems are needed.

This chapter presents a proposed model to manage and control computer- related crime. The basic principles of internal control apply equally to the Information Services (IS) department as they do to all other departments within that organisation.

4.2 THE CONTROL METHODOLOGY

Controls over computer-based accounting systems are usually considered under two main headings, namely application controls and general controls.

Application controls cover the transactions and standing data used by each application and are, therefore, specific to each application. The objectives of application controls are to ensure the completeness and accuracy of the accounting records and the validity of the entries therein resulting from both computer and manual processing. Application controls may be performed manually, such as the checking of batch total reconciliation's, or by computer, such as input edit checks included in computer programs.

General controls cover the environment within which applications are developed, maintained and operated and within which application controls operate. The objectives of general controls are to ensure the integrity of application development and implementation, program and data files, and computer operations. General controls may be performed manually, such as restricted physical access to data files, or by computer, such as password protection for program files.

Although there will be general controls common to all applications, some applications which are deemed sensitive by the enterprise may be subjected to additional general controls.

The following categories of control need to be addressed ;

- deterrent prior to input
- preventive after input and
- corrective before processing
- detective during processing
- recovery after processing
- report upon detection of an unwanted event

Within an organisation the following major control categories can be identified and will be discussed :

- organisation controls
- access controls
- development & maintenance controls
- operations controls
- physical security and recovery controls

Each control category will be dealt with in turn. Proposed objectives have been identified for each category. These objectives are followed by the relevant control procedures which could be considered appropriate. This control methodology has been developed for the IS department, but they can be applied equally to all other user departments as internal controls apply equally through out the organisation. These objectives and controls are not meant to be exhaustive but to serve as a framework on which an organisation can build.

Each control category together with its relevant objectives have been intentionally presented in a brief point format, similar to that of an audit manual, for the sake of brevity and in order that this material might form the basis on which an organisation might develop their own control methodology.

The following reference material was used in the preparation of this control methodology : Auditing Practices Committee of The Institute of Chartered Accountants of England and Wales, 1984; Australian Society of Accountants, 1984; New Zealand Society of Accountants, 1986; Gallegos, Richardson & Borthick, 1987; Perry & Kuong, 1987; South African Institute of Chartered Accountants, 1989; International Federation of Accountants (ISA15), 1991; International Federation of Accountants, 1991.

4.3 ORGANISATIONAL CONTROLS

4.3.1 GENERAL CONTROLS

4.3.1.1 INFORMATION SERVICES PRACTICES SATISFY AND ARE CONSISTENT WITH CORPORATE OBJECTIVES

A formal line of communication exists between management, users and Information Services (IS).

Senior executives from all parts of the organisation participate in IS through steering committees.

Senior management from all areas of the organisation are informed of control requirements and potential risks.

Steering committees consist of technically competent personnel.

A steering committee is responsible for the allocation of departmental resources and the resolution of conflicting demands.

Personnel policies are adhered to with regard to :

- staff evaluation
- training
- remuneration
- hiring and termination.

Information Services (IS) management should :

- control all aspects of IS activities
- standards, conventions and procedures clearly defined in writing
- monitoring and review of activities.

4.3.1.2 INFORMATION SERVICES DEPARTMENT RESPONDS TO AND PARTICIPATES EFFECTIVELY IN THE CHANGING BUSINESS ENVIRONMENT THROUGH PLANNING

There should be formal plans for the future which are approved (by the steering committee or board) and properly scheduled.

- expected growth rates for transactions and file sizes
- proposed major amendments and new system developments
- acquisition of new equipment and operating software
- changes to existing equipment and operating software
- changes in market trends and competition.

Income and expenditure should be controlled :

- preparation of budgets and reporting thereon
- recording of time spent and equipment usage
- billings for all IS services provided.

There should be liaison with user departments :

- notification and recording of requests and complaints
- follow-up of outstanding items
- regular meetings and minutes thereof
- user liaison functional position.

IS management should keep up to date with technological developments.

4.3.1.3 SENIOR MANAGEMENT EXERCISES SUITABLE CONTROL OVER METHODS AND PERFORMANCE STANDARDS

Senior executives from all parts of the organisation participate in IS through steering committees.

Top management should state a general operating principle or rule which governs the authority granted IS management and the responsibilities of user departments. IS documentation should be reviewed to assess compliance with top management's policy directives.

4.3.2 SEPARATION OF FUNCTIONS

4.3.2.1 IS INFORMATION SERVICES ADEQUATELY SEPARATED FROM USERS ?

The data processing manager reports to a director or other senior official who is independent of user departments.

The organisation chart should identify the relationship between IS and users.

Users should be actively involved in control procedures over their own applications (input and output).

IS personnel are prohibited from :

- initiating or authorising transactions
- making master file changes
- having custody of assets
- and from other non-IS responsibilities or duties.

Data control activities within IS are independent of user departments and other functions.

Staff responsible for input preparation should be separate from non- compatible functions.

- no custody of related assets
- no access to, or knowledge of, related programs
- no access to computer.

4.3.2.2 THE CONCENTRATION OF FUNCTIONS WITHIN INFORMATION SERVICES IS ADEQUATELY CONTROLLED

The organisation chart indicates the functions and job titles of all key personnel and there are formal job descriptions that define individual responsibilities.

The IS manager is satisfied that all functions are adequately staffed by competent personnel and that vacancies arising from staff turnover are both short lived and minimised.

The following functions should be separated and reported separately to the IS manager who should not be actively involved in any of the functions detailed below :

- systems analysis
- systems design
- programming
- computer operations
- data control
    - o data capture
    - o library control

Access to input (source documents) and output reports is limited to data control.

Access to data files, programs and supporting documentation is limited to the librarian who functions independently of programming and operating. Two exceptions would be :

- operations. When files have been released for authorised runs.
- programmers. When authorised program changes are being made under controlled conditions.

Access to the computer room should be limited to operating personnel during normal shifts. In certain instances however, over weekends for example, programmers might require access. This should be recorded and should only include program testing (non-production runs) and debugging.

4.3.3 PERSONNEL POLICIES

4.3.3.1 THE INFORMATION SERVICES DEPARTMENT IS ADEQUATELY STAFFED WITH COMPETENT PERSONNEL AND NOT UNDULY DEPENDENT ON A FEW KEY INDIVIDUALS

The following may affect the assessment of the competence of staff :

- reliance on vendor or software house
- staff turnover rates
- staff compensation and benefits

- reliance on key personnel
- recent or planned re-organisation.

Adequate liaison should be maintained with staff :

- regular reviews of work done
- discussions on plans and programs
- regular meetings on problems, status of work, training and other items of concern
- copies of relevant job descriptions, policies, standards and conventions given to each staff member
- vacation policy must exist requiring employees to take annual scheduled vacations
- blanket fidelity bond coverage should be maintained for all employees

4.3.3.2 EMPLOYMENT PROCEDURES CONSIDER PERFORMANCE AND SECURITY HISTORY AND PROVIDE ADEQUATE INITIATION TRAINING

All employees must receive orientation, ongoing and periodic evaluations in security responsibilities.

Documented background verifications must be performed on all prospective employees to include :

- verification procedures with former employees
- job history and reasons for leaving.

Employees should sign statements of responsibility for security matters.

4.3.3.3 TERMINATION POLICIES PROVIDE FOR INSTANT DISMISSAL AND REMOVAL OF ACCESS PRIVILEGES.

A written termination policy must exist and provide for :

- exit interview
- immediate dismissal if employee is assigned sensitive duties
- immediate retrieval of all company materials
- final pay
- notification of termination to company employees
- change of locks or combinations.

4.3.3.4 ADEQUATE TRAINING IS PROVIDED TO ENSURE COMPETENT STAFF

A formal IS training program should address most of the following points :

- on-the-job training
- self study (programmed instruction)
- adequate cross training (vendor or internal)
- training for user of data processing services
- training in both IS and industries serviced by the company
- specific programs of training for each employee
- a training schedule
- evaluation of training effectiveness
- accurate training records
- skills inventory as a basis for planning training.

4.4 ACCESS CONTROLS

4.4.1 TO ENSURE THAT PHYSICAL AND LOGICAL ACCESS TO DATA, PROGRAMS, EQUIPMENT AND DOCUMENTATION IS LIMITED TO AUTHORISED PERSONNEL

Physical access to the computer room is restricted to those authorised employees engaged in direct support of operations:

- the computer room design and the location of the equipment, physically segregate the operations function from the control function which is , in turn, isolated from other sections and departments.
- security locks, combinations and/or alarms control entrance doors to the scheduling area and to the computer room on all shifts and after hours.
- access is limited to screened computer operators and supervisors who accompany at all times any unauthorised employees and external users or personnel needed in the computer room.

Written operational procedures during program testing and system software (utilities) control the access of the programmers to hardware, data, and programs:

- except for emergency debugging under specific management authority, programmers are denied access to the computer room during production runs.

- live master and transaction data files are password protected or physically removed from the computer room during program testing for which only authorised copies or test versions of data files may be used.
- tape and diskette versions of production programs are physically removed, or software libraries are divided into testing and production sections for which separate access techniques and passwords are respectively available to programmers and operators.
- testing libraries are maintained in source code only and written standards control their approval, cataloguing and compilation in object format, for execution.

Strict authorisation and identification procedures prevent data files and programs being accessed by unauthorised personnel via terminal:

- both terminals and the rooms in which they are located, are locked when not in use and they are regularly inspected to verify adequacy of physical access restrictions.
- terminals are hard wired for functional capability or otherwise authorised by means of terminal identification tables that are controlled, and periodically changed, by management through system software.
- master terminal capability is closely controlled by management and requires written authorisation, while terminals for program development and testing, are locked out from application transaction initiation, live data files and approved programs. (Applicable to remote job sites).
- authorised users are validated by user identification codes which are periodically changed to preserve confidentiality and currency. This procedure should be reviewed for compliance by the computer or management. This should include terminal identification codes.
- access to program and data files, especially on-line files, is protected and user functions (i.e. program execution) are restricted by passwords, the table of which is regularly reviewed and updated under management control. Off-line files should be under the control of the librarian.
- encrypt on-line system password files and compare password in encrypted form in privileged mode computer operation to prevent technical compromise.
- security violations concerning signing-on or program/data file access attempts, are all detected and reported on the main operating console, while the offending terminal is switched out.
- call back to sender before access to system.
- until acceptable output is received, users maintain control over data transmitted with the help of audit trails, log files and recovery procedures.

Regular management review of console logs to ensure that only authorised jobs have been run.

Job accounting system to control the usage of the machine.

Sensitive programs/files not in use should be stored off-line in a restricted library.

No access whatsoever to system or application software by operators.

There should be no change in controls for files and programs used in test runs.

The librarian function is independent of operations and maintenance/systems development:

- there are written policies governing the organisation, handling, retention and control of magnetic disc and tape files, related and other privileged information.
- maintenance and control of the library is divided into an operations section (master and intermediate transaction data files, production program schedules and job control schedules) and a systems/program section (system software and source program securities, related documentation not being currently amended and documentation securities).

Proper barriers and locks respectively restrict access to the library area during and after normal hours:

- the design and location of the library and the construction of storage facilities adequately protect the contents from possible destructive hazards elsewhere in the IS complex.
- computer operators, other operations staff, analysts and programmers are specifically prohibited from entering the library at all times except under management supervision.

Only authorised individuals may obtain files or documentation from the library and a log is maintained to control the issue and required return of appropriate items:

- operators and programmers/analysts are prohibited from receiving application data files from the library unless authorised by management or, in the case of operators, if supervised by scheduling.
- a file history system is used to record physical reel location in the library and elsewhere; recording error, cleaning and refurbishing histories; age and status (scratch/master); and final scrambling on recruitment of files.

- software documentation, file layouts, program assembly and customer listings etc., are inaccessible to operators and only available to maintenance programmers/analysts under controlled conditions.
- the user and location of each documentation element is logged in a register which is maintained as a permanent record.

4.4.2 TO PREVENT THE INTRODUCTION OF UNAUTHORISED TRANSACTIONS

Ensure that adequate batching procedures are followed.

Review of all input documented by data control to ensure that they have been adequately authorised prior to processing.

Batch control totals to ensure that no unauthorised transactions have been added to batches.

Use of run to run control totals, over record counts for example, which should be checked by a person not responsible for the input of transaction.

Review by users of output to ensure all transactions processed were initiated by them (i.e. daily edit lists/transaction listings).

Sequence checking of pre-numbered input documents and batches.

Management review of reports listing master file additions, deletions and amendments.

In an on-line environment the authorities required for transactions are controlled by physical and programmed access controls and accordingly the majority of the controls applicable to the above objective have been included under access controls.

4.4.3 TO RESTRICT THE EXPOSURE OF SENSITIVE OR CONFIDENTIAL DATA AND OUTPUT

An independent control group should be responsible for the distribution of all output to provide an element of security for confidential data and to help prevent errors or irregularities that might result from the diversion of output.

Output awaiting distribution should be produced and signed for by the recipients.

The number of report copies is limited to the number of authorised recipients.

The reports are distributed in secure containers.

Sensitive on-line enquiries are controlled by multi-level passwords.

Where output is being transmitted to remote locations it should be encrypted.

The printing of confidential files should be password protected.

4.4.4 TO ENSURE THAT ALL PROCESSING IS AUTHORISED

Records of jobs run should be checked against records of runs authorised:

- procedures documented and distributed to staff
- signed request forms for special or infrequent reports
- computer recording of all jobs run
- operations log
- checked to authorised schedule and request forms
- independent checks
- operators should be instructed to stick to the operations schedule unless otherwise advised by the operations supervisor.

Terminal use should be restricted to certain types of transactions or activities. For example:

- operational programs cannot be initiated from terminals outside the computer room.

The use of utility programs, particularly those with the capability of modifying data files, should be restricted and monitored.

Sensitive programs stored in on-line libraries are protected by passwords. When not in use, these should be stored in a restricted library.

4.4.5 TO ENSURE THAT THE ACCURACY AND SECURITY OF DATA TRANSMITTED IS MAINTAINED

Procedures should protect data transmitted by line:

- data scrambled or transmitted cryptographically
- call back to sender before access to system
- keeping codes, telephone numbers etc. confidential
- edits and validations performed at receiving location
- response to sender on receipt of data or detection of error
- ability to reconstruct data lost or corrupted in transmission, this should include restart procedures in the event of the line going down during transmission
- balancing procedures
- control totals for data entered by on-line systems should be auto-matically accumulated at each terminal. This information should be verified to input accepted by the computer.

