THE MANAGEMENT OF INFORMATION SECURITY AND CONTROL AT KYNOCH FERTILIZER (PTY) LTD

Louis Cyril Henry Fourie

B.A., Lis. Teol., D.Th.

Dissertation submitted in partial fulfilment of the requirements for the degree

MASTER IN BUSINESS ADMINISTRATION

at the Potchefstroom Business School

Potchefstroomse Universiteit vir Christelike Hoër Onderwys

Study leader : Dr S.P. van der Merwe

Potchefstroom

November 1998

Dedicated to

Louie
Christiaan
and
Janlo

ACKNOWLEDGEMENTS

I would like to express my gratitude and appreciation to:

- My study leader, Dr S.P. van der Merwe for his invaluable assistance, excellent guidance and friendship.
- The Potchefstroom Business School for providing an excellent academic background.
- The members of my study group for their devotion and hard work.
- All family, friends and colleagues for continued interest.
- Kynoch Fertilizer (Pty) Ltd - specifically Mr Andries Jacobs, previous manager business process support, and all respondents who completed the questionnaires.
- My wife, Louie, for her perseverance, encouragement and understanding during the entire M.B.A. course, as well as a million cups of coffee.
- My children Christiaan and Janlo for their love and support.
- God, who gave me the persistence – "let the words of my mouth, and the meditation of my heart, be acceptable in thy sight, O Lord, my rock and my redeemer" (Psalm 19:14).

UITTREKSEL

DIE BESTUUR VAN INLIGTINGSEKURITEIT EN BEHEER TE KYNOCH FERTILIZER (EDMS) BPK

deur

L.C.H. FOURIE

STUDIELEIER: DR. S.P. VAN DER MERWE

FAKULTEIT: EKONOMIESE EN BESTUURSWETENSKAPPE

GRAAD: MAGISTER IN BESIGHEIDSADMINISTRASIE

Die groeiende misbruik van inligtingstegnologie en die verhoogde afhanklikheid van rekenaar tegnologie en stelsels het die vereistes ten opsigte van inligtingsekuriteit dramaties verhoog. Ongelukkig is daar dikwels vanaf bestuur 'n gevoel van apatie teenoor inligtingsekuriteit, wat lei tot 'n ad hoc benadering tot inligtingsekuriteit en gevolglike inligting en finansiële verliese.

Die hoofdoel van hierdie studie was dus om die huidige status van inligtingsekuriteit te Kynoch Fertilizer (Edms) Bpk te bepaal en om praktiese en uitvoerbare bestuursaanbevelings ten opsigte van 'n inligtingsekuriteit raamwerk en multivlak plan te doen wat huidige en toekomstige inligting bedreigings sal weerstaan.

Om bogenoemde doel te verwesenlik, en om 'n gesonde teoretiese agtergrond tot die probleem te vestig, is eerstens 'n literatuurstudie ten opsigte van drie hoof aspekte van inligtingsekuriteit en beheer gedoen. Die resultate is:

- Die belangrikste inligtingsekuriteit bedreiginge wat tans ondervind word is eksterne bedreiginge, hardeware misbruik, vermomming, pes programme, ontwykings, aktiewe misbruik, passiewe misbruik, onaktiewe misbruik, en indirekte misbruik.

- Alhoewel dit nie moontlik is om 'n algehele veilige inligtingstelsel te bou en alle bedreiginge en probleme te elimineer nie, is dit wel moontlik om die impak en besigheid ontwrigting te minimaliseer deur administratiewe, fisiese, prosedurele, operasionele, inligtingstelsel, stelsel ontwikkeling en laaste uitweg beheermaatreëls te implementeer.

- Die inligtingsekuriteit maatreëls moet egter behoorlik bestuur word deur die implementering van 'n inligtingsekuriteit beleid, doelwitte, standaarde en riglyne; sekuriteit vereistes; 'n beheerstrategie; en 'n inligtingsekuriteit beheerraamwerk.

Tweedens is 'n empiriese veldondersoek by die sentrale streek van Kynoch Fertilizer (Edms) Bpk, 'n groot kunsmis vervaardiger in Potchefstroom, gedoen. Drie gestruktureerde vraelyste oor inligtingsekuriteit was die belangrikste komponent van hierdie veldondersoek. Die resultate van die drie vraelyste in statisties verwerk. Gebaseer op die literatuurstudie oor die ideale inligtingsekuriteit en beheer situasie én die empiriese resultate, was dit moontlik om die gaping, probleem areas en spitsvrae rondom inligtingsekuriteit en beheer by Kynoch Fertilizer (Edms) Bpk te bepaal. Die navorsing het duidelik aangetoon dat daar talle areas is waar ruimte vir verbetering bestaan.

Om die huidige inligtingsekuriteit gaping wat by Kynoch Fertilizer (Edms) Bpk bestaan te oorbrug, is 'n praktiese en uitvoerbare inligtingsekuriteit raamwerk en plan aanbeveel. Alhoewel 'n algehele veilige inligtingstelsel te Kynoch Fertilizer (Edms) Bpk nie haalbaar mag wees nie, kan die waardevolle inligtingsbate in 'n groot mate beskerm word. Inligtingsekuriteit mag soms 'n reis sonder einde wees, maar kan wel 'n koste effektiewe oplossing tot inligtingsekuriteit bedreigings verskaf indien dit behoorlik geïmplementeer word.

Sleutelterme: Bestuur, inligting, sekuriteit, inligtingsekuriteit, sekerheid, beheer, Kynoch, rekenaar, bedreiginge, stelsels, en tegnologie.

ABSTRACT

THE MANAGEMENT OF INFORMATION SECURITY AND CONTROL AT KYNOCH FERTILIZER (PTY) LTD

by

L.C.H. FOURIE

STUDY LEADER: DR. S.P. VAN DER MERWE

FACULTY: ECONOMIC AND MANAGEMENT SCIENCES

DEGREE: MASTER IN BUSINESS ADMINISTRATION

The growing misuse of information technology and the increased dependence on computer technology and systems heightened the requirements for information security. Unfortunately there often is a feeling of apathy towards information security by management, which leads to an ad hoc approach to information security and resultant information and financial losses.

The main objective of the study thus was to determine the current state of information security at Kynoch Fertilizer (Pty) Ltd and to provide practical and feasible managerial recommendations for an information security framework and multilevel plan that will withstand the current and future information security threats.

To realise this objective, and to establish a sound theoretical background to the problem, firstly, a literature study was done regarding three major aspects of information security and control. The results were:

- The major information security threats currently experienced are external threats, hardware misuse, masquerading, pest programs, bypasses, active misuse, passive misuse, inactive misuse, and indirect misuse.

- Although it is not possible to build a completely secure information system and to eliminate all threats and problems, it is possible to minimise the impact and business disruption by implementing administrative, physical, procedural, operational, information systems, systems development and last resort control measures.

- The information security controls should be managed properly by the implementation of an information security policy, objectives, standards and guidelines; security requirements; a control strategy; and an information security control framework.

Secondly, an empirical field investigation was done at the central region of Kynoch Fertilizer (Pty) Ltd, a large fertiliser manufacturer in Potchefstroom, by means of a field study of which three structured questionnaires on information security were an important component. The results of the three questionnaires were processed statistically. Based on the literature study concerning the ideal information security and control situation, and the empirical results, it was possible to determine the gap, problem areas and issues of information security and control at Kynoch Fertilizer (Pty) Ltd. The research clearly showed that numerous areas for improvement exist.

To bridge the present information security gap that exists at Kynoch Fertilizer (Pty) Ltd a practical and feasible information security framework and plan was recommended. Although a completely secure information system at Kynoch Fertilizer (Pty) Ltd may not be attainable, the valuable information asset can to a large extent be protected. Information security may sometimes be a journey without end, but can provide a cost-effective solution to information security threats if implemented properly.

Key words: Management, information, security, control, Kynoch, computer, threats, systems, and technology.

TABLE OF CONTENTS

THE MANAGEMENT OF INFORMATION SECURITY AND CONTROL AT KYNOCH FERTILIZER (PTY) LTD

ANNEXURES

Annexure A: Cover letter

Annexure B: General computer user questionnaire

Annexure C: Departmental and functional heads questionnaire

Annexure D: Business process support questionnaire

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

NATURE AND SCOPE OF THE STUDY

1.1 INTRODUCTION

The 1990s are characterised by continual and rapid change in technology. One specific aspect that is having a major impact on everyday life is the phenomenon generally known as the information explosion. Information has in fact become the essential ingredient for profits and success (Du Toit, 1992:9). In the bid to use this massive volume of information economically and effectively, computers increasingly played a more significant role. This increased dependence on computer technology and computer-based information systems in organisations to enable diverse business activities, has redefined corporate risk and thus necessitated closer scrutiny of security practices and procedures to offset the risk inherent in giving more people access to computer systems (Lubbe & Armstrong, 1995:19; Pottas, 1995:vi,3; Von Solms, 1993:1).

Organisations rely on information every day to serve their customers, monitor their transactions, manufacture their products and to make key decisions. Requirements for security have escalated to the protection of a myriad of autonomous and integrated information systems, data and information residing on mainframes, minicomputers, servers, workstations and personal computers (Scott, 1996:1; Eloff, 1980:1). It is therefore necessary that the confidentiality, integrity and availability of information should be ensured on all levels (Menzies, 1993:164-165).

This urgent necessity for information security is also found in the highly competitive manufacturing world. This study will therefore closely study information security and control at Kynoch Fertilizer (Pty) Ltd, a large and diversified manufacturing company, in order to develop a multilevel security plan, practical frame of management and an implementing strategy for information security an control.