Alternative procedures should be established for when line is "down" or terminal is inoperative:

- procedures documented and given to staff
- identification of data not yet transmitted
- short periods of breakdown
- manual checks in place of those done by computer, terminal etc.
- notification of problem to person concerned
- alternative means of data capture and transmission
- balancing procedures
- periodic tests of procedures

Procedures should protect data transported physically (e.g. on floppy disc or tape):

- procedures documented and distributed to staff
- transmittal slip or other record of data transported
- identification of data and individual floppy disks, tapes, etc.
- use of locked case and control over keys
- evidence of receipt
- balancing procedures
- ability to reconstruct data

4.5. DEVELOPMENT AND MAINTENANCE CONTROLS

4.5.1 TO DEVELOP A COMPUTER SYSTEM ONLY IF IT WILL PRODUCE GREATER BENEFITS THAN OTHER ALTERNATIVES

Economic desirability of new application or amendment should be evaluated prior to development work starting:

- procedures documented
- feasibility studies are performed by the company personnel with appropriate experience, independent consultants or equipment manufacturers
- consideration of alternatives
- users participate in the investigations which include cost-benefit and return on investment analyses, and reviews by accounting personnel concerning the accuracy and validity of financial calculations
- senior management is responsible for approving the conclusions of the study group and for authorising new projects for each of which a project development committee is set up
- retention of documentation
- project committees, comprising users and IS technicians, establish target dates for each key development point, the actual progress of which is monitored and approved by the steering committee

New application or amendment should conform to long-term plans:

- acquisition and utilisation of equipment
- agreed upon priorities
- independent review against long-term plans

4.5.2 TO ENSURE THAT CHANGES TO EXISTING INFORMATION SYSTEMS ARE AUTHORISED, AND ARE IMPLEMENTED IN A CONTROLLED FASHION, AND THAT THEY DO NOT IMPAIR PREVIOUSLY TESTED PROCESSING ROUTINES OR CONTROLS

In accordance with written policies and procedures for maintaining existing systems, authorised amendment request forms are required before program changes are initiated.

Request forms detail descriptions of, and reasons for changes which must be approved in writing by senior officials in user departments.

Request forms, authorised in writing by the IS manager, are sequentially numbered and centrally controlled by a computerised (manual) register into which requests are logged together with planned deadlines for key development points and subsequent achievement dates.

Program revisions are formally tested and approved before being placed into production.

Amendments are approved by a senior official experienced in the coding language but independent of the programming work.

Test results are reviewed by users and supervisory personnel to confirm the proper operation of the program and compatibility with other programs in the system.

Program and related documentation is properly updated for completed changes.

All program changes are dated and documented in a manner which provides an accurate, chronological history of the systems.

A check list on the request form is signed off by the appropriate reviewer to signify approval of changes made to run manuals and operation instructions; user manuals; systems and other program documentation.

Preventative and detective measures preclude unauthorised changes being made to production programs.

Final user and IS manager acceptance, recorded on the request form, is required before an independent official compiles the object code into production.

Security copies are made and the central register is updated automatically or by reference to appropriate operations logs and job accounting reports.

Emergency program changes and temporary amendments are strictly controlled and discouraged as far as possible.

Authority is required from a senior person in the IS department before programmers may assist operators to respond to technical problems or to request forms for one-off requests, changes to parameters etc.

Program status reviews by the IS manager initiate procedures which control the proper approval of changes, testing and documentation updates.

4.5.3 TO ENSURE THAT DOCUMENTATION STANDARDS AND PROCEDURES ADEQUATELY CONTROL SYSTEMS DEVELOPMENT

- Documentation standards should be established, documented and complied with, by members of staff:
  - o system specifications and information
  - o project control
  - o program documentation
  - o run manuals
  - o jcb control language
  - o user manuals
  - o data capture instructions

- All documentation produced should be reviewed and approved:
  - o use of a check list
  - o reviewed for completeness and adequacy
  - o evidence of approval
  - o checks that copies are made and distributed
  - o independent test checks

- All users of the systems such as user departments, systems analysts/- programmers and the IS manager, are responsible for developing the documentation, the location of, and access to, which is controlled by librarian procedures.

Standard procedures and conventions should be established for systems design and programming:

- standards and conventions documented and given to staff
- reviewed to ensure adherence

4.5.4 TO CONTROL NEW SYSTEMS DEVELOPMENT VIA A STRUCTURED METHODOLOGY TO ENSURE THAT USERS NEEDS ARE MET

All aspects of projects should be scheduled and monitored:

- procedures documented and distributed
- project committees
- establishment of target dates and budgets
- recording of time and costs
- regular preparation of progress reports and review against plan

Management, user departments, internal and external auditors should participate in the development process:

- compliance with required accounting principles and procedures
- content and format of reports
- desirable controls
- preparation and review of test data
- conversion
- post implementation review

Review and approval should be required at each major phase:

- adequate user and IS controls are incorporated into the application which must be signed off by both users and the IS manager, or a more senior official, when the design affects systems in other departments.
- the most commonly used programming language is named in the compre-hensive systems specifications which are reviewed for adherence to company policies and practices and, by the auditors for the adequacy of internal controls, before being approved by management.
- procedures documented and distributed.
- formalised record.
- approval by management and user department.
- retention of documentation.

Systems and programs must be sufficiently tested to ensure reliability in accordance with original specifications:

- testing procedures require the participation of users and their formal approval of test results before written acceptance of the program is received from management/the steering committee, and authority granted to commence live, parallel runs.

- all major conditions in the program are tested and debugged, and link testing of modules making up the program suite is also performed.
- a combination of techniques available to test the limits of the program logic is used, including test data partly compiled by users; controlled copies of live data; erroneous data; and a visual check of the program flowchart.
- tests include all phases of the system such as the use of operating instructions by operators (without programmer assistance) and the clerical and control procedures used by data control, source and user departments.
- procedures documented and given to staff.
- tests independent of programmer.
- data representative of actual conditions.
- all possible errors and conditions.
- review of results.
- retention of test data and results.

4.5.5 TO ENSURE THAT CONVERSION TO NEW SYSTEMS ARE AUTHORISED, COMPLETE AND ACCURATE

The conversion of data and initial processing should be effectively controlled:

- there are written plans and standard procedures for controlling initial file creation; conversion of basic data; and parallel runs. The plan covers the collection and verification of financial data, its conversion into machine readable form, and the logical or compatible relationship of transactions, and other data, within the records.
- converted data is tested with the new program, and master file record changes (using fix utilities or input documents) are controlled between initial conversion and final testing prior to production.
- cut-off procedures.
- the contents of new master files are thoroughly checked against input take on sheets and balanced to original records, to establish accuracy, completeness and no duplication.
- to totally test the program, pilot/parallel runs ought to last at least one full processing cycle but they are otherwise confined to their limited test period in order to reinforce commitment to the new system.

Development and maintenance of system software is controlled by the same standards as application programs but procedures differ slightly:

- initial file creation and data conversion is not a pertinent phase in the development or acquisition of system software and may be supplanted by a review of a data base management system in the appropriate environment.
- as the IS department is itself the main user of system software, participation and approval at key development point by the traditional user department is replaced by IS management.
- written standards relating to systems documentation cover problem definition, system description and flowcharts; list of required programs; description and examples of source documents and output reports; processing details and I/O controls; conversion procedures and schedules; user department instructions.
- implementation procedures are concluded with training or retraining schemes for appropriate personnel, and the collation of comprehensive documentation.
- both user department and IS personnel receive adequate training on procedures, including the use of manuals and system control points, that need to be monitored on a continual basis.
- retention of documentation.
- independent checks.

4.6. OPERATIONS CONTROLS

4.6.1 INPUT SUBMISSION

4.6.1.1 TO ENSURE THAT DATA IS COMPLETE, ACCURATE AND AUTHORISED WHEN RECEIVED FOR PROCESSING

There should be adequate procedures for the preparation and submission of data to be processed:

- procedures documented and distributed to all people concerned
- use of turn around and specially designed, precoded documents where possible
- sequence checks
- batching procedures
- anticipation of receipt
- establishment of hash and value totals
- batch header/transmittal slips
- numbering of batches
- recording of register
- evidencing receipt and submission

- indicating cut-off points

Data should be received and controlled by a separate section or person (also applicable to data captured at remote locations):

- recording of data received
- anticipation of receipt

- checks on data for
  - correct assembly of batch etc.
  - batch sequence number
  - authorisation by user department
- balancing procedures
- error recording and follow-up for correction and re-submission

User departments and not the data centre are primarily responsible for controls over input and output.

Data control activities within the IS department are independent of other functions and user departments:

- the data control section is responsible for production liaison between data processing and other departments
- control functions covering all production runs on every shift are performed in an area with restricted access.

4.6.1.2 TO ENSURE THAT DATA IS ACCURATELY TRANSCRIBED INTO MACHINE READABLE FORM

Data capture should be adequately scheduled and controlled:

- record of data submitted for capture
- monitoring of progress
- return of input forms after capture
- maintenance and review of data capture statistics

Adequate procedures should be established for data capture:

- procedures documented and given to staff
- indication of persons responsible
- no correction of errors on input forms
- recording and reviewing overrides

The computer, terminal, etc. should be used to check accuracy of data captured wherever possible:

- format checking
- sequence checks
- range and logic checks
- anticipation
- comparison with master file
- agreement of batch and hash totals

Procedures should be established for handling errors:

- procedures documented and distributed to staff and users
- consistent method (e.g. batch rejected, suspense file, etc.)
- recording of errors
- follow-up
- re-submission of corrections
- documentation of corrections
- cut-off points
- review of corrections made
- maintenance of error statistics

4.6.1.3 TO ENSURE THAT ALL DATA AND ONLY AUTHORISED DATA IS PROCESSED

Outputs should be reconciled to input:

- procedures documented and distributed to staff
- reconciliation and balancing procedures by
  - users
  - data control
- agreement of batch totals
- evidencing of agreement in registers
- where appropriate, detailed checks
- independent checks

Error and exception reports should be properly controlled:

- procedures documented and distributed to staff
- nil reports produced
- no action by operators
- check that action taken where necessary

- submission of corrections
- cut-off points
- independent checks

Accuracy of data must be maintained during processing:

- run to run controls exercised by operators or computer
- trailer label totals
- editing of data
- hardware checks
- scrutiny of reports for reasonableness

Access should be restricted to data capture and control areas.

4.6.2 OPERATORS

4.6.2.1 TO ENSURE THAT POLICIES AND STANDARDS ACHIEVE A HIGH DEGREE OF PERSONNEL AND OPERATING EXCELLENCE

An adequate training programme should be established for all IS staff:

- training related to duties and career paths
- formal records kept of training
- review of results of courses, etc.

Polices, standards and conventions should be clearly defined in writing and should cover:

- broad policies of the company and IS department
- procedures to be followed by different sections of department
- standards and conventions to be adhered to in programming, operating and other activities
- documentation to be prepared and examples thereof (e.g. user manuals, operating instructions, etc.)

The department should be adequately staffed with competent personnel:

- recruiting practices should consider education experience and security risks relative to the job requirements
- reliance on vendor or software house
- staff turnover rate

- staff compensation and benefits
- reliance on key personnel
- recent or planned re-organisations

Adequate liaison should be maintained with staff:

- regular review of work done
- discussions on plans and progress
- regular meetings on problems, status of work, training and other items of concern
- copies of relevant job descriptions, policies, standards and conventions, should be given to each staff member
- regular review of job descriptions

4.6.2.2 TO ENSURE THAT ACTIVITIES OF OPERATORS ARE CONTROLLED

Standard procedures should be distributed for all operations:

- procedures documented and distributed covering:-
  - o operating procedures
  - o messages and codes
  - o run manuals
  - o emergency procedures
- management review of adequacy of procedures
- updating for changed equipment or circumstances
- independent review

Operators' activities should be regularly reviewed:

- operator and programmer segregation should prohibit programmers from operating the computer during normal production runs
- operators should not be permitted to modify software (or correct errors); console program debugging should be against installation practice and rigorous controls should authorise and monitor the use of file amendment utilities, that by pass access controls
- there should be management supervision on all shifts which are jointly operated, or alternatively, are operated by a supervisor
- through shift rotation and annual leave requirements, no operator has responsibility for continually running a sensitive, or other given application
- every operating run is programmed to print out all operator intervention and console messages on sequentially numbered console sheets

- spooling to a password protected disk area should provide an automated log of all console activity which may be retrieved by management in report form, preferably on an exception basis
- the console print out, job accounting report and operations log are reviewed and initialed daily; compared with scheduled and previous run times; and variations from the operations schedule are investigated
- a report is prepared for management noting all exceptions occurring during each shift (re-runs, error halts, down time, program changes, console input etc.)
- logs are retained for a sufficient time to meet audit requirements, to permit further analysis and facilitate problem solving
- periodic spot checks on night shifts
- independent checks

It desirable to restrict operators knowledge of programming.

Batch processing runs should be authorised:
- recorded in writing
- authorised by appropriate official
- priority of runs indicated

There are written standards that expedite the flow of input data and control job set-up procedures:
- scheduling is responsible for collecting input data and for monitoring an input/output log that records relevant details of prepared data and its movement, through processing, back to data control, together with output reports
- appropriate data files and programs are drawn from the library and assembled with prepared data, and required job control statements and operating instructions, for submission to operations for processing
- runs on request of users etc. supported by signed forms
- interface with file library
- independent checks on applications run with authorisation records

All operations should be scheduled.

A separate section (or official) within the IS department is responsible for job assembly on all shifts, and, in consultation with data control and system development, for all job scheduling.

The computer workload is controlled by operations schedules prepared for both routine and non-routine work. This workload should be evenly spread.

- daily and weekly schedules are maintained, showing the programs to be run, set-up times, run times, time set aside for program testing and debugging; and the assignment of partitions in a non multi programming environment. Runs should be co-ordinated with user requirements and submission of data
- the scheduling section receives copies of daily operating logs, maintained by operators, or job accounting information reports prepared by the computer, that contain details of actual run start and stop times; operator, program and report identification etc.
- schedules and actual processing reports are compared and initialed after obtaining reasonable explanations for outages, error halts, re-runs, other corrective actions and unscheduled operations
- management reports are prepared summarising machine utilisation and application schedule performance

4.6.2.3 TO ENSURE THAT THE CORRECT VERSIONS OF FILES AND PROGRAMS ARE USED IN PROCESSING

A record should be kept by the custodian of all files giving their location and applications in which they are used:

- files in library
- files in off-premises storage

All files should be labelled externally and internally:

- clear and distinctive external label specifying, VSN, creation date, creation program, retention date and owner of the file or a reference number
- periodic independent agreement of internal and external labels
- use of trailer labels containing control totals and counts
- generation of a file catalogue by an automatic library utility

Details of files used in each run should be documented and made available to operators:

- run manuals
- run schedules
- files to be used

File labels should be checked:

- external labels by operators
- internal labels by system and/or application software
- console log recording of errors in file labels and overrides

Files should be issued in accordance with authorised processing schedule:

- schedule of processing runs formally documented
- schedule checked for correct authorisation
- independent checks on files assembled
- evidencing of receipt of files by operations
- protect rings

Only authorised programs are issued to production:

- system development library should be separate from production library
- in a data-base environment, data integrity is preserved by a data base administrator who is independent of the systems and programming functions, and controls data base design, security procedures and documentation adequate for accounting control purposes
- in an on-line environment the system software should ensure that the correct version of files or data bases are used

4.6.2.4 TO ENSURE THAT FILES REQUIRED FOR FURTHER PROCESSING OR BACKUP PURPOSES ARE CORRECTLY RETAINED

Checks should be made to ensure all files are returned after processing:

- check against record of files issued
- evidence of return
- follow-up on outstanding files
- programming file control

Files should be retained in accordance with laid down policy:

- retention policy established and documented
- custodian of files aware of policy
- record of files to stay in library and files to go to off premises storage
- housekeeping within library
- documentation of movements to and from off-premises storage

- accurate records of files and their location
- retention dates in file records and header labels
- independent checks on files retained

4.6.2.5 TO ENSURE THAT SYSTEM SOFTWARE IS USED TO MONITOR AND ASSIST OPERATOR FUNCTIONS

The need for operator intervention and decisions is kept to a minimum.