1.2 PROBLEM STATEMENT

Despite management claims that information is one of the most valuable and strategic corporate assets (Pfleeger, 1989:299; Von Solms, 1993:1; compare Clarke, 1976:1; Davis & Olson, 1987:216; Du Toit, 1992:7; Christoffersson, *et al.*, 1988:1)[1], there is often not much pressure from executive level or adequate funding to ensure that information stored on computer systems is protected from bumbling, break-ins, electronic fraud, viruses, and natural disasters (compare Louw, 1990:213; Pfleeger, 1989:2; Rilley, 1981:5; Thibodeau, 1997). Many organisations do not implement an active information security plan, and when implemented it is often done half-heartedly (Van Dyk, 1990:18). It is also true that management often conceal the truth about the status of information security in their organisations (Stang, 1992:16). Although they are well aware of the shortcomings and dangers they rationalise and believe their own fabrication (Highland, 1993:2).

Linked to this apathy towards security by senior management, De Ru (1992:3) pointed out, is the growing concern regarding the ability of current tools, methods, procedures, solutions, and human resources to meet the information security challenges and issues confronting management in the years to come (compare also Pfleeger, 1989:xix; Witten, 1990:105; against Clement, 1992:1).[2] While the use of information technology is increasing, misuse and security risks associated with the deployment of information technology are increasing even faster and often results in huge financial losses (Rilley, 1981:2-3; Wong & Watt, 1990:1-2). Industrial espionage, fraud, crime and subterfuge are escalating in frequency and in adverse impact on victim organisations (Wong & Watt, 1990:2). It is also a well-known fact that computer crimes are becoming more sophisticated (Holton, 1996).

Besides all the above-mentioned problems, normal operating conditions and natural disasters (fire, water, and power failures) pose their own risks. Taken together with inherent flaws of fourth and fifth generation languages[3] with respect to data control and validation, the

---

[1] Also compare the empirical findings of Norton (1984:90) that although security was considered by management to be important, controls to ensure security had been given a low priority or even no consideration at all.

[2] Also see the findings of the study of Ernst & Young (1997:3).

[3] Compare for instance the use of ActiveX to create an applet that searches the host computer for Quicken. If it finds the package, it creates a transaction order requesting the transfer of money from the owner's account to the account of the thief. Various reports also indicated security problems regarding Java and JavaScript (Fisher, 1998a).

powerfulness of search engines[4], audit trail and error recovery, as well as the increased network sharing with outside organisations, office automation, electronic mail, electronic data interchange, and unattended operation, it is quite clear that top management can no longer ignore the security of the valuable information asset (compare Denning, 1990:iii-iv; Wong & Watt, 1990:15-20). If it is born in mind that in South Africa legislation concerning hacking is almost non-existent and that the computer crime division of the South African Police Services is understaffed and under-skilled, it becomes evident that most hackers go undetected and unprosecuted (Campling, 1997:1). Information security can thus not remain a technical issue, delegated to technical specialists, but will have to become a business issue, addressed by corporate executive management (Wong & Watt, 1990:20).

This urgency for the addressing of information security by senior management is furthermore highlighted by the inherent danger of the continuing departure from traditional mainframe computing to departmental computing, distributed platforms, decentralised security, the "openness" of today's systems architectures,[5] greater accessibility, interconnectivity, networks, and a large scale connection to the relatively insecure Internet (Claassen, 1994:1-1; Eloff, 1995:39; Heydenrych, 1996:16; Menaugh, 1997; Smith, 1996; Sundaram, 1998).

Recent studies done in South Africa by the consulting company Ernst and Young (1996; 1997) support the above-mentioned threats to information security. The following statistics regarding causes of information loss, presented in table 1.1, came to light in their studies:

---

[4] Search engines such as Yahoo, Alta Vista and Lycos are so powerful that doing a search for keywords such as "root" and "passwd" will return back a few stray /etc/passwd or etc/group files, located on systems that have poor Web configurations (Fisher, 1998b).

[5] For a thorough discussion of the security problems concerning open distributed systems, see the thesis of Claassen (1994).

Table 1.1: Causes of information loss

	1995	1996
Inadvertent errors	23%	47%
Lack of systems or telecommunications availability	21%	46%
Viruses	38%	28%
Internal malicious acts	15%	18%
Natural disasters	10%	18%
External malicious acts	5%	13%
Industrial espionage	-	13%

The major network security concerns that organisations in South Africa have are presented in table 1.2.

Table 1.2: Network concerns (1996)

NETWORK CONCERNS (1996)	
Unauthorised access by way of external remote dial-in methods	81%
Network security	78%
Loss of message integrity	74%
Tampering or interference with intended operation of the network	72%
Inability to identify network users	72%
Loss of message confidentiality	71%

Ernst & Young (1996:12; 1997:5-6,11)

From the above statistics a few conclusions regarding information security can be made:

- Information security risks are on the rise.
- Information losses continue to mount.
- The primary causes for the losses were inadvertent errors and a lack of systems or telecommunications availability. A recent study involving 2400 companies in The United States of America found that 65% of the money lost in computer-related incidents originated not from malice, but from simple user errors and omissions. This finding stresses the information security problem than can be created by employee ignorance (Lowe, 1994:17; compare Stang, 1992:32-34).

- Employees are the greatest threat to information security.
- Losses due to virus attacks are the only aspect that decreased.
- Network concerns are relatively high probably because of inadequate incident monitoring and planned incident responses (Ernst & Young, 1997:9).

The studies by Ernst & Young (1996:2-14; 1997:1-13) also found:

- Information security awareness is relatively strong, but actions not.
- Management deems information security to be important.
- The use of information technology is increasing, but the security risks associated with technology deployment are increasing at a greater pace.
- Protection measures are inadequate.
- Most organisations do not have a planned incident response to crises or a formal incident response team.
- Many organisations do not have a business continuity plan in place or have not tested it.
- Lack of human resources, tools and solutions are serious obstacles to information security.
- The Internet remains unproven and unsecured.
- Distributed computing exacerbates the issues of control over security.
- Although inadvertent errors are a major contributor to information losses, the importance placed on security awareness through training is very low.

Because of the above-mentioned aspects, it is of the utmost importance that information security is addressed in every organisation. Alexander (1995:31,33), however, pointed out that while information security is important, security measures that are onerous or cumbersome often end up being circumvented by legitimate users of the network in order to get their work done. Because of this, usability - or "user friendliness" - in security features should always be borne in mind (Avolio & Ranum, 1997).

1.3 OBJECTIVES OF THE STUDY

1.3.1 PRIMARY OBJECTIVE

The main objective of this study is to provide practical and feasible managerial recommendations and guidelines for the implementation of a cost effective information security framework and multilevel plan that will withstand the current and future information security threats to one of the most valuable assets of Kynoch Fertilizer (Pty) Ltd, namely information.

1.3.2 SECONDARY OBJECTIVES

To realise the above mentioned primary objective the following secondary objectives will be pursued:

- To establish the main factors, key issues and problems that influence information security and control.
- To delineate current trends and solutions in information security and control.
- To assess the management of information security and control.
- To determine the overall state of information security at the central region of Kynoch Fertilizer (Pty) Ltd, for example strategy, policy, security plan, structures, implementations and controls, and to measure it against the ideal information security situation.
- To make recommendations regarding the improvement of information security and control at Kynoch Fertilizer (Pty) Ltd in order to fill the gap between the ideal level of information security and the current level.

1.4 SCOPE OF THE STUDY

1.4.1 FIELD OF STUDY

The study will concentrate on the various aspects of computerised and non-computerised information security and control, including vulnerabilities, threats, risks, countermeasures and the management of information security and control.

1.4.2 GEOGRAPHIC DELIMITATION

The research will be undertaken at the head office and factory of the central region of Kynoch Fertilizer (Pty) Ltd. Kynoch Fertilizer (Pty) Ltd is situated in the industrial area of Potchefstroom and is a division of AECI. It is a modern company that has established itself as an international supplier of a variety of fertiliser products.

Kynoch is regarded as one of the largest businesses in the Potchefstroom area with an annual turnover of approximately R761 267 million for the 1997 financial year. Detail information regarding the organisation and its background will be given in chapter two.

1.5 RESEARCH METHODOLOGY

In pursuing the above-mentioned objectives, two approaches will be used:

1.5.1 LITERATURE STUDY

In order to establish a sound theoretical background to the problem, an in depth analysis, evaluation and integration of the different aspects relating to information security and control will be conducted by *inter alia* paying attention to:

- Authoritative people in the field of information security and control.
- Standard works on information security and control, although some of them date before 1990.
- The latest and most relevant literature on information security and control.
- The analysis and interpretation of recent research results concerning information security in South Africa.

The literature study will concentrate on three major aspects of information security and control, namely:

- The various information security risks, threats, vulnerabilities and problems.
- The solutions and countermeasures to prevent and limit the impact of these threats and vulnerabilities.

- The management of information security and control.

This theoretical knowledge, based on the literature study, will be used to determine the ideal state concerning information security and control, and to develop the various questionnaires that will be used in the empirical investigation.

1.5.2 EMPIRICAL FIELD INVESTIGATION

The second approach will be to do an empirical field investigation at the central region of Kynoch Fertilizer (Pty) Ltd to determine the current situation regarding information security at the company. This process will entail the following aspects:

1.5.2.1 Data gathering

For the gathering of data use will be made of survey questionnaires (Huysamen, 1994:128-133). The questionnaires will strive to assist a gap analysis between the requirements of future information security and control (the ideal situation) as was determined by the literature study and the present information security situation at Kynoch Fertilizer (Pty) Ltd.

The following steps will be followed to collect the data:

1.5.2.1.1 Development and composition of the questionnaires

Based on the important issues gathered from the literature study, the questionnaires will strive to determine the current state of information security and control at Kynoch Fertilizer (Pty) Ltd by making use of related questions that will measure the importance of various aspects of information security and control. The eventual aim is to realise the objectives of the study.

The reliability of these draft questionnaires will then be tested by means of a pilot study. In this pilot study the questionnaires will be distributed to five computer users at Kynoch Fertilizer (Pty) Ltd, as well as the manager of the business process support department. Indistinct and ambiguous questions will thus be adapted if necessary to ensure intelligibility and reliability.

The final questionnaires will again be checked with the manager of the business process support department at Kynoch Fertilizer (Pty) Ltd and amended if necessary.

1.5.2.1.2 Structuring of the questionnaires

An introductory letter to explain the importance and goal of the study will accompany the questionnaires (annexure A). The three questionnaires will be divided into five sections, namely:

- Section A: biographic and general information of the respondents (annexure B).
- Section B: general information security, microcomputer security and viruses (general employees) (annexure B).
- Section C: general information security, microcomputer security and viruses (management) (annexure C).
- Section D: detailed questions for information technology personnel regarding various aspects of information security, as well as controls (annexure D).
- Section E: summarised rating of the level of information security of various aspects (annexure C and D).

A four point Likert scale will be used for most of the statements of sections B, C, D and E (Huysamen, 1994:133-136).

1.5.2.1.3 Distribution of the questionnaires

The final questionnaires will be furnished to the total population of computer users of the central region of Kynoch Fertilizer (Pty) Ltd in Potchefstroom, including management and information technology specialists. This will be done by personal delivery and will be followed up by telephone calls and the personal collection of the completed questionnaires to ensure a good response rate.

Where more information will be needed, the questionnaires will be followed up by interviews to clarify answers.

1.5.2.2 Editing and recording of the data

The gathered data will be edited carefully to eliminate questionable data (Steyn *et al.*, 1994:3). After the data has been edited it will be captured on computer in a Statistica for Windows 4.5 database.

1.5.2.3 Analysis of the data

The results of the survey will be processed statistically and will be subjected to statistical analysis, namely descriptive statistics. Descriptive statistics involves the organising and summarising of collected numerical data by means of tables (for example frequency distributions), graphs and the calculation of descriptive criteria to indicate the inherent tendencies (central tendency and dispersion) and characteristics of the recorded data (Lind & Mason, 1994:5-6, 22, 58).

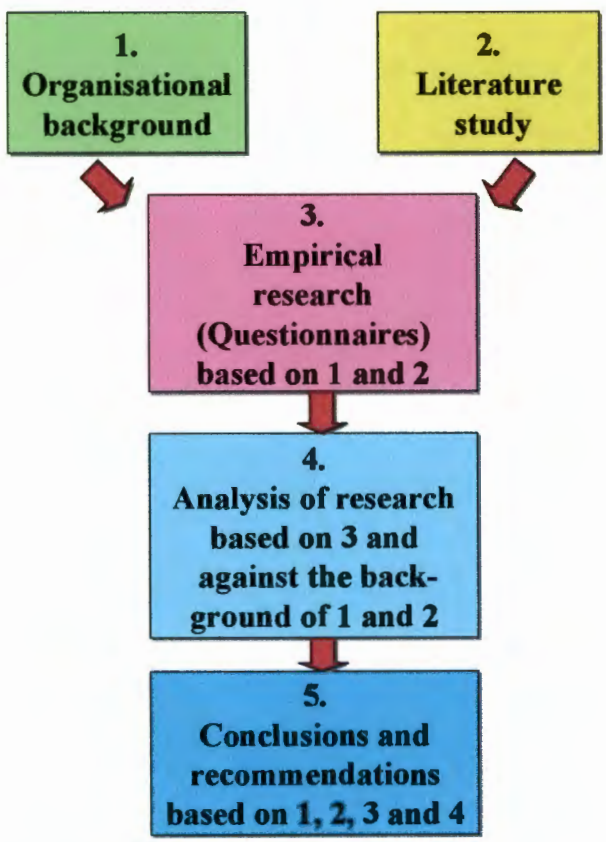
1.5.2.4 Conclusions and recommendations

The results of the statistical analysis will eventually be used to make certain conclusions and recommendations with regard to information security and control at Kynoch Fertilizer (Pty) Ltd as stipulated in the primary and secondary objectives.

1.5.3 SUMMARY OF THE RESEARCH METHODOLOGY

The research methodology is graphically illustrated in figure 1.1.

Figure 1.1: Research methodology



From figure 1.1 it is clear that the organisational background and literature study will be used as basis for the development of the questionnaires and the empirical study. The results of the empirical research will be analysed and interpreted against the organisational background and literature study before conclusions and recommendations will eventually be made.

1.6 LIMITATIONS OF THE STUDY

Because of the extent of the topic, the research will be limited to a study of information security and control in the central region of Kynoch Fertilizer (Pty) Ltd, more specifically the head office and factory in Potchefstroom. Although the possibility exists that the results may be representative of the information security situation in South Africa and other manufacturing companies, the results of this study are only representative of Kynoch Fertilizer (Pty) Ltd. Where applicable, reference will be made to a correlation between the results of information security studies done in South Africa and the results of Kynoch Fertilizer (Pty) Ltd.

Although the total information resource covers all information handling systems, manual and computerised, formal and informal, the main focus or attention of this dissertation will concern formal computerised information systems, as it is this area where the greatest vulnerability and security risk lies.

Despite the fact that attention was paid to the various formal security models, it was not included in the study, because in the light of the above-mentioned objectives, a detailed discussion of logical mathematical models do not fall within the scope of the study.[6]

Formal verification, where the operating system is reduced to a "theorem" and then proved, is often regarded as a very precise method of analysing information security, but will not be employed in this study because of its extent and the use of specialised computer programs, namely theorem provers.

---

[6] For a thorough discussion of the various logical security models, for example the monitor model, information flow model, access matrix model,, the Bell-LaPadula model, Biba model, Graham-Denning model, the lattice model, the high-water-mark model, the schematic protection model, the Harrison-Ruzzo-Ullman model (HRU model), the take-grant model, the send-receive model, the Path Context Model (PCM), and the expert systems based security model (EXMOD), see Claassen (1994:4-1 to 4-33), Edwards (1988), Pfleeger (1989: 243-258) and Van Zyl (1990).

1.7 TERMINOLOGY CLARIFICATION

Security: Security is the securement and protection of assets and property against threats, exposure and accidental or intentional harm, including destruction of computer hardware and software, physical loss of data, deception of computer users, disclosure or modification of data, or the deliberate invasion of databases by unauthorised individuals (Parker, 1996).

Information security: Information security refers to the technological safeguards and managerial procedures which can be applied to the whole computer system, information resources and services to ensure the protection of the organisational information assets (Martin, 1973:5; Rilley, 1981:34; Von Solms, 1993:2; Wong & Watt, 1990:23).

Control: Control refers to the methods, policies and organisational procedures that are used to safeguard assets and to ensure the integrity of inputs, processing and outputs of an information system (Lay *et al.*, 1994:356-357; Laudon & Laudon, 1998:635).

Information: Information is any input (for example data) that has the potential to be processed intellectually or cognitively to have meaning (Du Toit, 1992:3).

Data: Data is a portrayal of facts, concepts or instructions in a formalised way in order that it may be communicated, interpreted or processed by human or mechanical means (Du Toit, 1992:3).

It is important to note that the terms "information" and "data" are often used interchangeably in the field of information security, and refer to all data regardless of its physical form (Du Toit, 1992:4; compare also Van der Spuy, 1971:27).

1.8 LAYOUT OF THE STUDY

In order to achieve the objectives defined above, the deployment and contents of the various chapters are as follows:

Chapter two introduces the organisation that will be studied in the empirical research. The background of the organisation, present security situation and responsibility of management are discussed. The chapter is concluded with a few remarks on the causal factors to the study.

In **chapter three** the results of the literature study on information security and control regarding the different kinds of vulnerabilities and threats to which computer systems are prone, as well as how these vulnerabilities are exploited, is presented. The literature study thus relates to the factors that are important in information security and control and discusses certain aspects relating to developments in the information security field that could be of use in the recommendation phase of the study.

In **chapter four** attention is paid to effective countermeasures and controls to prevent attacks on systems, as well as to ensure reliable operation of systems and integrity of stored information. A synergistic approach of several control measures is recommended to minimise the impact of security threats and business interruption.