Comprehensive operating instructions should be available to operators:

- instructions for all runs and all contingencies documented
- full list of system messages and responses
- run manuals, which have been developed by programmers for each program suite should describe run times; console messages; programmed halts; required responses; recovery procedures
- kept up to date for all changes
- any special instructions recorded on run sheet

Operating system and standards of systems developed should require little or no operator intervention:

- the operating system comprising supervisor; control and documentation as an application program but maintenance and testing is confined to system programmers who are independent of operators and application development
- the capabilities of the operating system include system action and hardware error logging; device assignment; program loading and communication; check point restart and job accounting; multi-programming, data communication and remote job entry control; file handling, checking and library etc.

4.6.3 EQUIPMENT AND SYSTEMS SOFTWARE

4.6.3.1 TO ENSURE THAT BUILT-IN HARDWARE AND SOFTWARE CHECKS WILL DETECT AND REPORT MALFUNCTIONS

Procedures should prevent and detect operator error and machine or programming malfunction:

- hardware controls include double reading of input; read after write onto magnetic media; longitudinal and lateral parity checking; block counts and count reconciliation's
- edit checks including, range, format, limit and validity checks
- balancing procedure (manual and computer)
- monitoring of file utilisation
- preventative maintenance is scheduled to minimise program disturbance and it is performed on all equipment by vendor engineers
- operators only execute recommended cleaning procedures and tests, incorporating the transmission control mechanism, and network links for operations integrity

4.6.3.2 TO ENSURE THAT THE USE OF UTILITIES IS RESTRICTED TO AUTHORISED USERS AND SITUATIONS

Use of utilities and generalised software that is capable of up-dating files, should be strictly controlled:

- authorisation for use by senior officials
- regular review of usage reports
- independent checks
- multi level password control

4.6.3.3 TO ENSURE THAT HARDWARE AND SOFTWARE WILL CONTINUE TO OPERATE EFFECTIVELY

Recommended preventative maintenance procedures should be followed:

- contract with vendor or 3rd party
- record of maintenance carried out
- environment specifications adhered to
- maintenance times included in scheduling

Adequate housekeeping procedures should be followed:

- procedures documented and given to operators
- regular inspection by operations manager/other official

Records should be kept of all malfunctions and downtimes:

- recorded and summarised on a regular basis

- reviewed by IS and company management
- discussed with vendor/maintenance firm.

4.6.4 OUTPUT

4.6.4.1 TO ENSURE THAT ALL OUTPUT REQUIRED IS PRODUCED

Checks should be made to ensure that all reports have been produced:

- expected reports documented and distributed to staff
- number of copies
- nil reports produced
- reports checked against list by data control
- no reports retained by operations
- anticipation by users
- special request reports

4.6.4.2 TO ENSURE THAT OUTPUT IS DISTRIBUTED TO AUTHORISED PERSONNEL

Reports should be delivered to the correct user departments:

- required distribution recorded in writing
- evidence of receipt by users
- independent checks

4.6.4.3 TO ENSURE THAT CONFIDENTIAL OUTPUT IS CONTROLLED

- control of input documentation
- special procedures for data capture
- restriction on who can run applications
- printing, decolating and distribution reports
- destruction of carbon paper
- encryption of files sent to remote sites
- encryption of transmission data

4.6.4.4 TO ENSURE THAT PROCESSING IS ACCURATE AND COMPLETE

- control information is reconciled to run reports and balanced to final output which is also reviewed for completeness and reasonableness
- all errors are reported to appropriate users and operations supervisors, and the correct re-submission of data by originators is controlled through error listings, suspense accounts or registers
- input and output logs are reviewed and initialed by appropriate management on a continuing basis
- run to run control totals

4.7 PHYSICAL SECURITY AND RECOVERY CONTROLS

4.7.1 PHYSICAL SAFEGUARDS

4.7.1.1 TO ENSURE THAT ENVIRONMENTAL CONTROLS ADEQUATELY SAFEGUARD FILES AND EQUIPMENT FROM DAMAGE OR CORRUPTION

The facility is physically secure as are the equipment, files and documentation it contains:

- various lock and key combinations reduce levels of access within the installation to authorised personnel, whose entrance is recorded on appropriate logs.
- together with suitable sealing, drainage and the use of non-combustible materials, tested manual/automatic corrective systems protect the facilities from fire, flooding, dust and political riots.

Checks should be made to ensure that only authorised items are allowed into and out of IS area:

- cases, bags, etc. examined
- documentation for movement of files, etc.
- recording of details of incidents

References should be obtained and security checks made on all new members of staff employed.

There should be laid down procedures for action to be followed in the event of fire or other catastrophe:

- procedures documented and distributed to all staff
- procedures practised periodically

Protection test checks should be done to ensure files have not been corrupted.

4.7.1.2 TO PREVENT INTERRUPTIONS IN INFORMATION SERVICES OPERATIONS

At least two generations of programs, transaction and master files are maintained in secure, on-site storage (vaults) according to written standards.

Off-site back-up comprising regularly rotated, recent generations of vital records (operating system software code, application software libraries, relevant documentation, data files, forms etc., JCL summaries, run manuals) permits total and program recovery from minor disasters.

Regular maintenance and backup of equipment in conjunction with a stable power supply, minimise processing difficulties caused by hardware failure.

Emergency procedures, and drills contribute towards good housekeeping and low risk of complete disaster whatever the cause.

There is a written, comprehensive contingency plan and adequate insurance cover. The contingency plan should be corporate wide and not only address the IS department.

Alternative sources of supply ensure that forms and stationery are always available at short notice.

Insurance policies are reviewed annually and cover is upgraded when necessary for hardware, software, business interruption (includes loss of profits), reconstruction of data, and blanket fidelity guarantee for all IS personnel including outside operators.

4.7.2 RECOVERY

4.7.2.1 TO MAINTAIN CONTINUOUS OPERATIONS AFTER LOSS, DAMAGE OR DESTRUCTION OF PREMISES EQUIPMENT FILES OR DOCUMENTATION

Suitable back-up facilities should be available:

- written agreements are obtained negotiating the emergency usage of standby processing sites
- compatible equipment
- compatible system software
- sufficient number of peripheral devices
- sufficient machine time available
- data capture and transmission facilities
- signed contract
- agreement on charges

4.7.2.2 TO PROVIDE SECURITY AGAINST DESTRUCTION OF RECORDS AND TO ENSURE CONTINUOUS OPERATIONS

- plans and procedures documented and distributed
- partial destruction
- on-line processing
- batch processing
- processing priorities
- maintenance of essential controls
- handling, transport and storage of data
- hours of work
- address of key employees and vendors
- continued off-premises back-up of files and documents
- insurance cover for additional costs involved
- periodic tests of plans and procedures
- provisions for re-establishing the communications network following an interruption in service
- provision for backup CPL power
- manual procedures which may be necessary until backup computer service is re-established

4.8 CONCLUSION

The creation of an environment that will prevent computer-related crime and will possibly detect those instances that do occur, is the responsibility of management. How that environment and culture is created varies between organisations as do the actual controls and culture that is put in place to prevent employee fraud.

Management cannot simply give lip service to the problem believing that it will not happen to them. The chapters that follow attempt to identify whether there is in fact a problem and, if so, the magnitude of such computer-related criminal acts within our selected population. The information obtained from our sample can serve to highlight the dangers of assuming that computer-related crimes will not occur. Management has a legal responsibility to ensure that an adequate system of internal control for that organisation has been instituted.

This chapter has attempted to define a framework of controls that would assist management in creating an environment that would severely restrict the opportunity for, as well as the detection of, computer-related criminal acts.

CHAPTER 5

RESEARCH METHODOLOGY

5.1 STATEMENT OF THE RESEARCH

This study investigated the perceptions of management on computer-related crime. The literature has identified what can be constituted as comprising a computer-related crime as well as any legal definitions of computer- related crime as defined by case law, both local and overseas.

There are three major investigative problems :

1. Assess whether management are solely responsible for detecting computer-related crime within their organisation.

2. Ascertain the extent management perceive that they are assisted by their external auditors in the detection of computer-related crime within their organisation.

3. Determine whether management are able to rely solely on their auditors to detect computer-related crime within their organisation.

The experimental design for the study required that data be collected from the management of local organisations.

A series of variables were defined :

- four definitions of a computer-related crime
- seven computer-related criminal activities
- fifteen computer-related methods to perform such a crime
- six methods of perpetrating a computer-related crime
- five areas of management that might prevent and detect such a crime

- o seven avenues by which a computer-related crime might be detected have been extracted from past research. These variables served as the basis for the questionnaire items.

5.2 THE QUESTIONNAIRE

5.2.1 PILOT STUDY

The questionnaire was validated for reliability by performing a pilot study. The goal of the pre-testing was to refine the research instrument, in this case the questionnaire. Appendix B contains a copy of this questionnaire.

The pilot study questionnaires were administered to three organisations. The one was a manufacturer, whilst the other two were both manufactures and distributors. These respondents were asked to complete the questionnaire to the best of their ability and to make notes on the clearness, ambiguities and conceptual problems encountered while completing the questionnaire.

The results of the pilot study were carefully evaluated focusing specifically on ;

- o question clarity, and
- o question format.

After corrections were done to the questionnaire, they were sent out to the senior executive of each of the respondent organisations for final comment. Each of the three pilot survey organisations were also sent a copy of the final questionnaire. The results of the pilot study were not included in the final results as these three organisations returned a completed final questionnaire.

5.2.2 SURVEY CONTENT

The survey consisted of :

- o a covering letter written by the Rector of the University encouraging the respondents to complete the questionnaire
- o the questionnaire

- o an addendum explaining specific terms used within the questionnaire to describe methods of computer abuse
- o a stamped return envelope.

5.2.3 QUESTIONNAIRE DESIGN

The variable items were identified from the literature and the questionnaire items were constructed with these variables. The design of the data collection instrument was based on the idea that the questionnaire would be mailed to selected organisations. The questionnaire appears in Appendix B.

The questionnaire comprised :

- o a number of structured questions from which the respondent must choose the appropriate response from a given number of specific response categories. This comprised dichotomous questions, multiple choice questions, rank order questions and scaled questions.

- o a number of unstructured questions where the respondent was encouraged to formulate and express the response freely in relation to preventative measures that they have implemented to minimise computer- related crime as well as any incidence's of computer-related crime that they might have experienced.

The questionnaire sought to lead the respondent on a logical basis from initially expressing an opinion of what comprised a computer-related crime to the final question which sought to ascertain whether the respondents organisation had been the victim of a computer-related crime.

Confidentiality of the organisation and respondent was maintained. The questionnaire sought to identify the managerial position of the respondent, the business sector in which that organisation operated, and the number of employees employed by that organisation. The number of employees was used to estimate the significance of that respondent's answers to the questionnaire.

5.3 THE SAMPLING TECHNIQUE

It was decided that a random selection of 100 organisations would be made from the Eastern Cape, Border and Southern Cape to form the selection of organisations to be surveyed. This extended region is defined as the Eastern Cape for the purpose of this exercise.

Schedules were obtained of those organisations registered with the Chamber of Commerce and the Midland Chamber of Industries. This information was also obtained on a personal computer diskette. These schedules were to form the basis of the population from which the sample would be drawn of those local organisations to be surveyed. Most of the larger organisations are registered with one of these bodies, and it was therefore considered that these lists would be representative of the organisations to be sampled. An analysis of these schedules revealed the following information :

Region	No. of registered organisations
o Eastern Cape	1 148
o Border	594
o Southern Cape	234

This represents a total of 1 976 potential organisations.

A decision had been made that the sample selected should be representative of those organisations with a local head office, regional or branch office in the Southern Cape, Eastern Province or Border as currently defined. In order to achieve this only those organisations with an annual turnover in excess of R 5 million should form the basis of the population. However, both the Chamber of Commerce and the Midland Chamber of Industries had no means of identifying member organisations that met this criteria.

Each organisation had an alphabetical code on their record on the diskette that indicated the maximum potential number of persons employed. These codes represented size categories of the number of potential employees, examples of which are : "A" = 0 to 10 employees, "B" = 11 to 20 employees, and "C" = 21 to 50 employees.

From discussions held with the director of the Chamber of Commerce as well as two audit partners from two of the large local audit firms, it was agreed that a similar result could be obtained by excluding those organisations with 10 or less employees from the schedules. An

analysis of these schedules revealed that most of the organisations employing 10 or less employees were either agencies, speciality shops, cafes, or engineering works, and did not meet our original selection criteria.

Excluding those organisation employing 10 or less person resulted in a population of 921 organisations - as 53,4% of the members on the schedules received employed 10 or less employees.

A random selection of 100 organisations were selected from this final population of 921 organisations. These 100 companies selected randomly represents 10,8% of our population and can be regarded as being sufficient to be able to obtain representative findings from our population group.

The organisations within the population were numbered from 1 to 921. A computer program that generates random numbers was used to generate the numbers for selecting the 100 organisations that were to be surveyed. This program runs on a personal computer. The current date was converted into a relative number expressed as elapsed days from 1 January 1900, and entered as the initial base random number from which the random numbers were to be generated. Six digit random numbers were generated of which the last three digits were used to select organisations for the sample.

Prior to mailing the questionnaires, it was decided that a response rate of at least 30% of the total number of questionnaires mailed would be required from this survey. In the event of the initial mailing producing at least this number, then there would be no necessity to perform a second or subsequent follow-up. The initial response, in fact, resulted in thirty two questionnaires being received, a response rate of 32%.

5.4 RELIABILITY OF THE DATA

The initial questionnaire for the pilot study was field tested by three organisations as discussed in point 5.2.1 above. The senior executive of each of these organisations was contacted who arranged to have the questionnaire completed. The completed questionnaires were collected and discussed with the respondents. These discussions revealed minor changes that were required to the questionnaire. These changes were incorporated in the final version of the questionnaire that was circulated.

The questionnaire was designed in such a manner that each question flowed into the following question in order to ensure that the answers given were factual and not theoretical or based on what the respondent perceived the answer should be. The final question sought to determine whether that organisation had, in fact, experienced a computer-related criminal act.

The completed questionnaires were coded by one person to ensure that a uniform coding system was applied prior to processing. The results were tabulated using a computer.

5.5 INTERVIEW TECHNIQUES

A postal survey was considered to be the most appropriate method in view of the vast area to be covered by the sample population.

The advantages of this method are :

- lower unit costs
- freedom of the respondents in completing the questionnaire
- relative speed in contacting all respondents simultaneously
- permits a large geographical coverage
- homogeneous stimulus
- processing is relatively easy
- maintains anonymity of the respondent
- ease of processing.

Limitations considered in the design of the questionnaire :

- representativeness
- negative attitudes
- impersonal
- literacy
- lack of control
- interdependence of the responses
- time consumption.

An attempt was made to reduce the impact of these limitations by :

- inviting respondents to request a copy of the survey findings
- directing the questionnaire to the senior executive of that organisation

- o enclosing an addendum summarising the computer-related crime methods mentioned in the questionnaire.

5.6 SUMMARY

The design of the study provided the capability for investigating the identified variables influencing the perception of computer-related crime.

One hundred organisations were selected randomly from which a sample was to be obtained. Data were collected through a questionnaire that was developed from the literature defining the components of, classifications of, and methods of computer-related crime. The data were collected through a postal survey and were analysed to determine management perceptions of, as well as any actual instances of, computer-related crimes.

CHAPTER 6

ANALYSIS AND PRESENTATION OF FINDINGS

6.1 INTRODUCTION

The data collected by the questionnaire are presented in the tables that follow. Each question is tabulated, analysed and interpreted separately. However, in certain cases, these results in isolation might not be meaningful and have therefore been cross-tabulated with other questions to obtain a more meaningful result. Where the answers to various questions are closely related to one another, they have been presented together in the same table.

Thirty two responses to the questionnaire were received. However, this included five blank questionnaires. These blank questionnaires were excluded which reduced the sample size to twenty seven usable questionnaires. This sample size of 27 is considered to be adequate although it falls below the required response of at least 30%, and is used in all the analyses that follow.

Appendix C presents the detailed results of the statistical analysis. These data are presented for information purposes only, as the results have been summarised under question headings below.

6.2 RESULTS AND DISCUSSION

QUESTION 1

Question number 1 sought to identify the person who had been assigned to complete the questionnaire. The questionnaire had been sent to the Senior Executive, as a number of the selected organisations were either regional or branch operations of their parent company.

An examination of the titles of the persons completing the questionnaire revealed an interesting cross section of positions ranging from the Chief Executive Officer of a listed company to the Cost Accountant for a branch office of a national group. An interesting point is that for the municipalities surveyed, the City Treasurers responded. This revealed the seriousness with which they viewed the subject matter of this questionnaire.

Table I Capacity of the person completing the questionnaire

Category	Percent
Senior Management	51,8
Middle Management	40,8
Operational Management	7,4
Total	100,0

QUESTION 2

Question number 2 dealt with the period that the person completing the questionnaire had been in that position. The period employed in that position ranged from 1 to 20 years.

The respondents appeared to have been in these positions for a sufficient length of time to be able to accurately complete this questionnaire.

Table II Period employed in that capacity

Number of years	
High	20,0
Low	1,0
Average	5,4

QUESTION 3

Question number 3 sought to identity that sector in which that organisation operated. The respondents are seen as being representative of those organisations operating within the Eastern Cape.

Table III Sector

Category	Percent
Banking	0,0
Distribution	0,0
Education	3,7
Finance	7,4
Local government	11,2
Manufacturing	44,4
Retail	0,0
Service	25,9
Wagering	3,7
Wholesale	3,7
Total	100,0

QUESTION 4

The purpose of question number 4 was to ascertain that the respondents were representative of all the organisations within the selected region as defined. The survey was found to have included organisations with staff complements ranging from 9 to 7 000 employees, and is considered to be representative of the population.

Table IV Number of employees

	Number
High	7 000
Low	9,0

Table V Staff complement

No. of employees	Percent
1 - 50	18,5
51 - 100	7,4
101 - 500	33,3
501 - 1 000	11,2
1 001 plus	29,6
Total	100,0

QUESTION 5

Question number 5 sought to identify what the respondents considered comprised a computer-related crime, as there is no definitive definition of what comprises such a crime. The findings in Table VI support the views expressed in this study (cf. chapter 2) as to what comprises a computer- related crime.

Table VI Components of a computer-related crime

Category	Percentage		
	Yes	No	Do not know
The introduction of fraudulent information into a computer system.	96,3	3,7	0,0
Unauthorised use of computer facilities.	81,5	14,8	3,7
The alteration or destruction of information.	85,2	14,8	0,0
The stealing by electronic means of money, financial instruments, property, services, or valuable data.	88,9	11,1	0,0

QUESTION 6

Respondents were asked for their opinion, in question number 6, on the importance of having to have a computer to be able to perpetrate a number of different criminal activities. Table VII tabulates the findings of the respondents. These findings supported the study which defined how a computer might be utilised in perpetrating such crimes. A point of note is that the respondents generally felt that the destruction of equipment and supportive facilities, and the misrepresentation of the quality and extent of computer technology in use, do not constitute a computer-related crime.

This, however, is not borne out by the conclusions from Table IX and Table XVI where a major fraud was committed involving the private use of facilities.

Table VII The significance of the use of a computer in being able to commit a criminal activity

Category	Rated as:
Destruction of equipment and supportive facilities	Slightly important
Destruction of data	Important
Manipulation of information	Very important
Falsification of records	Important
Covering up fraudulent activities	Important
Unauthorised use of confidential information	Important
Misrepresentation of the quality and extent of computer technology actually in use	Slightly important

QUESTION 7

Question number 7 was intended to determine the perceptions of the respondents as to what methods could be used in perpetrating a computer- related crime. The respondents rated these methods as they perceived that they were applicable to both their own organisations as well as for the Eastern Province as a whole. Of concern is the low assessment given to these items. Management appear to be unaware of the methods perpetrators could employ in committing such crimes. The respondents rated their own organisations lower than that for the region. An interesting point arising from this sample is that the respondents in general perceived that the incidence of computer-related crime to be very low. This was not supported by the analysis which follows of crimes actually perpetrated within the Eastern Cape. Of interest is that the two popular media methods of hacking and the planting of viruses were considered to be very low.

Table VIII Prevalence of methods for committing a computer-related crime

	The average rating for the sample is:	
	Own organisation	Eastern Province
Data diddling	Very seldom	Seldom
Trojan horse	Almost never	Very seldom
Salami techniques	Almost never	Very seldom
Superzapping	Never	Very seldom
Trap doors	Almost never	Very seldom
Logic doors	Almost never	Very seldom
Asynchronous attacks	Almost never	Almost never
Scavenging	Almost never	Very seldom
Data leakage	Very seldom	Very seldom
Piggybacking and impersonation	Almost never	Very seldom
Wire tapping	Almost never	Very seldom
Simulation and modelling	Almost never	Very seldom
Hacking	Almost never	Very seldom
Planting of viruses	Very seldom	Seldom
Invasion of privacy by unauthorised access to data	Very seldom	Seldom
Fraud	Almost never	Very seldom

QUESTION 8

Respondents were asked in question number 8 to indicate what type of computer-related crime, if any, they had experienced within the last 18 months. Table IX reveals that 8% of the sample of 100 organisations, or 29,6% of the 27 respondents, had experienced some form of computer-related crime within this period. A major concern is the number of instances reported which range from 1 to 5 per organisation. Dividing the total number of reported instances by the number of organisations involved, results in an average of 2 instances per organisation for those having reported some form of computer-related crime.

Appendix C presents the results of the statistical analysis of the questionnaires actually received. The standard deviation determined for question 8 was 1,96, with a mean of 0,704. Based on a confidence level of 95%, the precision limits calculated for this question are 0 to 1,478.

From this it could be deduced that one could be 95% confident, that most organisations could expect to experience up to 1,5 instances of computer- related crime within an 18 month time frame.

Table XVI analyses those crimes reported in Table IX where additional information was supplied. However, Table IX contains limited information as most respondents were unprepared to disclose additional information on the crimes that they reported under this question.

Table IX Computer-related crimes perpetuated within the last 18 months

Category	Instances		Number of organisations involved
	Number	Percent	
Modification of programs	5	31,3	1
Modification of data	2	12,5	2
Destruction of equipment	0	0,0	0
Disclosure of information	1	6,2	1
Unauthorised use of equipment	5	31,3	2
Denial of use of equipment	3	18,7	2
Total	16	100,0	8

QUESTION 9

Table X, prepared from the findings of question number 9, indicates that management rely heavily on the computer department and the internal audit department to detect occurrences of computer-related crime, whilst senior management and the computer department are relied on to prevent such crimes. An interesting point is the very high reliance placed upon the computer department to detect and prevent computer-related crime. This should be of concern to management in view of the fact that the computer department staff are ideally placed to perpetrate such crimes. If they were to check on themselves, then one could expect any such instances to go unreported. The external auditors are also seen as being very important in the process of detecting and preventing computer-related crime.

Table X Detection and prevention of computer-related criminal acts

Category	Detection	Prevention
Senior management	Very important	Extremely important
Middle management	Very important	Very important
Operational management	Extremely important	Extremely important
External auditors	Very important	Very important
Computer department	Extremely important	Extremely important

QUESTION 10

Question number 10 sought to identify that person within each organisation that is entrusted with the responsibility for the detection and prevention of computer-related crime. Tables XI and XII indicate that such a person is either the Information Services Manager (once again the Computer Department Manager) within Middle Management or the Financial Director within Senior Management. This tends to support the views expressed in Table X that management rely heavily on the Computer Department manager to prevent and detect computer-related criminal acts.

Table XI Person entrusted with the detection and prevention of computer-related crimes

Category	Percent
Senior management	37,4
Middle management	50,1
Operational management	12,5
Total	100,0

Table XII Analysis of management structures

Job title	Percent	Percent
Senior management:		37,5
Chief Executive Officer	4,2	
Managing Director	4,2	
Financial Director	20,7	
Deputy Director Finance	4,2	
Director	4,2	
Middle Management:		50,1
Information Services Manager	29,2	
Financial Manager	8,3	
Administration Manager	4,2	
Internal Audit Manager	4,2	
Systems Manager	4,2	
Operational Management:		12,4
Systems Accountant	8,2	

Systems Accountant		4,2	
	Total	100,0	100,0

Table XIII Department in which the person responsible for the prevention and detection of such crimes is employed

Department	Percent
Finance	41,7
Information Services	33,4
Administration	4,1
Internal Audit	4,1
Senior Management	16,7
Total	100,0

QUESTION 11

Table XIV indicates that sound control procedures will assist management in detecting computer-related crime. It should be noted that the external auditors were rated as only being fair regarding their suitability in detecting such crimes, even though Table X indicated that management relied on their external auditors to detect and prevent such crimes.

Table XIV Department suitability in detecting computer-related crime

Department	Rating
Internal audit	Good
External audit	Fair
Control procedures	Excellent
Fellow workers	Good
Customer complaints	Good
Investigation after suspected foul play	Good
Chance/accident	Fair

QUESTION 12

Table XV is prepared from question number 12. This indicated that the most common preventative measures in force related to user codes and passwords, access controls and limits, daily control checks, and internal audits. Internal audit was also relied upon to prevent computer-related crimes which is also supported by Table X. The emphasis appears to fall on internal audit and the computer department to prevent such crimes.

Table XV Preventative measures implemented to minimise the incidence of computer-related crime

Measures	Percent
Access controls and limits	38,9
Authorisation levels	5,6
Change control procedures	5,6
Code of conduct	5,6
Computer systems audits	5,6
Control procedures	22,2
Daily control checks & procedures	22,2
External auditors	11,1
Fellow workers	5,6
Internal audits	22,2
Monitoring of computer processing	11,2
Monthly control checks & procedures	5,6
Quality of staff	5,6
Record of report originator	5,6
Restricted access to premiums	11,1
Restricted access to programs	22,2
Segregation of duties	16,6
Software security packages	5,6
Timeous management information	5,6
User codes and passwords	50,0
User logs and profile lists	11,1
Well designed systems	5,6

QUESTION 13

Table IX reported 16 computer-related crimes, whereas only 2 such instances are tabulated in Table XVI. Only 2 respondents were prepared to supply the information requested in this question.

This table was prepared from question number 13. The survey results were to small to indicate a definite conclusion other than that there appeared to be a reasonable possibility of perpetrators of computer-related crime not being prosecuted and that such crimes were usually committed by only one person.

Of concern is the high Rand value of the losses incurred in these two cases. These losses might be high for an individual but not for the organisations involved. In terms of these organisations turnovers, these losses are immaterial which might serve to explain the reluctance to prosecute and draw attention to that organisation. The remaining 6 respondents appeared to be unwilling to disclose further information on those computer-related crimes that they had experienced.

Table VII indicated that the respondents generally felt that the destruction of equipment and supportive facilities, and the misrepresentation of the quality and extent of computer technology in use, did not constitute a computer-related crime. This, however, was not borne out by the conclusions from Table IX and Table XVI where a major fraud was committed involving the private use of facilities.

Table XVI Details of computer-related crimes experienced within the last 18 months

Types of crime	Perpetrated by	No. involved	Detected by	Value of loss	Prosecuted
1 Payroll fraud	Accounts Supervisor	1	Manpower Manager	R 65 000	Yes
2 Private use of facilities	Manager	1	EDP Audit Manager	R 250 000	No

CHAPTER 7

SUMMARY AND CONCLUSION

7.1 INTRODUCTION

This study sought to define what is a computer-related crime as well as a number of methods for perpetrating such crimes.

The South African criminal legislation was examined as it pertained to computer crime and it was found that there is no specific legislation in place as in either the United Kingdom or the United States of America for the prosecution of such crimes.

A control methodology has been presented that could assist management in the detection and prevention of computer-related crime.

7.2 DEFINITION OF A COMPUTER-RELATED CRIME

The results from the survey revealed that the respondents agreed that a broad definition of a what comprises a computer-related crime includes :

- the introduction of fraudulent information into a computer system
- the unauthorised use of computer facilities
- the alteration or destruction of information
- the stealing by electronic means of money, financial instruments, property, services, or valuable data.

The respondents also agreed that a computer can be used in perpetrating the following types of computer-related crimes :

- destruction of equipment and supportive facilities
- destruction of data
- manipulation of information/data
- falsification of records
- covering up fraudulent services

- o unauthorised use of confidential information
- o misrepresentation of the quality and extent of computer technology actually in use.

The smaller organisations did not believe that the destruction of equipment and supportive facilities, or that the misrepresentation of the quality and extent of computer technology actually in use, were components of a computer-related crime, whereas the larger organisations believed that these were.

7.3 COMPUTER-RELATED CRIME METHODS

The respondents confirmed that they considered the following methods as being part of a computer-related crime :

- o asynchronous attacks
- o data diddling
- o data leakage
- o fraud
- o hacking
- o invasion of privacy by the unauthorised access to data
- o logic bombs
- o piggybacking and impersonation
- o planting of viruses
- o salami techniques
- o scavenging
- o simulation and modelling
- o superzapping
- o trojan horses
- o trap doors
- o wire tapping.

The above methods were seen as resulting in the following activities being perpetrated against other computer services, computer equipment, computer programs or data :

- o denial of the use of information
- o destruction of equipment
- o disclosure of information
- o modification of data
- o modification of programs
- o unauthorised use of equipment.

7.4 DETECTION OF COMPUTER-RELATED CRIME

Operational management, including the computer department were seen as being extremely important in detecting any computer-related crime within the organisation.

Control procedures were seen as being excellent in detecting such crimes.

Internal audit, fellow workers, and subsequent investigation after suspected foul play were perceived as being good in detecting computer abuse. Whereas, external audit and chance or accident were perceived as only being fair in detecting such abuse.