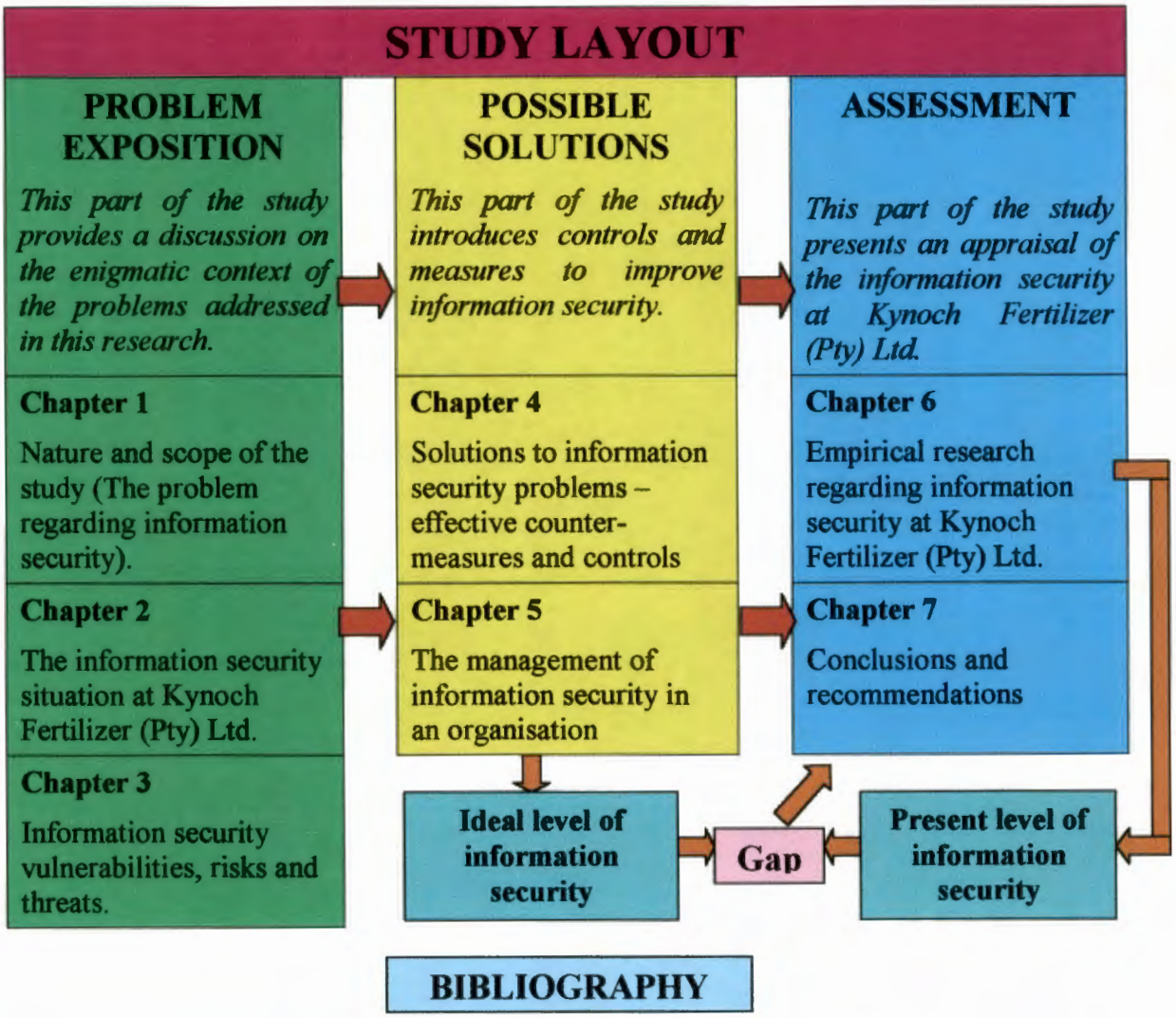
Chapter five addresses the subject of the management of information security in an organisation. The responsibility, policies, standards and guidelines are discussed, whereafter an information security management framework is conceptualised.

Chapter six contains the results of the empirical research. The information gathered in the literature study is used to develop and structure a questionnaire that will measure the gap between the present and ideal information security set-up. The questionnaire will be applied to all relevant computer users at Kynoch Fertilizer (Pty) Ltd. The second part of the chapter contains the statistical analysis and results.

Chapter seven contains the conclusions regarding the results of the empirical research, as well as recommendations and an information security framework and plan to improve information security and control at Kynoch Fertilizer (Pty) Ltd.

The layout of the study and chapters is schematically illustrated in figure 1.2.

Figure 1.2: Layout of the study



1.9 SUMMARY

The study is required to provide an answer to a very serious problem being experienced world wide, namely the threatening of information security and control. This will be achieved by means of a literature study that provides a background against which the empirical study will be done and on the basis of which the questionnaires will be formulated. The questionnaires will measure the current level of information security at Kynoch Fertilizer (Pty) Ltd, which will be compared with the requirements of the ideal information security plan and system established during the literature study. Clear guidelines and recommendations for the implementation of an effective information security framework and plan that would meet future requirements

regarding information security at Kynoch (Pty) Ltd. will eventually be made against the background of the literature study, as the gap between the ideal and current level of information security becomes apparent.

Whoever said, "crime doesn't pay" obviously hadn't heard about computer crime!

Anonymous

CHAPTER 2

THE COMPANY BEING RESEARCHED AND CAUSAL FACTORS TO THE STUDY

2.1 INTRODUCTION

The problems with information security and control outlined above will be specifically studied at the hand of a manufacturing organisation, namely the central region of Kynoch Fertilizer (Pty) Ltd. Kynoch Fertilizer (Pty) Ltd is one of the market leaders in the fertiliser industry in South Africa and produces a rich variety of fertiliser products in the solid and liquid fertiliser industry.

This chapter will therefore give a brief introduction to Kynoch Fertilizer (Pty) Ltd. After a brief historical overview and background, the organisational structure, information systems and technology, and the present information security situation will be discussed.

The second part of the chapter will be devoted to the organisation specific causal factors that lead to the study.

2.2 THE COMPANY

2.2.1 HISTORICAL OVERVIEW OF KYNOCH FERTILIZER (PTY) LTD

George Kynoch became involved in the arms industry in 1853. After destruction of his Birmingham factory by an explosion, a new factory was build at Witton. This factory, called "Kynoch Works", soon became the second largest producer of ammunition in Britain with agencies all over the world. In 1888 he emigrated to South Africa and opened branches in Johannesburg, Kimberley, Port Elizabeth (head office) and Pretoria, and agencies at Potchefstroom, Barberton, Middelburg (Transvaal), Makwassie, Chrissiemeer, Bergendal, Heidelberg (Transvaal), Rustenburg, Klerksdorp, Bloemhof, Lydenburg and Jacobsdal. In 1891 George Kynoch died (Anon., 1995a:1).

In 1895 a team of German carpenters and bricklayers arrived at Zuurbekom (now Kempton Park) to build a building on the farm Modderfontein, which later became the largest explosives factory in the world (Anon., 1995a:1).

A similar, but rival factory, known as De Beers-Plofstofwerke, started in July 1903 with production at Somerset West. In 1909 Kynoch started a fertiliser and sheep-wash factory at Umbogintwini. De Beers opened a superphosphate plant at Somerset West in the early 1920's and sold the superphosphate under the name of Capex-Fertilizer (Die misstofvereninging van Suid-Afrika, 1994:81; Anon., 1995a:1).

Eventually a decision was taken to merge the different fertiliser and explosives factories and thus in 1924 AECI Limited was registered. After the merging of two explosive plants in 1924, AECI decided to market its fertiliser under the trade name of "Kynoch/Capex" (Anon., 1996b:22). In 1970 AECI and Triomf merged their fertiliser interests and traded under the name Triomf Kunsmis (Pty) Ltd. During March 1984 their paths separated and AECI again operated under the name Kynoch Fertilizer Limited in the fertiliser industry (Die misstofvereniging van Suid-Afrika, 1994:81-82). During the period of 1970 to 1984 only Kynoch Voere (Pty) Ltd used the name Kynoch (Anon., 1995b:1).

In order to increase its stakeholding in the fertiliser industry, the Triomf factory in Potchefstroom, in existence since 1967, was acquired by AECI during February 1987 (Die misstofvereniging van Suid-Afrika, 1994:82). During that period, the current central region, were operating as two separate regions and structures. The Potchefstroom and Chloorkop factories supplied fertiliser to both regions (Anon., 1995b:1).

Since 1991, during rationalisation, the two regions were combined to form the central region with its own structures. The central region serves customers in Gauteng, North West, Mpumalanga, Northern Province (all part of the old Transvaal), Free State, Northern Cape, Namibia, Swaziland and Lesotho. Simultaneously the Chloorkop factory was closed down. Over the last three years various expansions have been undertaken at the Potchefstroom factory like the MAP technical grade plant, the restarting of the sulphuric acid plant and the upgrading of the phosphoric acid plant.

2.2.2 BACKGROUND

The business of Kynoch (Pty) Ltd can be described as the sourcing of raw materials, manufacturing and marketing of fertiliser products mainly for the agricultural markets. For this purpose raw material is transported in for the production of intermediate and final products. These raw materials include sulphur, ammonium nitrate, phosphoric acid, potassium sulphate, and sulphuric acid (Anon., 1996a:19; 1996b:22). The intermediate products, which are manufactured on the premises, are MAP technical grade, MAP, SSP, phosphoric acid, and sulphuric acid. The final products consist of two basic products, namely fertiliser solids and fertiliser liquids. Each product is subdivided into nitrogen, phosphate, potassium ratios and plantfood content, for example 3.2.1(25) Zn or 2.3.4(30) Zn. (Die misstofverenigning van Suid-Afrika, 1994:82-83). Different nitrogen, phosphate, and potassium granulated mixtures are manufactured at granular I and II plants and clear liquid mixtures are manufactured at liquid plants (Van Rooyen, 1997).

These products are marketed on the local retail, wholesale, trade, export and inter company markets. The major customers of Kynoch Fertilizer (Pty) Ltd are farmers (60%), traders (30%) and manufacturers (10%). The most important competitors of Kynoch Fertilizer (Pty) Ltd are imports, Sasol (14%), Omnia (34%) and other local fertiliser companies (Anon., 1997:3; Viljoen, 1997:3). Presently the market share of the central region is calculated to be approximately 37% (Anon., 1996c:7).

The annual turnover and trading profit is summarised in table 2.1.