7.5 PREVENTION OF COMPUTER-RELATED CRIME

Senior management, operational management, and the computer department were seen as being extremely important in the prevention of computer-related crime.

Middle management and the external auditors were rated as being very important in preventing such abuse.

The most common preventative measures that organisations had implemented were :

- access controls and limits
- control procedures
- daily control checks
- internal audits
- monitoring of computer processing
- restricted access to premises
- restricted access to computer programs
- user codes and passwords
- user logs and profile lists.

The respondents tended to rely on segregation of duties, password and access controls to prevent and detect computer-related crimes. The controls mentioned by the respondents revealed a lack of seriousness on the part of management towards the control and monitoring of their computer activities. This was supported by management's perception that a computer-related crime would not happen to their organisation as they could rely on the integrity and honesty of their employees.

Since computer-related methods to perpetrate such a crime vary widely from the clumsy to the sophisticated, countering them can be achieved only through the use of a diverse range of counter measures - the most important of which is the correct treatment of employees. No internal control system is any more reliable than the people who operate and maintain it. It is easy to think of computer security and fraud in terms of technology alone, but computer-related security and crime is more than a technological problem - it is a people problem (Parker, 1986). Motivated, challenged employees will be far less likely to perpetrate computer-related crimes than employees who feel resentful toward their superiors and the company in general. The literature would indicate that increasing the awareness of computer-related crime and the use of counter measures may serve to reduce the incidence of such criminal acts.

The survey identified a common point of view, which was that management is primarily responsible for the prevention and detection of computer-related crime. In addition to this, it was held that the internal auditor and the information systems manager (or Computer Department manager) should share the responsibility with management for the prevention of computer-related crime, whilst the external auditor should share senior management's responsibility for detecting computer-related crime.

7.6 PERCEPTIONS ON THE LEVEL OF COMPUTER-RELATED CRIME

An interesting point revealed by the survey was on the perception of the level and incidence of computer-related crime within the surveyed organisations as well as within the region in general.

Management perceived that the level and incidence of computer-related crime within their organisations was minimal. Whereas the perception concerning the incidence of these crimes in the Eastern Cape was seen as high.

This supports the media view, that management believe such crimes will not occur in their organisations but in some one else's. This view could have disastrous results for management if they do not see computer-related crime as both a danger and a threat.

Those organisations that reported having experienced a computer-related crime tended to be more realistic in their assessments.

7.7 REPORTED COMPUTER-RELATED CRIMES

The most common types of crimes that respondents admitted to having had perpetrated within their organisations were :

- o the unauthorised use of equipment, and
- o the modification of programs, closely followed by
- o the denial of the use of information.

The invasion of privacy by the unauthorised access to data was seen to be a problem for the Eastern Cape region as a whole rather than for the individual organisations.

The modification of data and the disclosure of information appeared low on the list of actually committed computer-related crimes.

Having discussed the nature of computer-related crime in the initial stages of this report, it was discovered that specific properties peculiar to most computer environments make computer-related crime more attractive to potential criminals than non-computer fraud. It is an unfortunate fact that the computer lends itself to ingenious schemes of fraud and that the really cunning perpetrators are yet to be revealed. Most of the detected computer- related crimes appear to have been discovered through mere chance or luck.

Of concern is the fact that 29,6% of respondents acknowledged that they had experienced between 1 and 5 computer-related crimes within the last 18 months. This study did not investigate whether the reduction of risk of being a victim of such a crime is in any way related to the level and awareness of security.

This survey also indicated that management appear to be giving computer security a low level of importance.

The survey also identified that not all such crimes are being prosecuted. This could be attributed to the fact that South Africa has no specific computer crime legislation.

The survey also indicates that most of the companies in our sample appear to be vulnerable to computer-related crime in view of the low level of controls that they have implemented.

7.8 VALUE OF REPORTED COMPUTER-RELATED CRIMES

The popular notion that computer-related crimes tend to be insignificant was not supported by this survey. The survey, in fact, revealed that in terms of the magnitude and value of the crimes perpetrated, such crimes were, in fact, significant when expressed in monetary terms. The actual value of the losses reported ranged from R 65 000 to R 250 000 per incident. However, if these losses were to be expressed as a percentage of that organisations turnover or net profit, they would be seen to immaterial which might also indicate why these organisations preferred to follow the incident up internally rather than to become involved in public court cases.

Computer-related crimes are difficult to detect, very costly in terms of loss per incident, as borne out by the survey, and undoubtedly far more prevalent than the survey results indicate.

Computer-related criminals stand little chance of being detected, and if detected they are unlikely to be prosecuted. From the cases reported it would indicate that if such individuals are prosecuted, they are unlikely to be convicted.

7.9 AUDITORS ROLE IN DETECTING COMPUTER-RELATED CRIME

A greater knowledge of computer-related crime on the part of auditors is also important, if the majority of computer-related criminals are to be caught and punished. Though no one can hope to eliminate it completely, computer-related crime can be reduced by an awareness of the risks, and a readiness to implement plans to combat it.

Case histories indicate that the external auditor could not be held responsible for the discovery of all fraud and it was implied that this was management's responsibility. The courts have, in the mean-while, ruled that the external auditor should accept responsibility for detecting cases of computer-related fraud as they had been negligent in carrying out their tasks with the necessary care and skill. This did not resolve the question as to who should be held responsible for the prevention and detection of computer-related fraud.

Auditing pronouncements world-wide state that management should bear the main burden of responsibility for the prevention and the detection of computer-related crimes through their task of developing and maintaining adequate systems of internal control which thereby safeguard that organisation's assets. These pronouncements also state that the external

auditor's primary responsibility is to express an opinion as to the fairness of the financial statements. If these financial statements do not "fairly present" the financial position of the organisation because of undisclosed fraud, the external auditor will not be held responsible unless there had been failure to comply with generally accepted auditing standards. This relieves the external auditor of the primary responsibility for preventing and detecting computer-related fraud. The internal auditor, on the other hand, is given the responsibility for reviewing the accounting and internal control systems as laid down by management, thereby ensuring that the information received by management is accurate.

These survey results are in line with the auditing pronouncements and sought to answer the question which was initially posed, as to who is responsible for preventing and detecting computer-related crime.

7.10 CONCLUSION

The motivations of white collar crime, and of computer-related crime in particular, can be attributed to some extent to the attitude of society towards the criminal, who is often hailed as a genius, rather than condemned as a criminal. The average computer criminal gives credence to this hypothesis in that this person is usually a respected first-timer and usually feels that they have borrowed rather than stolen, or was doing it to beat the system. In addition, the reluctance on the part of the victims to prosecute the offender is a factor contributing to the risk of further frauds.

The three hypotheses defined for this study were :

HO^1 : Management perceive that they are solely responsible for detecting computer-related crime within their organisations.

The survey results supported this hypothesis.

HO^2 : Management perceive that they are assisted by their auditors in detecting computer-related criminal acts.

The survey indicated that the auditors have a role in the detection and prevention of computer-related crime.

Their role in the detection of computer-related crime is limited to their activities in being able to express an opinion on that organisation's financial statements.

The auditors role in the prevention of computer-related crime is seen as being in an advisory role to management in the ongoing development of that organisation's system of internal controls.

Management are seen as being solely responsible for detecting computer-related crime.

HO^3 : **Management perceive that they can rely on their auditors to detect computer-related criminal type acts.**

This was not supported by the survey.

The role of the auditors is a psychological one, whereby an independent outside organisation examines the accounting records and possibly detects any such computer-related crime during the course of their audit activities. The annual independent audit serves as a strong potential preventative measure as that organisation's staff are unaware of those areas that will be subjected to detailed scrutiny by the independent auditors.

Future research

This survey sought to identify management's perceptions on computer-related crime as well as the extent of any computer-related crime problem within the surveyed region. For future research a national survey would be useful in substantiating the results obtained from this local survey. The national survey could be extended to :

- o include additional details of perpetrators of computer-related crimes, such as qualifications, age, and sex
- o identify the method used to perpetrate the crime
- o obtain explanations as to why any computer-related crimes were not prosecuted
- o investigate whether the reduction of risk of being a victim of such a crime is in any way related to the level and awareness of security.

Recommendations

The following recommendations arise from this local survey.

Emphasis should be placed in bringing to management's attention that they are solely responsible for the prevention and detection of computer-related crime within their organisation. The individual roles within lower management, middle management, and senior management need to be defined that all may know what is expected of them and that all may work as a team in detecting and preventing computer-related crime within their organisation. Consideration should be given to utilising either the national press or national financial journals to disseminate this information.

Organisations experiencing computer abuse should be encouraged to prosecute the perpetrators of such crimes. Insurers should be encouraged to prosecute rather than to settle out of court. The fear that insurers have that where the crime is published, potential perpetrators would be able to refine and improve on the methods used in order to perpetrate another crime which would be more difficult to detect would be reduced if our legislation imposed severe fines and lengthy periods of imprisonment for all such crimes.

Consideration could be given to the maintenance of a national register of persons who have committed computer-related crimes. Currently the organisation that experiences a computer-related crime releases that employee, who then is able to perpetrate such crime at the next organisation that they are employed with. The unsuspecting organisation is unaware of this employees criminal potential.

The current deficiencies within the South African legislation relating to the prosecution of computer-related crime should be addressed as a matter of urgency.

BIBLIOGRAPHY

Auditing Practices Committee of The Institute of Chartered Accountants in England and Wales. 1984. Auditing in a Computer Environment.

Australian Society of Accountants, 1984. Auditing in an EDP Environment. Australian Accounting Research Foundation. Statement of Auditing Practice. No. 4. March.

Becker, J. 1978. Operational Guide to White-Collar Crime Enforcement on the Investigation of Computer Crime. Seattle, Washington: Battelles Law and Justice Centre.

Bequai, A. 1983. How to Prevent Computer Crime - A Guide for Managers. Washington, D.C.: John Wiley & Sons.

Boberg, P.Q.R. 1989. Aquilian Liability. The Law of Delicit. Cape Town : Juta & Company, vol I.

Burchell, E.M. Milton, J.R.L. & Burchell, J.M. 1982. General Principles of Criminal Law. South African Criminal Law and Procedure. Cape Town : Juta & Company, vol. I.

Bureau of Justice Statistics. 1984. Criminal Justice Resource Manual. Washington, D.C.: U.S. Department of Justice.

Clough, B. & Mungo, P. 1993. Approaching Zero. Data Crime and the Computer Underworld. St Ives Place, London: Clays Limited.

Cornwall, H. 1987. Data Theft. London: Heinemann.

Credo, P.W. Aiken & Carter, & Michels, J. 1985. Computer Crime in South Africa. Kelvin: Data Time.

Gallegos, F. Richardson, D. & Borthick, F. 1987. Audit and Control of Information Systems. New York.

IBM. 1992. Using Information Strategically. An IBM Position Paper. Poughkeepsie, New York: International Business Machines Information and Telecommunications Systems.

International Federation of Accountants. 1991. Auditing in an EDP Environment. International Standard on Auditing, no. 15. October.

International Federation of Accountants. 1991. Risk Assessment and Internal Control - EDP Characteristics and Considerations. International Statement on Auditing. October.

Kraus, L.I. & MacGahan, A. 1979. Computer Fraud and Countermeasures. Englewood Cliffs, New Jersey : Prentice Hall, Inc.

Lampson, B.L. 1977. A Note on the Confinement Problem. California: Xerox Palo Alto Research Centre.

Loeffler, S. 1986. Report of the Trustee of Equity Funding Corporation of America. Final report of the trustee. Washington, D.C. October 31.

Longenecker, J.G. 1979. Principles of Management and Organizational Behavior. Columbus, Ohio : Charles E. Merril Publishing Company.

Melamed, I.M. 1994. How to Fight Computer Crime. Proceedings. Port Elizabeth : BSS Management Services.

Miller, H. 1978. Manual for Prosecution of Computer-Related Crime. Atlanta, Georgia.

Milton, J.R.L. 1990. Common Law Crimes. South African Criminal Law and Procedure. Cape Town : Juta & Company, vol. II.

New Zealand Society of Accountants. 1986. Auditing in an EDP Environment. Auditing Guideline, no. 10. Wellington : Accounting Research and Standards Board. June.

Parker, D.B. Nycum, S.H. & Oura, S. 1973. Computer Abuse. Menlo Park, California: SRI International. Distributed by National Technical Information Service. Springfield, Virginia: U.S. Department of Commerce.

Parker, D.B. 1976. Crime by computer. New York: Charles Scribner.

Parker, D.B. 1979. Computer Abuse Assessment and Control Study. Final Report, Menlo Park, California: SRI International. March.

Parker, D.B. 1981. Computer Security Management. Reston, Virginia: Reston Publishing Company, Inc.

Parker, D.B. 1985. Computer Security Conference for Auditors. Proceedings. Cape Town: Old Mutual.

Perry, W.E. & Kuong, J.F. 1987. EDP Risk Analysis and Controls Justification. Wellesley Hills : Management Advisory Publications.

Ribicoff, A. 1979. Computer Abuse Control Bill. Press Release. January 25.

Schabeck, T.A. 1979. Computer Crime Investigation Manual. Madison, Wisconsin: Assets Protection.

Seidler, L.J., Epstein, F.A. & Epstein, M.J. 1977. The Equity Funding Papers. New York : John Wiley & Sons.

South African Institute of Chartered Accountants. 1989. Computer Fraud in the 1990s. The Information Technology Series. Johannesburg.

South African Institute of Chartered Accountants. 1992. The Auditor's Responsibilty to Detect and Report Illegal Acts, other Irregularities and Errors. Statement on Auditing Standards, no. 5. Johannesburg.

Stix, G. 1987. Guaging security risks. EDP Audit, Control & Security Newsletter. Virginia : Harold Weis Publishers, vol. 14, no. 9.

Stoner, J.A.F. & Freeman, R.E. 1992. Management. Englewoods Cliffs, New Jersey : Prentice-Hall, Inc.

U.S.A. U.S. Senate Committee on Government Operations. 1976. Problems Associated with Computer Technology in Federal Programs and Private Industry. Washington, D.C.: U.S. Government Printing Office.

U.S.A. U.S. Senate Committee on Government Operations. 1977. Staff Study of Computer Security in Federal Programs. Washington, D.C.: U.S. Government Printing Office.

U.S.A. U.S. Senate Subcommittee on Criminal Law and Procedures. 1978. Hearing on the Federal Computer Systems Protection Act (S1766). Washington, D.C.: U.S. Government Printing Office. June.

Wong, K.K. & Farquhur, W.F. 1987. Computer Fraud in the United Kingdom. Manchester : BIS Applied Systems.

CASES

Northern Office Micro Computers (Pty) Ltd v Rosenstein, 1981 4 123 (C).

APPENDIX A

CURRENT PRESS RELEASES RELATING TO COMPUTER CRIME

Mexican authorities bust software pirates

The Business Software Alliance (BSA) and the Mexican Computer Software Industry Association recently made major raids on four Mexican software pirates located in Mexico City's Electronics Plaza shopping area.

Following leads from Mexican users and complaints from Autodesk, Lotus Development and Microsoft, agents from the BSA and the Mexican Intellectual Property Institute (IMPI by its Spanish acronym) raided the offices of four companies that resell illegally copied software. After one of the raids, agents sequestered one PC and several boxes of disks with unauthorised software, which will be used as evidence.