Table 2.1: Annual turnover and trading profit

	1995	1996	1997
Turnover (R millions)	519 596	736 649	761 267
Trading profit (R millions)	24 981	63 467	48 045

(Anon., 1995c:4; 1996c:4; 1997:5; De Vries, 1997)

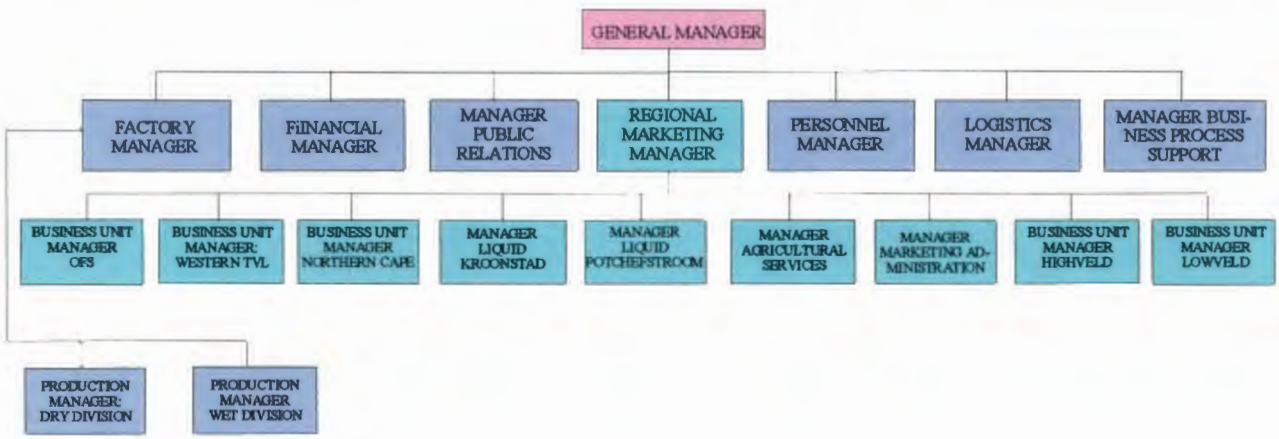
From the above table can be deducted that although Kynoch Fertilizer (Pty) Ltd experienced a growth in turnover there was a decline in trading profit of R15 422 million from 1996 to 1997.

2.2.3 ORGANISATIONAL STRUCTURE

Kynoch Fertilizer (Pty) Ltd is part of the greater Kynoch-group, of which AECI is the controlling company. Kynoch Fertilizer (Pty) Ltd is geographically divided into three regions, namely central, Cape and Natal. The central region consists of the Orange Free State, the four northern provinces and the Northern Cape. Five business units service this vast region with offices in Potchefstroom, Kroonstad, Bethal, Nelspruit and Niekerkshoop. In addition to the five geographical business units, the liquid division also forms a separate business unit (Van Wyk, 1997). A decentralised financial and administrative regional office in Potchefstroom supports these business units. Potchefstroom also is the main production plant from where a complete series of granular and liquid fertiliser products are supplied to customers. All the above mentioned business units are under the control of the regional marketing manager in Potchefstroom (Van Rooyen, 1997).

The organisational structure is graphically depicted in figure 2.1.

Figure 2.1: Organisational structure



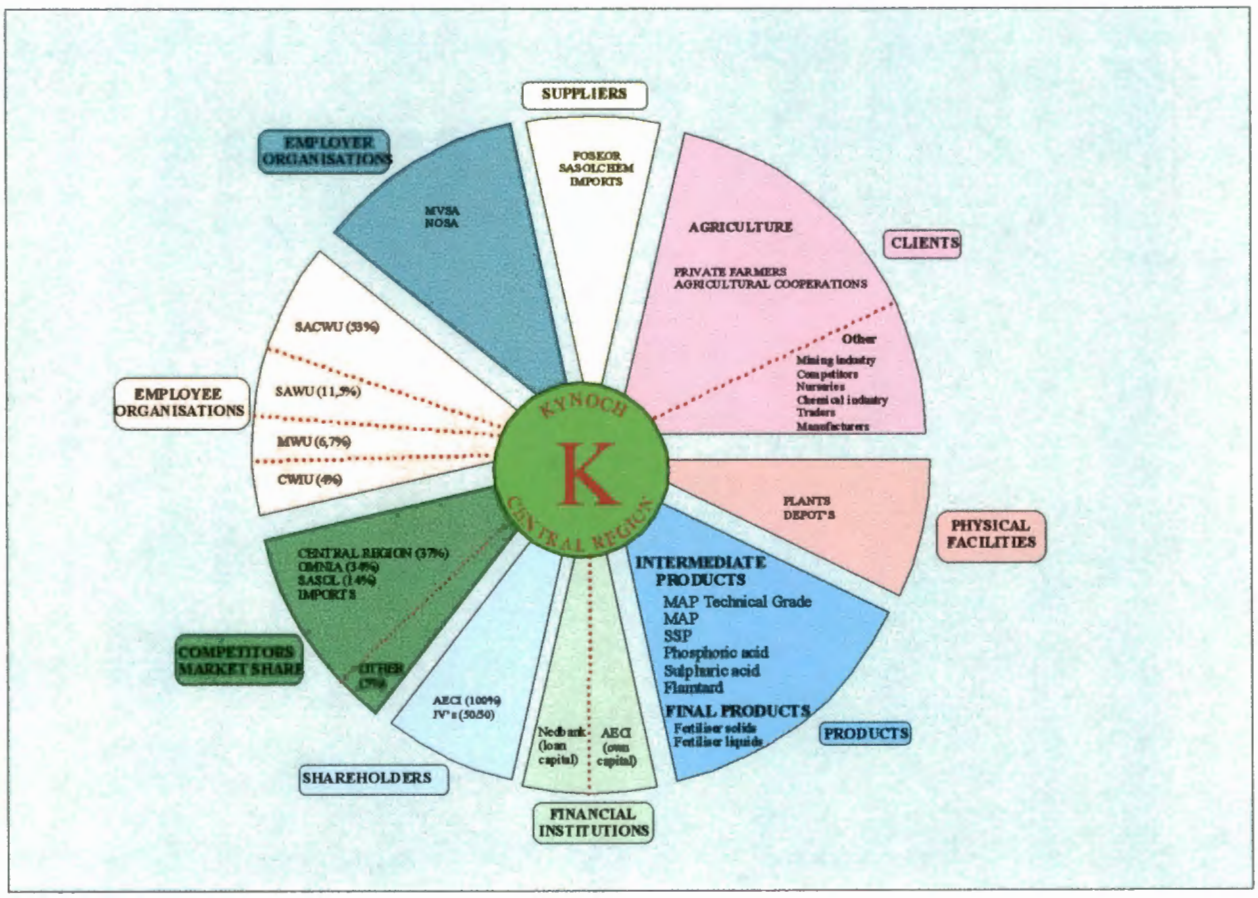
(Source: Jacobs, 1996b:6-7; Van Rooyen, 1997)

From the organisational structure above it can be seen that there are nine functional and departmental managers. The central region of Kynoch Fertilizer is further subdivided into nine business units under the control of the regional marketing manager.

2.2.4 PROFILE OF THE ORGANISATION

The profile of Kynoch Fertilizer (Pty) Ltd is schematically summarised in figure 2.2 below.

Figure 2.2: Organisational profile



(Source: Van Rooyen, 1997)

The profile in figure 2.2 illustrates all the various role-players and aspects of Kynoch Fertilizer (Pty) Ltd. The suppliers of Kynoch Fertilizer (Pty) Ltd is Foskor (phosphate), Sasolchem (chemicals) and Israel, Russia and Canada (potassium). These raw materials are processed and then sold mainly to farmers and agricultural cooperations in the agricultural sector, but also to the mining industry, competitors, nurseries, the chemical industry, traders and manufacturers. The physical facilities consist of various plants and depots where the intermediate en final products are manufactured.

Nedbank provides foreign capital while AECI, the controlling company, supply own capital. AECI has a 100% shareholding in Kynoch Fertilizer (Pty) Ltd. However, to promote entrepreneurship, as well as to limit costs, some joint ventures are operated on a 50/50 basis.

The major competitors of Kynoch Fertilizer (Pty) Ltd are Sasol and Omnia. Four employee organisations operate within Kynoch Fertilizer (Pty) Ltd, of which the South African chemical workers union (SACWU) is the largest. Other smaller unions are the South African workers union (SAWU), the mine workers union (MWU), and the chemical workers industry union (CWIU). Kynoch Fertilizer (Pty) Ltd is also affiliated with employer organisations, namely the fertilizer association of South Africa (MVSA) and the national operational safety association (NOSA).

2.2.5 MANAGEMENT INFORMATION SYSTEMS, TECHNOLOGY AND PRESENT SECURITY AT KYNOCH

2.2.5.1 The information technology platform

A full audit of the hardware, software, applications, databases en telecommunication technology (the information technology platform) was done. On the basis of this audit, as well as several interviews with business process personnel, the various aspects of the information technology platform will now be discussed.

2.2.5.1.1 Software

To supply accurate and timely management information for efficient and effective decision making with regard to the key performance areas of the organisation, several integrated and real time information systems, as well as leading software, have been implemented. These systems, programs and modules are summarised in table 2.2.

Table 2.2: Systems and software

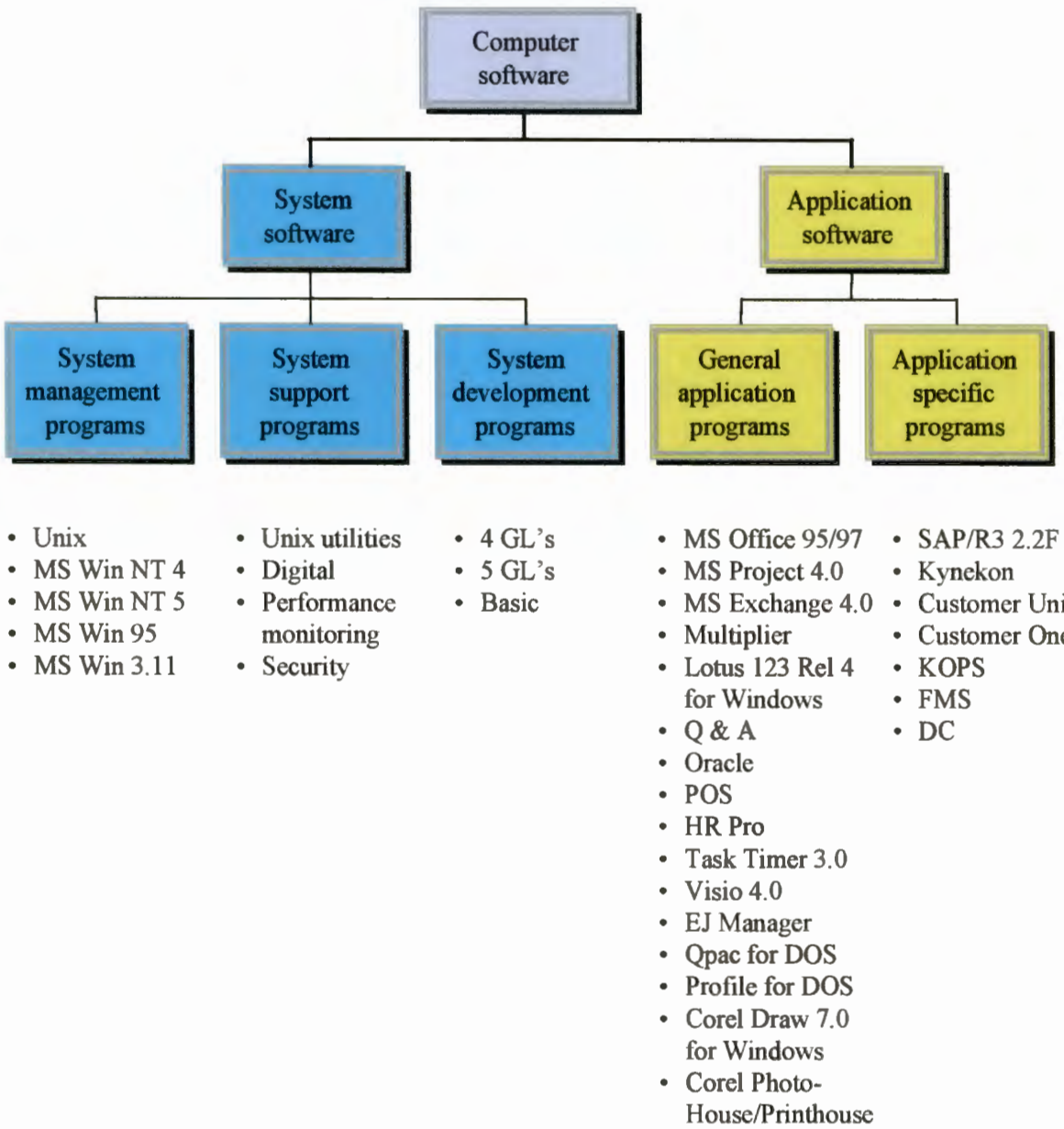
SYSTEM	PROGRAMS AND MODULES
Transaction processing	❖ SAP/R3 (June 1996) ❖ Customer Universe ❖ Point of Sale
Business information systems	❖ SAP/R3 ❖ SAP/R3 "Controlling" ❖ Total quality management (TQM)
Decision support systems	❖ Fertilisation recommender ❖ Kynekon (client needs and capabilities) ❖ Multiplier (strategic option generator) ❖ Market survey
Expert systems	❖ Customer One (complaints register and emergency line) - internal - external
Office automation	❖ E-mail ❖ Document management system ❖ Microsoft Office

(Jacobs, 1997b; Smith 1998)

From the above table can thus be deducted that Kynoch Fertilizer (Pty) Ltd employs various systems on the operational, tactical and strategic level (O'Brien, 1998:353). Of these systems the comprehensive SAP/R3 program forms an important part.

Kynoch Fertilizer (Pty) Ltd employs a large variety of software, which is illustrated in figure 2.3.

Figure 2.3: Software



(Source: Jacobs, 1996a:6-10; 1997; Van Wyk, 1997)

Kynoch Fertilizer (Pty) Ltd uses two main groups of computer software, namely system and application software. The system software consists of several operating systems, support and utility programs, and computer languages. The application software entails a variety of bought software, for example word processors, project managers, calendars, spreadsheets, desktop publishing, and databases. More dedicated programs, developed specifically for Kynoch Fertilizer (Pty) Ltd, are also used.

Some outdated software and systems are at the moment gradually being phased out, namely Windows 3.11, KOPS, FMS, DC Maintenance and "legacy" systems like Lotus, Q&A en Basic (Jacobs, 1996a:8).

SAP/R3

The base information system that is used at the central region of Kynoch Fertilizer (Pty) Ltd, is the SAP/R3 system. The various modules of the present SAP/R3 version 2.2F is listed in table 2.3.

Table 2.3: SAP/R3 system

Module	Facilities	
Financial accounting	General ledger	Financial control
	Accounts receivable	Financial assets
	Accounts payable	Funds management
	Consolidating	Credit control
Controlling	Cost element accounting	Income calculations
	Cost centre accounting	Profitability analyses
	Activity accounting	Profit centre accounting
	Order and project accounting	Business planning and control
	Product cost accounting	
Sales and distribution	Sales support	Dispatching
	Quotations	Billing
	Sales	
Materials management	Materials planning	Stock control
	Purchasing	Invoicing verification
	Warehouse management	
Production planning	Sales and operations planning	Production activity control
	Master planning	Quality management
	Material requirements planning	Production control and costs
	Capacity planning	
Plant maintenance	Maintenance notification	Maintenance history
	Maintenance ordering	Plant maintenance information
	Resource management	Client services
	Maintenance planning	

Table 2.3 (continued)

Module	Facilities	
Human resources	Personnel administration	Personnel information
	Time management	Organisational management
	Salaries and wages	Training room planning
	Travelling costs	

(Jacobs, 1997b)

Although the SAP/R3 system according to table 2.3 is a comprehensive system and covers various functional areas, not all modules are used to their full capacity. The SAP/R3 system has some outstanding features, for instance the fact that it is real-time, integrated, adaptable, configurable, and has an open architecture. The benefits of the program are functionality, flexibility, and comprehensiveness (Jacobs, 1997b).

2.2.5.1.2 Hardware

For the above mentioned software to function effectively it was necessary for Kynoch Fertilizer (Pty) Ltd to invest in quality information technology or hardware. The hardware presently being used is summarised in table 2.4.

From table 2.4 it is evident that a local and wide area network is used, which increases the information security risks dramatically (chapter 1). The representatives further endanger the security through remote access. The workstations or microcomputers are becoming old and will soon need upgrading.

Table 2.4: Hardware

Networks	**Types:** ❖ Local area network (LAN) – star typology, client-server system ❖ Wide are network (WAN) – head office and centres **Servers:** ❖ Two core servers • Database server (HP 9000 K Class) ‣ Unix operating system ‣ Looped with application server via optic fibre for backup purposes • Application server (HP 9000 K Class) - Unix operating system ❖ Data file server (Compaq) • Windows NT operating system • User data files for MS Word and Excel ❖ Communication server (Pentium) • Windows NT operating system • MS Exchange software ❖ Server for the remote access solution (RAS) system of the representatives (Pentium) • Windows NT operating system • Customer Universe ❖ Five Compaq Pentium file servers at the business units and plant ❖ Three servers at Randburg • Human resources server (HP 9000 D Class) • Development server • Maintenance server **Workstations:** ❖ Standard workstation • Mini tower with 200 watt power supply • Intel Triton Pentium motherboard • Intel Pentium 75 through 166 MMX CPU's • 16 to 48 Mb RAM • 425 to 2100 Mb hard disk drives • 1.44 Mb Stiffy drive • 1 Mb S3 SVGA PCI screen card • 3 COM ISA network card • 14" SVGA monitor • 101 keyboard and 3 button mouse ❖ Multimedia workstation • The same configuration as above, plus • 16 bit sound card • Multimedia speakers • CD-ROM drive

Table 2.4 (continued)

Communications	**Media:** ❖ Twisted pair cables ❖ Optic fibre ❖ Satellite (being tested) **Connections:** ❖ Diginet • 128 Kb line to Randburg (Human resources server, development server and maintenance server) • 64 Kb backup line via Milnerton to Randburg • Five 64 Kb lines to the five business units • Two 64 Kb lines and one 9600 b line (Niekerkshoop) to depots • EDI with Spoornet • EDI with Old Mutual ❖ Representatives • Fax/Modems • Five telephone lines • LANA server **Communication protocols:** ❖ Transmission control protocol (TCP) ❖ Internet Protocol (IP)
Output peripherals	**Printers:** ❖ Laser ❖ Inkjet (colour) ❖ Impact **Video display units:** ❖ VGA screens
Input peripherals	❖ Keyboards ❖ Mice ❖ Scanners
Storing devices	❖ Magnetic disks ❖ Tape streamers (DLT 2500 backup system on Unix servers) ❖ Optical disks

(Jacobs, 1997b; Smith, 1998)

2.2.5.1.3 Data classification

The data being handled at Kynoch Fertilizer (Pty) Ltd is mainly classified into five groups, namely:

Technical data: Data stored and processed in order to support the technological needs of the production, engineering and research functions.

Administrative data: Data processed in order to support infrastructural activities, for example payment of wages, payment of creditors, personnel records, budget and financial records, product ordering and despatch.

Production and maintenance data: Data processed in order to support the planning and control requirements of the production and engineering functions.

Management data: Data processed at a more senior level in the organisation to facilitate the orderly management of the organisation.

The bulk of administrative and production data are used for application systems rather than management information systems. There is, however, information derived from the application systems, which is used by top management (Jacobs, 1997b).

2.2.5.2 Policy

According to Jacobs (1997b) a carefully formulated information system policy exists at Kynoch Fertilizer (Pty) Ltd. The policy entails the following four aspects:

- Loading and removing of software.
- Computer ownership.
- Software standards.
- Central budget for equipment.