One of the four companies has approached the IMPI to reach a settlement before the 10-day deadline to respond to piracy allegations, according to people familiar with the case. A final resolution from the IMPI action is due in six months.

The association said this is the first time that authorities have used trademark rather than copyright law to lead an enforcement action in Latin America. The alleged resellers are accused of selling hundreds of copies of popular PC software, such as Lotus 1-2-3 and Word for Windows, thereby infringing on trademarked goods.

The advantage of using trademark law in Mexico is that the trademark authority itself can inspect and prosecute, rather than a federal Mexican prosecutor.

Moreover, the penalties for trademark infringement include closure of a guilty business and higher fees, typically in the range of $3 000 to $27 000 for first-time offenders and double for second-time actions, said Richard Neff, a Los Angeles-based attorney and legal advisor to the BSA for Latin American affairs.

Computing SA, vol. 14, no. 6.
13 February 1995.

Software developers could go to prison

by MONICA SNELL

A US state is on the verge of passing a law that will make planting secret "time bombs" in software a criminal offence.

The state of Virginia's House of Delegates has passed the bill, and it now awaits the governor's signature.

A powerful Virginia corporation that was involved in a lawsuit with Computer Associates and almost had to stop operations when a "time bomb exploded" is said to have lobbied hard for the law.

"This bill is coming from a vindictive background ... It is a terrible idea," said Doug Jerger, VP of US industry representative, Information Technology Associationof America (ITAA), referring to a 1992 lawsuit between Newport News Shipbuilding and CA.

The lawsuit, which was settled out of court, began after Newport News reportedly used CA software on two mainframes when it had only paid a licence for one.

A CA spokesperson denied any connection between the bill and the prior suit.

ComputerWeek, vol. 18, no. 6.
20 February 1995.

IT industry must educate public on computer crime

The IT industry has its work cut out to change public perceptions about computer crime.

So said Peter Davies, president of the Computer Society of SA, in reaction to recent press reports about the alleged illegal electronic transfer of more than R4m from the State Pension Fund into a private bank account.

In papers before the court, a senior government official reportedly said it was difficult to stanch such outflows of money from state coffers because transfers "could be programmed into a computer".

Davies contends this particular official clearly has little or no understanding of how, and by whom, computer crime is committed. "Unfortunately, the gentleman in question is not alone. Judging from similar comments made in recent months, there are many people - some in senior positions - who are just as poorly informed.

"It is in the computer industry's own interest, therefore, to educate the public that people, not computers, commit computer crime. Computers are merely the tools - albeit sophisticated tools - with which people in positions of trust abuse the confidence placed in them.

"In addition it must be emphasised that computer systems can be made extremely secure, with comprehensive checks and controls to prevent unauthorised access and misuse of facilities. It follows, therefore, that only people who are both skilled and trustworthy should be allowed to develop information systems - all the more so if the systems are as critical as the one in question."

The Computer Society, he says, is actively working with other industry bodies, both locally and overseas, towards a qualification programme that will enable the Computer Society to guarantee that its members have such knowledge, skills and professional attitude, as will engender confidence in their services.

In addition, the society has an all-encompassing Code of Conduct, complemented by a Code of Practice, by which its members are expected to exercise their professional competence. Disciplinary action is taken against members who violate these codes. "The CSSA is totally committed to working with computer user organisations, government and other representative bodies to find ways to limit this type of white-collar crime to the minimum, and where it does occur, to be able to swiftly identify the culprits and take immediate action," he says.

Computing SA, vol. 14, no. 9.
6 March 1995.

US software bodies out to nail pirates

WASHINGTON, DC: The software industry last week filed its recommendations to the US Trade Representative of countries that ought to be targeted for special attention because of their high rates of sofware piracy.

The Business Software Alliance has targeted 42 countries for inadequate protection of US intellectual property, particularly computer software.

BSA recommends four countries be included on the "priority foreign country" list, the highest level short of official trade sanctions. Those countries are China, Bulgaria, Turkey, and Indonesia.

"Software piracy continues to flourish worldwide, significantly undermining growth and development," says Robert Holleyman, president of BSA. "Losses to the global industry are pegged at more than $12,8 billion."

BSA is putting a special spotlight on Indonesia this year. "Indonesia is particularly egregious with regard to computer software," said Kim Willard, BSA spokeswoman. "We have had an ongoing struggle with their government." BSA estimates Indonesia's piracy rate at 99% and losses to US publishers at over $92 million annually.

The Software Publishers Association, in its USTR filing, targets China, Russia and Thailand for particular attention. SPA estimates the piracy rate exceeds 90% in all three countries.

ComputerWeek, vol. 18, no. 6.
20 February 1995.

SPA reports loss to piracy of $8,8 bn

WASHINGTON, DC: The good news is that software piracy revenues are down, but the bad news is that the rate of piracy remains high. In a report which addresses an $8,8 billion loss during 1994 to the software industry, the Software Publishers Association (SPA) states the reduced piracy revenues reflect a reduction in software prices from 1993 to 1994.

Perhaps as alarming, these figures only include business software and exclude the illegal copying of operating systems, education, entertainment and/or personal productivity software. In its report, the SPA estimates 49% of the business software in use worldwide during 1994 is pirated.

Losses to the software industry did drop $1,9 billion, but at the same time the report shows the number of pirated units has increased 14%. Topping the list of countries with very high rates of piracy are China, Russia, and Thailand. Their piracy rates are 98%, 95% and 92%, respectively.

According to the SPA, a 98% piracy rate means only two out of every 100 units of software in use have been legally acquired. The exceedingly high rates led the SPA to cite all three countries in its 1994 Section 301 filing with the US Trade Representative. The association does credit the three countries with enacting copyright laws, but says the problem of enforcement has to be addressed.

Among Western European countries, France topped the list, with piracy losses amounting to $482 million, a figure which reflects what the SPA calls a disappointing decline in the piracy rate from 66% to 62%.

Switzerland and Finland, on the other hand, are among those countries with the lowest piracy rates in the world. On the Pacific Rim, Australia and New Zealand reduced their piracy rates by 25% and 32%, respectively.

The report also estimates the highest loss of revenue to software developers occurred in Japan where loss was down in 1994 to $1,31 billion from $1,66 billion in 1993. The SPA says Japan's piracy rate dropped by 15% to 56% for 1994, but the loss of revenue is mainly attributable to lower software prices.

ComputerWeek, vol. 18, no. 8.
6 March 1995.

Phone fraud ringleader pleads guilty

VIRGINIA: The European leader of an international ring of phone hackers has pleaded guilty to stealing thousands of telephone calling card numbers used to make $100-million in unauthorised long-distance calls.

Max Louarn, 22, of Palma de Mallorca, Spain, entered his plea in the US District Court to conspiracy and wire fraud charges in a case investigated by law enforcement agencies in the US, Britain and Spain.

Louarn's guilty plea is the second in the case. Earlier this month, Andy Gaspard, 23, of Woodbridge, Virginia, entered a plea of guilty to trafficking in the calling card codes issued by telephone companies.

According to court documents, Louarn, Gaspard and a third defendant, Omar Flatekval, 20, of Northumberland, England, stole and sold between 40 000 and 100 000 code numbers. Flatekval was arrested in Britain.

Louarn faces up to five years in prison on each of two counts and a minimum $250 000 fine.

Louarn admitted taking delivery in Spain of about 40 000 calling codes stolen from AT&T, GTE and Bell Atlantic that Gaspard, working for Cleartel Communications, a long-distance company, stole.

Cooperating with the US Secret Service, Gaspard helped lure Louarn to the US in September, for a visit to turn over a new load of card numbers. The Secret Service videotaped a conversation in which Louarn claimed to make $18 000 a month on the scheme. Then the agents arrested Louarn.

ComputerWeek, vol. 17, no. 43.
7 November 1994.

Prosecuting software pirates

by LISA ARMSTRONG in Silicon Valley

Underground bulletin boards are no longer immune to the normal channels of law enforcement. With the aid of the US FBI, the first software pirate has been arrested in the US on charges of conspiracy and criminal copyright infringement.

Richard D Kenadek of Millbury, Massachusetts was arrested and charged by the United States Attorney for Massachusetts after an FBI investigation and raid which netted over 200 copyrighted software programs available for illegal downloading from Kenadek's 'Davy Jones Locker'.

Kenadek had been running the bulletin board from his home in Millbury. Pirating of commercial software through the operation of clandestine computer bulletin boards seriously jeopardises the investment of money and personnel which software companies put into the development of new programs, said US attorney Donald Stern. "We need to be clear: pirating is illegal."

Stern's Economic Crimes Unit is prosecuting the case.

The indictment alleges that subscribers solicited by Kenadek to Davy Jones Locker had been able to pay a fee in return for access privileges to the bulletin board. Online access allowed subscribers to download pirated software from Davy Jones Locker; subscribers were then urged to contribute their own copyrighted software for illegal distribution.

Allegedly, contributing subscribers received additional credit time to download the software they wanted.

If the SPA wins its lawsuit, Kenadek could face copyright infringement fines of up to $100 000.

The US government charges could net him six years in prison and $275 000 in fines as well as the forfeiture of all of the computer equipment used to run Davy Jones Locker.

Edutech International

ComputerWeek, vol. 17, no. 42.
31 October 1994.

BSA backs busts on illegal software

The Business Software Alliance's efforts to catch software pirates are showing in Finland.

The police knocked on the door of Teamsystems Tampere Oy earlier this year after Microsoft and WordPerfect had reported that the company was using their software illegally. Now the MD and two members of the board are charged with having sold dozens of microcomputers containing illegally copied Novell, WordPerfect and Microsoft programs.

The case of another company, JJ-Piirto Oy, is currently up in Helsinki district court. JJ-Piirto is accused of having illegally copied and used Microsoft, Autodesk and WordPerfect software.

Computing SA, vol. 13, no. 40.
17 October 1994.

Software Alliance awarded $260 000 piracy settlement

WASHINGTON, DC: Utica Enterprises, a leading auto parts manufacturer in the Detroit area, has agreed to pay the Business Software Alliance $260 000 to settle a software copyright infringement suit.

Under the settlement, Utica agrees to pay the fee to resolve claims that it had illegally copied software products published by Aldus, Autodesk, Lotus, Microsoft and WordPerfect.

BSA brought the suit following a report to its anti-piracy hot-line and after earlier attempts to negotiate an information settlement, according to the Washington-based trade group that represents personal computer software makers.

In addition to the payment, Utica has agreed to destroy all unlicensed copies and purchase legal software to meet its needs. The company is also developing a software management program to ensure future compliance with copyright law.

"Utica regrets that this situation has occurred," said attorney Pat Lanadt of Plunkett & Cooney, representing Utica. "Utica has taken immediate and positive steps, however, to ensure future compliance with software copyright requirements. For example, Utica has instituted a corporate policy modeled after BSA's software code of ethics, and is currently establishing a programme to teach all Utica employees about the importance of proper software management."

Bob Kruger, BSA's enforcement director, said: "Unfortunately, the situation at Utica is not unique. Despite efforts of the industry to draw attention to this issue, many companies still fail to comply with software copyright requirements."

Kruger said BSA is investigating a number of Great Lakes region companies that may face fines even higher than the $260 000 hit on Utica.

"It is important for all organisations to understand that software piracy is against the law and that violators are subject to severe criminal and civil penalties."

ComputerWeek, vol. 17, no. 42.
31 October 1994.

Hacker 'breaks in' at Rhodes

By STEUART WRIGHT

A HACKER has been using Rhodes University's link to the international computer network Internet to launch attacks on the United States space administration's computers.

Rhodes computing services director Dave Wilson said: "Someone broke in from somewhere on the Internet and launched attacks on sites in the United States. Stanford and Rutgers Universities and Nasa (National Aeronautics and Space Administration) were involved."

He said the American-based computer Emergency Response Unit, which monitors break-ins on Internet, notified the university about two weeks ago.

However, the hacker, believed to be operating from Thailand or New Zealand, has apparently been using the Rhodes system without authorisation since April 8.

"There is no actual damage caused to the Rhodes system. The person used our machine as a stepping stone to where he could have caused damage, but he couldn't get in."

He explained that once into the university's computer, the hacker might have left a "backdoor" open to make repeated entry easier.

To shut out the illegal user, the computer's operating systems were reinstalled at the weekend and security measures tightened so the university could be alerted quickly in future, Mr Wilson said.

"We have had minor incidents since we got a direct international link a couple of years ago, but this is the first serious intrusion by a hacker," he said.

"More incidents are likely as the number of users on Internet grows.

"A lot of machines are quite open to this kind of attack because people are not aware of the dangers."

Mr Wilson had "no idea" why Rhodes was chosen. — Ecna

Eastern Province Herald,
Tuesday, May 16, 1995

APPENDIX B

MANAGEMENT PERCEPTIONS OF COMPUTER-RELATED CRIME

UNIVERSITEIT
VISTA
UNIVERSITY

PORT ELIZABETH CAMPUS
PRIVATE BAG X613
PORT ELIZABETH 6000
REPUBLIC OF SOUTH AFRICA
TEL (041) 64-4200
FAX (041) 64-2859

PORT ELIZABETHKAMPUS
PRIVAATSAK X613
PORT ELIZABETH 6000
REPUBLIEK VAN SUID-AFRIKA
TEL (041) 64-4200
FAKS (041) 64-2859

September 1994

Dear Sir

This study is undertaken to obtain up to date information on external audit and company management perceptions of computer-related crime. The objectives are to :

1. investigate management's perception of what comprises a computer-related crime
2. ascertain what measures management have implemented to prevent computer- related criminal acts
3. determine the extent and magnitude of computer-related crimes committed within the Eastern Cape and to provide an analysis of these findings.

Attached to this questionnaire is an annexure describing specific terms used within this questionnaire.

Your participation in this study will remain confidential and all information recorded will be destroyed once the study is completed.

Please ensure that all questions are answered. A reply paid envelope is enclosed for your convenience. Responses on or before 15 September 1994 will be highly appreciated.

Please provide me with your name and postal address if you would like to receive a complimentary copy of the findings from this study.

THANK YOU FOR YOUR CO-OPERATION IN THE COMPLETION OF THIS QUESTIONNAIRE.