2.2.5.3 Risk management

Because of the key role of information systems in Kynoch Fertilizer (Pty) Ltd, the general risk of the business process support department is assessed quite high. Therefore the business process department formulated a risk management plan, which is summarised in table 2.5.

Table 2.5: Risk management plan

Key performance area	Key performance indicators	Risks related to non-performance	Controls	Risk rating
To manage the department in an efficient and cost effective manner	Segregation of duties between: • Systems design • Computer programming • Computer operations • Data entry • Custody of systems documentation, programs and files • Data control • Preparation and authorisation of source documents	Insufficient definition of responsibilities and the lack of segregation of duties, could lead to ineffective management and manipulation of the IS department and system	Specific assigned responsibilities	Low
To ensure the availability, accuracy, and integrity of all information systems	Hardware and software changes and manipulation	Lightning and cable protection could be inadequate, which could lead to the loss of management information	Regular internal inspections	Medium
		The hardware configuration not being documented could have cost implications when upgrading the system	Documented procedure for configuration changes	High
	Unauthorised access attempts	The lack of effective access and password control could result in unauthorised access and changes to the system.	Access and password controls	Medium
	Archiving and backup procedures	Statutory requirements might not be met	Strict adherence to backup policy Statutory requirements review	Medium High
	Unauthorised input	The risk of validity and completeness of data could be sacrificed due to ineffective input controls	Input controls	Low
	Distribution of system output information	System output information could be distributed to unauthorised users	Output controls	Medium
	System changes	The lack of adequate change management procedures could result in unauthorised and non-testing of changes	Development and documentation controls	High
	Disaster contingency plan	The business could experience a continuity problem if the worse case scenario occurred	Documentation and communication of disaster contingency plan	High
	System administration procedures	System maintenance process might not be performed	Documented system administration manual	Medium

(Jacobs, 1997b).

From table 2.5 it is clear that the insufficient assignment of responsibilities is mainly identified as a risk to ineffective management and manipulation of the system. A much higher risk is the availability, accuracy and integrity of information systems due to lightning, absence of

documentation, lack of access and password control, insufficient backup procedures, unauthorised input, lack of output controls, lack of change management, lack of a disaster recovery plan, and insufficient system administration procedures.

2.2.5.4 SWOT analysis

According to Thompson and Strickland (1996:92) a SWOT analysis is a useful technique to get a quick overview of an organisation's strategic situation. Such a SWOT analysis was done by Kynoch Fertilizer (Pty) Ltd under the leadership of the business process support manager in order to determine the various strengths, weaknesses, opportunities and threats of the business process support department. For information security it is important to determine the fit between an organisation's internal capability (strength and weaknesses) and its external situation (partly reflected by the opportunities and threats).

2.2.5.4.1 Strengths

Thompson and Strickland (1996:92) defines a strength as "something a company is good at doing or a characteristic that gives it an important capability." The following strengths were identified:

- Most depots are connected to the wide area network.
- Excellent base program, namely SAP/R3.
- Good application of software.
- Fine hardware.
- Effective management of information systems.
- Carefully planned information systems.
- Costs are strictly controlled.

(Jacobs, 1997b)

2.2.5.4.2 Weaknesses

A weakness can be defined according to Thompson and Strickland (1996:93) as "something a company lacks or does poorly (in comparison to others) or a condition that puts it at a disadvantage." Seven weaknesses were mentioned:

- Software are not fully utilised, for example Windows 95 and Multiplier (strategic planning program).
- The full potential of the hardware is not utilised.
- SAP/R3 version 2.2F does not have an electronic commerce facility.
- End user resistance against information technology.
- End user ignorance concerning the value and use of programs.
- End users do not feel part of the development process.
- Insufficient information security.

(Jacobs, 1997b)

2.2.5.4.3 Opportunities

Only three main opportunities were named:

- Electronic commerce.
- Electronic data interchange and electronic funds transfer with suppliers and clients.
- Utilisation of the Internet for International marketing and commerce

(Jacobs, 1997b; Van Rooyen *et al.*, 1997:9)

2.2.5.4.4 Threats

According to Jacobs (1997b) and Van Rooyen *et al.* (1997:9) the threats, which were referred to, were the following:

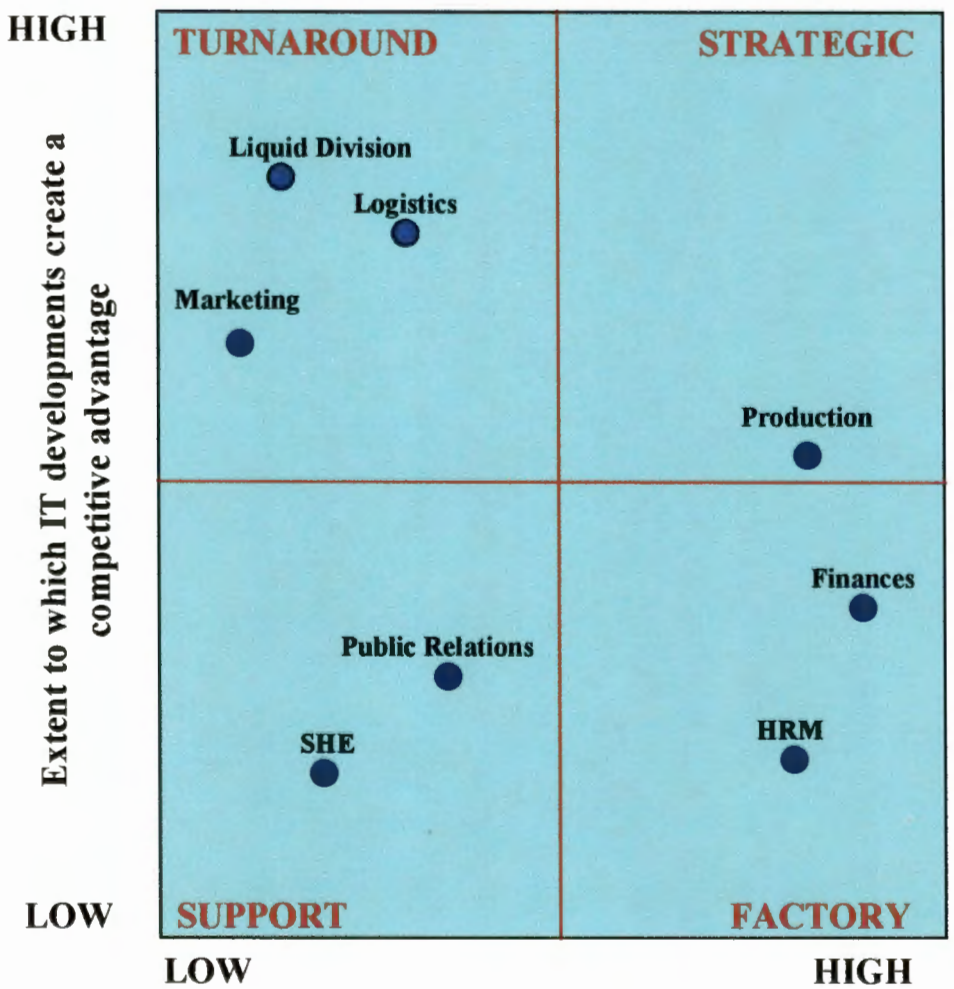
- Technological advantage of competitors.
- Natural disasters.

- Computer break-ins, fraud and viruses.

2.2.5.5 Strategic impact of information systems at Kynoch Fertilizer (Pty) Ltd

For management to fully realise the importance of information security it is crucial that they fully understand the strategic impact of information technology and systems. To analyse the strategic impact of information technology at Kynoch Fertilizer the strategic matrix of McFarlan and McKenney can be used (Martin *et al.*, 1994:508; Currie, 1995:32-33). The strategic information technology grid was drawn up with the help of the manager of the business process support department and is presented in figure 2.4.

Figure 2.4: Strategic impact of information technology



(Source: Jacobs, 1997b)

From the strategic information technology grid in figure 2.4 it is apparent that the production falls in the strategic class, which means that it is very much dependant on information technology for the performance of everyday routines (Martin *et al.*, 1994:508).

The liquid division, logistics and marketing fall into the turnaround classification. They are thus presently not heavily dependent on information technology, but may look to new information systems applications in the near future to bolster their competitive position in the marketplace (Martin *et al.*, 1994:509).

Although finances and human resource management may be heavily dependent on information technology for their day to day operations, they are not in a position where information systems can be seen as providing a competitive advantage. The important aspect is that their information technology systems should be reliable en readily available. Finances and human resources thus fall into the factory class (Martin *et al.*, 1994:509).

Public relations and safety, health and environment fall into the support class. Information technology is mainly used for support activities (Martin *et al.*, 1994:509).