Yours faithfully

PROFESSOR P. P. VOGES

THE PERCEPTIONS OF MANAGEMENT ON COMPUTER-RELATED CRIME

Office Use Only

3
4 [1]

1 Capacity in which you are filling out this form?

(1)		5

2 How long have you been involved in this management position?

(1)		7

3 In which sector are you classified? Please circle the most important sector if you are involved in more than one.

	(1) Manufacturing	(2) Wholesale	(3) Retail	(4) Finance	(5) Banking	(6) Service	(7) Other (specify)

8

4 How many employees do you have in your organisation?

(1)	Number of employees	12

5 Would you classify the following as being components of computer-related crime?
(1 = yes, 2 = no, 3 = don't know)

(1)	The introduction of fraudulent information into a computer system	1 2 3	13
(2)	Unauthorised use of computer facilities	1 2 3	14
(3)	The alteration or destruction of information	1 2 3	15
(4)	The stealing by electronic means of money, financial instruments, property, services, or valuable data	1 2 3	16
	Any other activity that you might consider as falling within the term of computer-related crime. Please describe:		
(5)			17
(6)			18

6 How significant is the use of a computer in the following criminal activities?
(1 = very important, 2 = important, 3 = slightly important, 4 = unimportant, 5 = don't know)

(1)	Destruction of equipment and supportive facilities	1 2 3 4	5	19
(2)	Destruction of data	1 2 3 4	5	20
(3)	Manipulation of information / data	1 2 3 4	5	21
(4)	Falsification of records	1 2 3 4	5	22
(5)	Covering up fraudulent activities	1 2 3 4	5	23
(6)	Unauthorised use of confidential information	1 2 3 4	5	24
(7)	Misrepresentation of the quality and extent of computer technology actually in use	1 2 3 4	5	25
	Other - please describe below:			
(8)		1 2 3		28
(9)		1 2 3		31
(10)		1 2 3		34

7 How prevalent are the methods listed below, in your organisation and in the Eastern Cape in general? (refer Addendum for brief description of each item):
1 = frequently, 2 = seldom, 3 = never, 4 = don't know

		Your Organisation		Eastern Cape		
(1)	Data diddling	1 2 3	4	1 2 3	4	30
(2)	Trojan horses	1 2 3	4	1 2 3	4	36
(3)	Salami techniques	1 2 3	4	1 2 3	4	40
(4)	Superzapping	1 2 3	4	1 2 3	4	42
(5)	Trap doors	1 2 3	4	1 2 3	4	44
(6)	Logic bombs	1 2 3	4	1 2 3	4	46
(7)	Asynchronous attacks	1 2 3	4	1 2 3	4	48
(8)	Scavenging	1 2 3	4	1 2 3	4	50
(9)	Data leakage	1 2 3	4	1 2 3	4	52
(10)	Piggybacking and impersonation	1 2 3	4	1 2 3	4	54
(11)	Wire tapping	1 2 3	4	1 2 3	4	56
(12	Simulation and modelling	1 2 3	4	1 2 3	4	58
(13)	Hacking	1 2 3	4	1 2 3	4	60
(14)	Planting of viruses	1 2 3	4	1 2 3	4	62
(15)	Invasion of privacy by unauthorised access to data	1 2 3	4	1 2 3	4	64
(16)	Fraud	1 2 3	4	1 2 3	4	66
	Other: please describe below					
(17)		1 2 3		1 2 3		70
(18)		1 2 3		1 2 3		74
(19)		1 2 3		1 2 3		78

Office Use Only

3 4 [2]

8 The methods listed above result in the following actions being perpetrated against other computer services, computer equipment, computer programs or data. If any of the following acts were perpetrated in your organisation within the last 18 months, please indicate the number of instances.

		number	
(1)	Modification of programs		5
(2)	Modification of data		6
(3)	Destruction of equipment		7
(4)	Disclosure of information		8
(5)	Unauthorised use of equipment		9
(6)	Denial of use of information		10
	Other: please describe below		
(7)			13
(8)			16
(9)			19

9 How important would you rate the responsibility of the following groups to detect and prevent computer-related criminal acts?
1 = unimportant, 2 = fairly important, 3 = very important, 4 = extremely important

		detection	prevention	
(1)	Top management	1 2 3 4	1 2 3 4	21
(2)	Middle management	1 2 3 4	1 2 3 4	23
(3)	Operational management	1 2 3 4	1 2 3 4	25
(4)	External auditors	1 2 3 4	1 2 3 4	27
(5)	Computer department	1 2 3 4	1 2 3 4	29

10 If management is responsible for the detection and prevention of computer-related criminal acts, then who in your organisation is the most important person entrusted with this function?

	Job Title	Department	
(1)			33

11 How suitable are the following in detecting computer-related crime?
(1 = very poor, 2 = fair, 3 = good, 4 = excellent, 5 = don't know)

(1)	Internal audit	1 2 3 4 5	34
(2)	External audit	1 2 3 4 5	35
(3)	Control procedures	1 2 3 4 5	36
(4)	Fellow workers	1 2 3 4 5	37
(5)	Customer complaints	1 2 3 4 5	38
(6)	Investigation after suspected foul play	1 2 3 4 5	39
(7)	Chance / accident	1 2 3 4 5	40
	Other - please describe below:		
(8)		1 2 3 4	43
(9)		1 2 3 4	46
(10)		1 2 3 4	49

12 Describe the preventative measures that your organisation has implemented to minimise the incidence of computer-related crime.

(1)		51
(2)		53
(3)		55
(4)		57
(5)		59
(6)		61

13. Has your organisation experienced a computer-related criminal act in the last 18 months? If the crime was perpetrated by a group, please use the most senior person for the job title and department question.

Please supply the following information:

details of crime				who perpetrated the crime									who detected the crime		prosecution	
	type of criminal act	instances in last 18 months	estimated monetary value of loss	number of perpetrators		employees		contractors		customers		other - describe	job title	department	Yes	No
				male	female	job title	department	yes	no	yes	no					
1																
2																
3																

Office Use Only

			3
	3		4

	details					perpetration		detection		
	type	no.	value	male	female	job title	department	job title	department	prosecution
1	6	8	11	13	15	17	19	21	23	24
2	26	28	31	33	35	37	39	41	43	44
3	46	48	51	53	55	57	59	61	63	64

COMPUTER-RELATED CRIME METHODS

In the study of computer-related crime a thorough understanding is essential of the various methods of using computer technology to perpetrate such a crime. Most technologically sophisticated computer-related crimes will use one or more of these methods. These methods result in one of the following acts being perpetrated against other computer services, computer equipment, computer programs or data:

- modification
- destruction
- disclosure
- unauthorised use of
- denial of use of.

1. Data Diddling
   This is the simplest, safest, and most common method used in computer-related crime. It involves changing data before or during their input to computers. The changing can be done by anybody associated with or having access to the processes of creating, recording, transporting, encoding, examining, checking, converting, and transforming data that ultimately enter a computer.

2. Trojan Horse
   The Trojan horse method is the covert placement of computer instructions in a program so that the computer will perform unauthorised functions but usually still will allow the program to perform its intended purposes.

3. Salami Technique
   An automated form of crime involving the theft of small amounts of assets from a large number of sources is identified as a salami technique (taking small slices without noticeably reducing the whole). One salami method in a financial system is known as the "round down" fraud.

4. Superzapping
   Superzapping derives its name from Superzap, a macro/utility program used in most IBM computer centres as a systems tool. Any computer centre that has a secure computer needs a "break glass in case of emergency" type computer program that will bypass all controls in order to modify or disclose any of the contents of the computer.

5. Trap Doors
   In the development of large applications and computer operating systems, it is the practice of programmers to insert debugging aids that provide breaks in the code for insertion of additional code and intermediate output capabilities. The design of computer operating systems attempts to prevent both access to them and the insertion of code or modification of such code. Consequently, system programmers will sometimes insert code that allows a compromise of these requirements during the debugging phases of implementation and later when the system is being maintained and improved. These facilities are referred to as trap doors. Normally, trap doors are eliminated in the final editing but sometimes they are overlooked or purposely left in to facilitate ease of making further access and modification.

6. Logic Bombs
   A logic bomb is a computer program executed at appropriate or periodic times in a computer system that determines conditions or states of the computer that facilitate the perpetration of an unauthorised, malicious act. A logic bomb can be programmed to trigger an act based on any specified condition or data that may occur or be introduced. Logic bombs are usually placed in the computer system using the Trojan horse technique.

7. Asynchronous Attacks

Asynchronous attack techniques take advantage of the asynchronous functioning of a computer operating system. The majority of computer operating systems function asynchronously based on the services that must be performed for the various computer programs presently in memory waiting to be executed. For example, several jobs may simultaneously call for output reports to be printed. The operating system actually stores these requests and, as resources become available, performs them in the order in which resources are available to fit that request or according to an overriding priority schedule. Therefore, rather than executing requests in the order they are received, the system performs them asynchronously based on available resources. There are highly sophisticated methods of confusing the operating system to allow it to violate the isolation of one job from another.

8. Scavenging

Scavenging can be defined as a method of obtaining information that may be left in or around a computer system after the execution of a job. Scavenging can be done by searching for residual data left in disc storage within the computer after the job has been executed.

9. Data Leakage

A number of known computer-related crimes involved the removal of data from computer systems or computer facilities. The removal of data presents the most dangerous exposure to the perpetrator. His technical act may be well hidden in the computer; however, to convert it to economic gain, he must get the data out of the computer system. Output reports are subject to examination by computer operators and other data processing personnel. Several techniques can be used to leak data from a computer system. The perpetrators may be able to hide the sensitive data in otherwise innocuous looking output reports. This could be done by adding to blocks of data. In more sophisticated ways the data could be interspersed with otherwise innocuous data. An even more sophisticated method might be to encode data to look like something different than it is.

10. Piggybacking and Impersonation

Piggybacking and impersonation can be done either physically or electronically. Physical piggybacking is a method for gaining access to controlled access areas controlled by either electronically or mechanically locked doors. Success of this method of piggybacking is dependent upon the quality of the access control mechanism as well as the alertness of authorised persons in resisting co-operation with the perpetrator. Electronic piggybacking can take place in an on-line computer system where individuals are using terminals, and identification is verified automatically by the computer system. When a terminal has been activated, the computer authorises access. Compromise of the computer can take place when a hidden computer terminal is connected to the same line and used when the legitimate user is not using his terminal. The computer will not be able to differentiate or recognise the two terminals, but senses only one terminal and one authorised user. Piggybacking can also be accomplished when the user does not sign off when his task on the terminal has been completed thus leaving the terminal in an active state or leaving the terminal in a state where it assumes that the user is still active.

11. Wire Tapping

The potential for wire tapping grows rapidly as more computers are connected to communication facilities and increasing amounts of electronically stored assets are transported from computer to computer over communication circuits. Interception of microwave and satellite communications represents even greater difficulty because of the complexity and cost of the equipment to perform such an operation. In addition, to further complicate matters, there might be active detection facilities built into the communications network.

12. Simulation and Modelling

A computer can be used as either a tool or as an instrument in a crime. The computer can be used for planning or to control the crime. Complex white- collar crime often requires the use of a computer because of its sophistication. An existing process can be simulated on a computer or a planned method could be modelled to determine its possible success.

APPENDIX C

DESCRIPTIVE STATISTICS - VARIABLES AND ROW PERCENTAGES

APPENDIX C

DESCRIPTIVE STATISTICS - VARIABLE AND ROW PERCENTAGES

1. CAPACITY OF THE PERSON COMPLETING THE QUESTIONNAIRE

Capacity	Freq.	Perc.
Audit Partner	2	7.4%
Computer Partner	0	0.0%
Chief Executive Officer	1	3.7%
City Treasurer	1	3.7%
Managing Director	2	7.4%
Financial Director	4	14.8%
Director	2	7.4%
Member Close Corporation	1	3.7%
Deputy Director Finance	1	3.7%
IS Manager	3	11.1%
Financial Manager	2	7.4%
Admin Manager	1	3.7%
Internal Audit Manager	4	14.8%
Regional Manager Finance	1	3.7%
Financial Accountnt	1	3.7%
Cost Accountant	1	3.7%
TOTAL	27	100.0%

2. PERIOD EMPLOYED IN THAT CAPACITY

SAMPLE SIZE = 27

VARIABLE	N	Mean	S.D.	Median	Min.	Max.
HowLong	27	5.44	4.85	4.00	1.00	20.00
Employ	27	1013.78	1828.12	308.00	9.00	7000.00

HowLong	Freq.	Perc.
1	3	11.1%
2	5	18.5%
3-5	11	40.7%
6-10	4	14.8%
11	4	14.8%
TOTAL	27	100.0%

3. SECTOR

Sector	Freq.	Perc.
Manufacturing	12	44.4%
Wholsale	1	3.7%
Retail	0	0.0%
Finance	2	7.4%
Banking	0	0.0%
Service	7	25.9%
Distribution	0	0.0%
Education	1	3.7%
Local Government	3	11.1%
Wagering	1	3.7%
TOTAL	27	100.0%

4. NUMBER OF EMPLOYEES

Employ	Freq.	Perc.
1 - 50	5	18.5%
51 - 100	2	7.4%
101- 500	9	33.3%
501-1000	3	11.1%
1001+	8	29.6%
TOTAL	27	100.0%

5. COMPONENTS OF A COMPUTER-RELATED CRIME

ROW PERCENTAGES

	Yes	No	DontKnow	TOTAL
5.1 Introduction of fraudulent information	26 96.3%	1 3.7%	0 0.0%	27 100.0%
5.2 Unauthorised use of computer facilities	22 81.5%	4 14.8%	1 3.7%	27 100.0%
5.3 Alteration/destruction of information	23 85.2%	4 14.8%	0 0.0%	27 100.0%
5.4 Stealing by electronic means	24 88.9%	3 11.1%	0 0.0%	27 100.0%

6. THE SIGNIFICANCE OF A COMPUTER IN BEING ABLE TO COMMIT A CRIMINAL ACTIVITY

Question	N	Mean	S.D.	Median	Min.	Max.
6.1	25	41.32	38.89	33.00	0.00	100.00
6.2	27	79.04	32.25	100.00	0.00	100.00
6.3	27	91.41	21.81	100.00	0.00	100.00
6.4	27	75.37	28.67	67.00	0.00	100.00
6.5	27	70.41	29.80	67.00	0.00	100.00
6.6	26	66.62	32.78	67.00	0.00	100.00
6.7	23	40.57	37.62	33.00	0.00	100.00

ROW PERCENTAGES

6.1 Destruction of equipment

VeryImp	Import	SlightIm	Unimp	DontKnow	TOTAL
5 20.0%	5 20.0%	6 24.0%	9 36.0%	0 0.0%	25 100.0%

6.2 Destruction of data

VeryImp	Import	SlightIm	Unimp	DontKnow	TOTAL
17 63.0%	5 18.5%	3 11.1%	2 7.4%	0 0.0%	27 100.0%

6.3 Manipulation of information

VeryImp	Import	SlightIm	Unimp	DontKnow	TOTAL
22 81.5%	4 14.8%	0 0.0%	1 3.7%	0 0.0%	27 100.0%

6.4 Falsification of records

VeryImp	Import	SlightIm	Unimp	DontKnow	TOTAL
13 48.1%	9 33.3%	4 14.8%	1 3.7%	0 0.0%	27 100.0%

6.5 Covering up fraudulent activities

VeryImp	Import	SlightIm	Unimp	DontKnow	TOTAL
11 40.7%	9 33.3%	6 22.2%	1 3.7%	0 0.0%	27 100.0%

6.6 Unauthorised use of confidential information

VeryImp	Import	SlightIm	Unimp	DontKnow	TOTAL
11 40.7%	5 18.5%	9 33.3%	1 3.7%	1 3.7%	27 100.0%

6.7 Misrepresentation of quality and extent of computer technology actually in use

VeryImp	Import	SlightIm	Unimp	DontKnow	TOTAL
4 14.8%	5 18.5%	6 22.2%	8 29.6%	4 14.8%	27 100.0%

7. PREVALENCE OF METHODS FOR COMMITTING A COMPUTER-RELATED CRIME

Question	N	Mean	S.D.	Median	Min.	Max.
7.1 Own	24	18.75	24.73	0.00	0.00	50.00
7.1 EP	10	50.00	33.33	50.00	0.00	100.00
7.2 Own	23	2.17	10.43	0.00	0.00	50.00
7.2 EP	10	30.00	25.82	50.00	0.00	50.00
7.3 Own	24	2.08	10.21	0.00	0.00	50.00
7.3 EP	12	37.50	31.08	50.00	0.00	100.00
7.4 Own	24	0.00	0.00	0.00	0.00	0.00
7.4 EP	10	35.00	24.15	50.00	0.00	50.00
7.5 Own	23	2.17	10.43	0.00	0.00	50.00
7.5 EP	10	30.00	25.82	50.00	0.00	50.00
7.6 Own	23	2.17	10.43	0.00	0.00	50.00
7.6 EP	10	30.00	25.82	50.00	0.00	50.00
7.7 Own	23	4.35	20.85	0.00	0.00	100.00
7.7 EP	10	15.00	24.15	0.00	0.00	50.00
7.8 Own	24	6.25	16.89	0.00	0.00	50.00
7.8 EP	12	33.33	24.62	50.00	0.00	50.00
7.9 Own	25	16.00	23.80	0.00	0.00	50.00
7.9 EP	10	35.00	24.15	50.00	0.00	50.00
7.10 Own	24	4.17	14.12	0.00	0.00	50.00
7.10 EP	13	23.08	25.94	0.00	0.00	50.00
7.11 Own	22	2.27	10.66	0.00	0.00	50.00
7.11 EP	12	33.33	24.62	50.00	0.00	50.00
7.12 Own	23	4.35	14.41	0.00	0.00	50.00
7.12 EP	10	25.00	26.35	25.00	0.00	50.00
7.13 Own	24	4.17	14.12	0.00	0.00	50.00
7.13 EP	11	31.82	25.23	50.00	0.00	50.00
7.14 Own	24	20.83	25.18	0.00	0.00	50.00
7.14 EP	12	41.67	19.46	50.00	0.00	50.00
7.15 Own	24	22.92	25.45	0.00	0.00	50.00
7.15 EP	12	58.33	35.89	50.00	0.00	100.00
7.16 Own	26	9.62	20.10	0.00	0.00	50.00
7.16 EP	12	37.50	31.08	50.00	0.00	100.00

ROW PERCENTAGES

7.1 Data Diddling

	Freq		Seldom		Never		DontKnow		TOTAL	
Own	0	0.0%	9	33.3%	15	55.6%	3	11.1%	27	100.0%
EP	2	8.0%	6	24.0%	2	8.0%	15	60.0%	25	100.0%

7.2 Trojan horse

	Freq		Seldom		Never		DontKnow		TOTAL	
Own	0	0.0%	1	3.7%	22	81.5%	4	14.8%	27	100.0%
EP	0	0.0%	6	24.0%	4	16.0%	15	60.0%	25	100.0%

7.3 Salami Techniques

	Freq		Seldom		Never		DontKnow		TOTAL	
Own	0	0.0%	1	3.7%	23	85.2%	3	11.1%	27	100.0%
EP	1	4.0%	7	28.0%	4	16.0%	13	52.0%	25	100.0%

7.4 Superzapping

	Freq		Seldom		Never		DontKnow		TOTAL	
Own	0	0.0%	0	0.0%	24	88.9%	3	11.1%	27	100.0%
EP	0	0.0%	7	28.0%	3	12.0%	15	60.0%	25	100.0%

7.5 Trap doors

	Freq		Seldom		Never		DontKnow		TOTAL	
Own	0	0.0%	1	3.7%	22	81.5%	4	14.8%	27	100.0%
EP	0	0.0%	6	24.0%	4	16.0%	15	60.0%	25	100.0%

7.6 Logic bombs

	Freq		Seldom		Never		DontKnow		TOTAL	
Own	0	0.0%	1	3.7%	22	81.5%	4	14.8%	27	100.0%
EP	0	0.0%	6	24.0%	4	16.0%	15	60.0%	25	100.0%

7.7 Asynchronous attacks

	Freq		Seldom		Never		DontKnow		TOTAL	
Own	1	3.7%	0	0.0%	22	81.5%	4	14.8%	27	100.0%
EP	0	0.0%	3	12.0%	7	28.0%	15	60.0%	25	100.0%

7.8 Scavenging

	Freq		Seldom		Never		DontKnow		TOTAL	
Own	0	0.0%	3	11.1%	21	77.8%	3	11.1%	27	100.0%
EP	0	0.0%	8	32.0%	4	16.0%	13	52.0%	25	100.0%

7.9 Data Leakage

	Freq		Seldom		Never		DontKnow		TOTAL	
Own	0	0.0%	8	29.6%	17	63.0%	2	7.4%	27	100.0%
EP	0	0.0%	7	28.0%	3	12.0%	15	60.0%	25	100.0%

7.10 Piggybacking and Impersonation

	Freq		Seldom		Never		DontKnow		TOTAL	
Own	0	0.0%	2	7.4%	22	81.5%	3	11.1%	27	100.0%
EP	0	0.0%	6	24.0%	7	28.0%	12	48.0%	25	100.0%

7.11 Wire Tapping

	Freq		Seldom		Never		DontKnow		TOTAL	
Own	0	0.0%	1	3.7%	21	77.8%	5	18.5%	27	100.0%
EP	0	0.0%	8	32.0%	4	16.0%	13	52.0%	25	100.0%

7.12 Simulation and Modelling

	Freq		Seldom		Never		DontKnow		TOTAL	
Own	0	0.0%	2	7.4%	21	77.8%	4	14.8%	27	100.0%
EP	0	0.0%	5	20.0%	5	20.0%	15	60.0%	25	100.0%

7.13 Hacking

	Freq		Seldom		Never		DontKnow		TOTAL	
Own	0	0.0%	2	7.4%	22	81.5%	3	11.1%	27	100.0%
EP	0	0.0%	7	28.0%	4	16.0%	14	56.0%	25	100.0%

7.14 Planting of Viruses

	Freq		Seldom		Never		DontKnow		TOTAL	
Own	0	0.0%	10	37.0%	14	51.9%	3	11.1%	27	100.0%
EP	0	0.0%	10	40.0%	2	8.0%	13	52.0%	25	100.0%

7.15 Invasion of Privacy by Unauthorised Access to Data

	Freq		Seldom		Never		DontKnow		TOTAL	
Own	0	0.0%	11	40.7%	13	48.1%	3	11.1%	27	100.0%
EP	4	16.0%	6	24.0%	2	8.0%	13	52.0%	25	100.0%

7.16 Fraud

	Freq		Seldom		Never		DontKnow		TOTAL	
Own	0	0.0%	5	18.5%	21	77.8%	1	3.7%	27	100.0%
EP	1	4.0%	7	28.0%	4	16.0%	13	52.0%	25	100.0%

8. COMPUTER-RELATED CRIMES PERPETRATED WITHIN LAST 18 MONTHS

Question	N	Mean	S.D.	Median	Min.	Max.
8.1	25	0.20	1.00	0.00	0.00	5.00
8.2	25	0.08	0.28	0.00	0.00	1.00
8.3	25	0.00	0.00	0.00	0.00	0.00
8.4	25	0.04	0.20	0.00	0.00	1.00
8.5	25	0.28	1.06	0.00	0.00	5.00
8.6	25	0.16	0.62	0.00	0.00	3.00
8.7	0					
8.8	0					
8.9	0					
Total	27	0.70	1.96	0.00	0.00	9.00

ROW PERCENTAGES

	0		1		2+		TOTAL
8.1 Modification of Programs	24	96.0%	0	0.0%	1	4.0%	25 100.0%
8.2 Modification of Data	23	92.0%	2	8.0%	0	0.0%	25 100.0%
8.3 Destruction of Equipment	25	100.0%	0	0.0%	0	0.0%	25 100.0%
8.4 Disclosure of Information	24	96.0%	1	4.0%	0	0.0%	25 100.0%
8.5 Unauthorised use of Equipment	23	92.0%	0	0.0%	2	8.0%	25 100.0%
8.6 Denial of use of Information	23	92.0%	1	4.0%	1	4.0%	25 100.0%

9. DETECTION AND PREVENTION OF COMPUTER-RELATED CRIMINAL ACTS

VARIABLE	N	Mean	S.D.	Median	Min.	Max.
9.1 Det	27	56.74	31.91	67.00	0.00	100.00
9.1 Pre	25	84.00	29.11	100.00	0.00	100.00
9.2 Det	27	69.26	22.59	67.00	33.00	100.00
9.2 Pre	25	82.72	23.83	100.00	33.00	100.00
9.3 Det	27	81.56	26.68	100.00	0.00	100.00
9.3 Pre	25	85.36	27.37	100.00	0.00	100.00
9.4 Det	27	61.70	40.04	67.00	0.00	100.00
9.4 Pre	25	57.32	39.18	67.00	0.00	100.00
9.5 Det	27	87.63	28.03	100.00	0.00	100.00
9.5 Pre	25	89.32	23.09	100.00	33.00	100.00

ROW PERCENTAGES

9.1 Senior Management

	Unimp	FairImp	VeryImp	ExtrImp	TOTAL
Det	2 7.4%	11 40.7%	7 25.9%	7 25.9%	27 100.0%
Pre	1 4.0%	3 12.0%	3 12.0%	18 72.0%	25 100.0%

9.2 Middle Management

	Unimp	FairImp	VeryImp	ExtrImp	TOTAL
Det	0 0.0%	5 18.5%	15 55.6%	7 25.9%	27 100.0%
Pre	0 0.0%	3 12.0%	7 28.0%	15 60.0%	25 100.0%

9.3 Operational Management

	Unimp	FairImp	VeryImp	ExtrImp	TOTAL
Det	1 3.7%	2 7.4%	8 29.6%	16 59.3%	27 100.0%
Pre	1 4.0%	2 8.0%	4 16.0%	18 72.0%	25 100.0%

9.4 External Auditors

	Unimp	FairImp	VeryImp	ExtrImp	TOTAL
Det	5 18.5%	6 22.2%	4 14.8%	12 44.4%	27 100.0%
Pre	5 20.0%	6 24.0%	5 20.0%	9 36.0%	25 100.0%

9.5 Computer Department

	Unimp	FairImp	VeryImp	ExtrImp	TOTAL
Det	1 3.7%	3 11.1%	1 3.7%	22 81.5%	27 100.0%
Pre	0 0.0%	3 12.0%	2 8.0%	20 80.0%	25 100.0%

10.1 PERSON ENTRUSTED WITH THE DETECTION AND PREVENTION OF COMPUTER-RELATED CRIMES

Question 10 (a)	FREQ.	PERC.
Chief Executive Officer	1	4.2%
Financial Director	1	4.2%
IS Director	5	20.8%
Director	1	4.2%
Member Close Corporation	1	4.2%
IS Manager	6	25.0%
Financial Manager	2	8.3%
Administration Manager	1	4.2%
Internal Audit Manager	1	4.2%
Comp Security Manager	1	4.2%
Systems Manager	1	4.2%
Financial Accountant	2	8.3%
Cost Accountant	0	0.0%
Systems Accountant	1	4.2%
TOTAL	24	100.0%

10.2 DEPARTMENT IN WHICH THE PERSON RESPONSIBLE FOR THE PREVENTION AND DETECTION OF SUCH CRIMES IS EMPLOYED

Question 10 (b)	FREQ.	PERC.
Finance	10	41.7%
Computer Security	1	4.2%
City Engineers	1	4.2%
IS Department	6	25.0%
Administration	1	4.2%
Internal Audit	1	4.2%
Senior Manager	4	16.7%
EDP Audit	0	0.0%
TOTAL	24	100.0%

11. SUITABILITY OF DEPARTMENT IN DETECTING COMPUTER-RELATED CRIME

Question	N	Mean	S.D.	Median	Min.	Max.
11.1	27	72.89	26.30	67.00	33.00	100.00
11.2	26	43.54	28.07	33.00	0.00	100.00
11.3	27	87.74	18.75	100.00	33.00	100.00
11.4	27	65.59	26.98	67.00	0.00	100.00
11.5	26	61.65	20.61	67.00	33.00	100.00
11.6	27	66.70	29.34	67.00	0.00	100.00
11.7	24	30.50	35.36	33.00	0.00	100.00

ROW PERCENTAGES

11.1 Internal Audit

VeryPoor	Fair	Good	ExcelInt	DontKnow	TOTAL
0 0.0%	6 22.2%	10 37.0%	11 40.7%	0 0.0%	27 100.0%

11.2 External Audit

VeryPoor	Fair	Good	ExcelInt	DontKnow	TOTAL
4 14.8%	12 44.4%	8 29.6%	2 7.4%	1 3.7%	27 100.0%

11.3 Control Procedures

VeryPoor	Fair	Good	ExcelInt	DontKnow	TOTAL
0 0.0%	1 3.7%	8 29.6%	18 66.7%	0 0.0%	27 100.0%

11.4 Fellow Workers

VeryPoor	Fair	Good	ExcelInt	DontKnow	TOTAL
2 7.4%	3 11.1%	16 59.3%	6 22.2%	0 0.0%	27 100.0%

11.5 Customer Complaints

VeryPoor	Fair	Good	ExcelInt	DontKnow	TOTAL
0 0.0%	7 25.9%	16 59.3%	3 11.1%	1 3.7%	27 100.0%

11.6 Investigation after Suspected Foul Play

VeryPoor	Fair	Good	ExcelInt	DontKnow	TOTAL
1 3.7%	7 25.9%	10 37.0%	9 33.3%	0 0.0%	27 100.0%

11.7 Chance/Accident

VeryPoor	Fair	Good	ExcelInt	DontKnow	TOTAL
11 42.3%	7 26.9%	3 11.5%	3 11.5%	2 7.7%	26 100.0%

12. PREVENTATIVE MEASURES IMPLEMENTED TO MINIMISE THE INCIDENCE OF COMPUTER- RELATED CRIME

		FREQ.	PERC.
1	Segregation/division of duties	3	16.7%
4	Restricted access - programs	4	22.2%
5	Restricted access - premises	2	11.1%
6	Password control	5	27.8%
7	User codes & passwords	4	22.2%
9	Access controls & limits	7	38.9%
10	Authorisation levels	1	5.6%
13	User logs/profile lists	2	11.1%
14	Daily control checks & procedures	4	22.2%
15	Monthly control checks & procedures	1	5.6%
16	Timeous management information	1	5.6%
17	Control procedures	4	22.2%
18	Monitoring of computer processing	1	5.6%
20	Change control procedures	1	5.6%
21	Computer system audits	1	5.6%
22	Internal audits	4	22.2%
23	Code of conduct	1	5.6%
24	Quality of staff	1	5.6%
25	Software security packages	1	5.6%
28	Disk storage evaluations	1	5.6%
30	External audit	2	11.1%
34	Fellow workers	1	5.6%
40	Name of person recorded originating report	1	5.6%
44	Well designed systems	1	5.6%
	TOTAL	18	100.0%