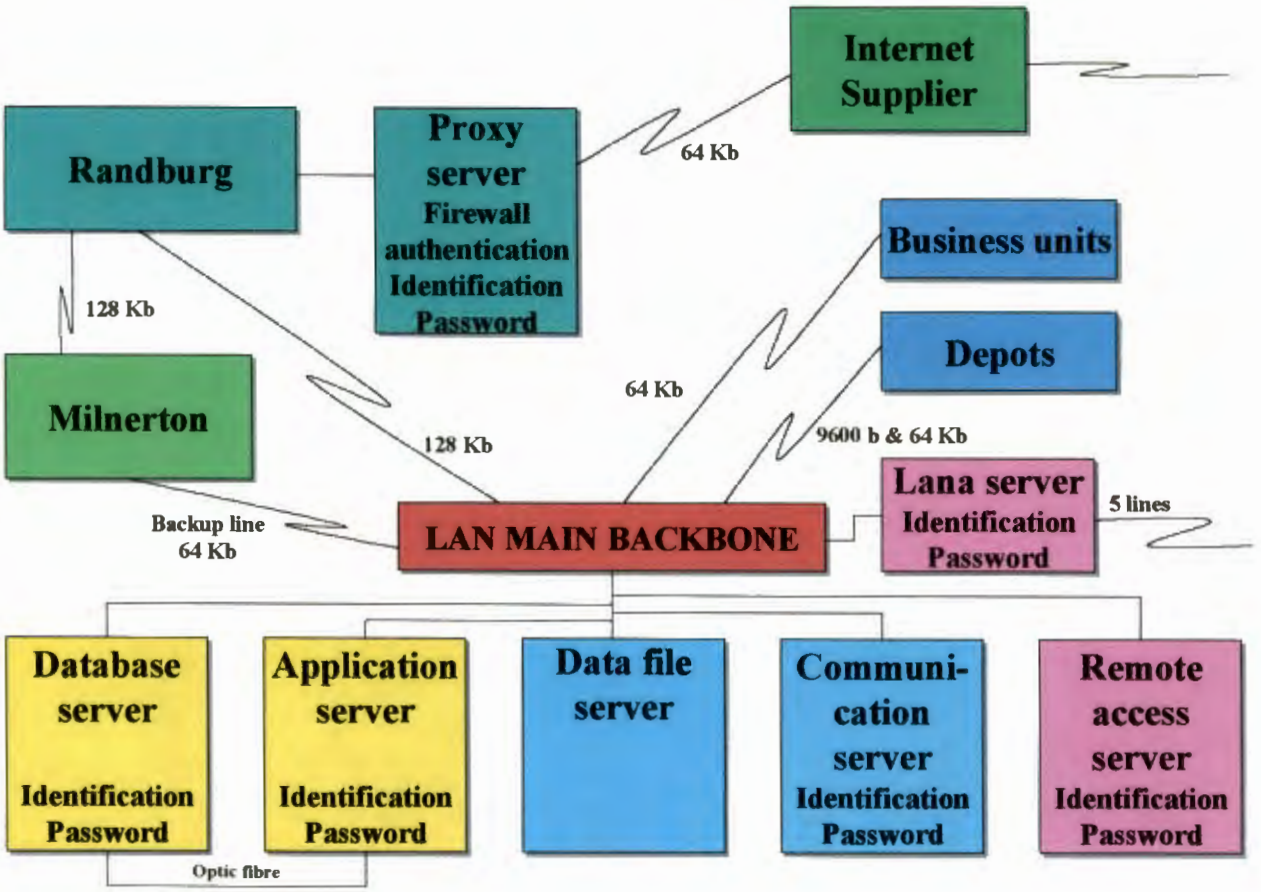
2.2.5.6 Present information security situation

In the formal business plan for 1997-2002, information security only features in a very limited way. The business plan states that the objective is to "develop and implement information system reliability and security", which is spelled out as the "the development and implementation of information systems to protect the information and systems of the Central Region through an investigation of information security (January 1998), an investigation of systems security (January 1998), change of passwords (July 1997), and the revaluation of profiles (August 1997)" (Jacobs, 1997a:1-16).

Although information security is mentioned as one of the objective of the business plan, it became apparent that no formal documented information security policy, written standards or guidelines for the central region of Kynoch Fertilizer (Pty) Ltd existed (Jacobs, 1997b).

During the audit that was done at Kynoch Fertilizer (Pty) Ltd, it became apparent that some information security controls were implemented. The interconnectivity of Kynoch Fertilizer (Pty) Ltd and present security measures are illustrated in figure 2.5.

Figure 2.5: Kynoch Fertilizer (Pty) Ltd interconnectivity and security



(Source: Jacobs, 1997b and Smith, 1998)

From figure 2.5 it can be seen that Kynoch Fertilizer has a high level of interconnectivity by means of a local and wide area network, Internet connection, and dial-in lines. This connectivity dramatically increases the vulnerability of the information resource. Therefore Kynoch Fertilizer (Pty) Ltd implemented some information security control measures, for example identification procedures and passwords. Access to the Internet is via Randburg and is protected by a proxy server, firewall, as well as authentication and identification procedures, and passwords.

2.3 ORGANISATION SPECIFIC CAUSAL FACTORS LEADING TO THE STUDY

Several factors lead to the need for this specific study on information security. Only the most important factors are briefly discussed.

2.3.1 DYNAMIC CHANGES IN THE COMPUTER ENVIRONMENT

As indicated in the problem statement in chapter one, the information technology environment experienced dramatic changes over the past few years, which lead to an increase in information security risks and threats. It became evident that Kynoch Fertilizer (Pty) Ltd experienced the very same changes in the computer environment. Some of the more important changes were:

- A dramatic increase in the use of personal computers.
- An increase in the use of local and wide area networks.
- An ever-increasing dependency on information.
- Totally new information needs.
- An increasing complexity and integration of systems and technology.
- An increasing end user involvement.

These changes in the information technology environment inevitably lead to an increase in the following information security risks and threats:

- Fraud and theft.
- Violation of information privacy and security.
- Lost of resources and finances.
- Sabotage and industrial espionage.
- Misuse of assets and resources.

These factors all contributed to a greater risk in information security at the central region, which urgently needs to be researched and addressed (Jacobs, 1997b). This observation is supported by the research done by Ernst & Young (1996; 1997), which indicated that computer fraud in the manufacturing environment is escalating in occurrence and in rand value.

2.3.2 UPGRADE TO SAP/R3 VERSION 3

Kynoch Fertilizer (Pty) Ltd will shortly be upgrading to SAP/R3 version 3, which will enable them to use electronic data interchange and electronic commerce in the highly competitive

global market. Electronic commerce and an increased usage of the Internet will certainly increase the information security risks and demand higher information security (Jacobs, 1997b).

From the preliminary research it became evident that a lack of information security policies, standards, guidelines, employee training and control procedures exist. The possibility is great that the existing security is not up to standards and will probably not be adequate for the proposed upgrade.

2.3.3 THE RESPONSIBILITY OF MANAGEMENT

To understand corporate information management responsibility, requires that top management have a good idea of the importance and strategic nature of information in modern business practices. To be able to have a strategic advantage in the world of intense competition, it is essential to have the right information at the right time. The importance of information in the management process cannot be overemphasised. Management should therefore realise that their information resources have to be properly and responsibly managed (Rilley, 1981:14-15).

Management information systems are thus a valuable asset and therefore also open to risks. The management of information security risks are the primary responsibility of senior management (Von Solms, 1993:3). It is too important to be left in the hands of a few computer specialists. However, the preliminary research revealed that senior management at Kynoch Fertilizer (Pty) Ltd has not yet attended to:

- The establishing of security policy.
- The allocating of information security responsibility.
- The development of a comprehensive security plan in view of the organisational strategic plans.
- The constant monitoring of the information security plan.

(Jacobs, 1997b)

Security objectives will only permeate an organisation if they are made an objective of the organisation by top management and form part of the total business plan. It is therefore of the utmost importance to determine the level of involvement of senior management at Kynoch Fertilizer (Pty) Ltd in information security.

2.4 SUMMARY

The organisation on which the research will be based is the central region of Kynoch Fertilizer (Pty) Ltd, a manufacturer of various solid and liquid fertiliser products that was established as early as 1903. Kynoch Fertilizer (Pty) Ltd manufacture a variety of intermediate and final products for the local retail, wholesale, trade, export and inter company markets. The central region of Kynoch Fertilizer (Pty) Ltd is part of the Kynoch-group and consists of seven business units.

Kynoch Fertilizer (Pty) Ltd makes extensive use of computerised information, the SAP/R3 system, local and wide area networks, as well as distributed computing, which emphasise the importance and necessity to study the current level of information security and control. This necessity is emphasised by the SWOT analysis and strategic information technology grid, as well as the absence of a formal documented information security policy.

Organisation specific causal factors leading to the study were thus mainly the dramatic information technology changes that took place over the last few years at Kynoch Fertilizer (Pty) Ltd and the resultant increase in information security risks and threats. Two other causal factors were the possible change to version 3 of the SAP/R3 system and certain managerial aspects regarding information security that were lacking.

CHAPTER 3

INFORMATION SECURITY RISKS AND THREATS

Every new technology carries with it an opportunity to invent a new crime.

Laurence Urgenson

3.1 INTRODUCTION

Although many organisations acknowledge the importance of information security, it is often only implemented after incidents of fraud, break-ins, theft, damage and financial losses occurred. Organisations frequently have well documented plans, policies, systems, procedures and controls, but it is not enforced. Sometimes organisations will only have a sort of instinctive and informal security control, but no formal policies at all.

As organisations become more dependent on computerised information and information systems, greater attention will have to be paid to information security in order to protect the valuable information resource and to retain a competitive advantage. However, to exercise effective information security it is important to know which methods are presently being used to exploit vulnerabilities in information security.

This aim of this chapter is therefore to study the various vulnerabilities, threats and risks regarding information, information security and control.

3.2 PROBLEMS WITH INFORMATION SECURITY

3.2.1 INFORMATION SECURITY RISKS

An important reason for the greater information security risk is the increasing number of computer applications and the consequent concentration of information and processing. Because

of technological advances it often happens that the development of important supportive functions like auditing and computer security that protect information from intentional losses are lagging behind. Sophisticated networks and use of the Internet further contribute to this problem.

There are basically three major types of primary risks concerning information security, namely:

- **The integrity of data, programs and systems:** Only authorised people, in the sense of writing, changing, deleting, and creating, should modify the assets (Alexander, 1995:30).
- **The confidentiality of data and systems:** The protected entity (for example information, software, and equipment) should be accessible only to authorised people in the sense of reading, viewing and printing (Alexander, 1995:30). The confidentiality goal often includes restrictions on the flow of information (Olivier, 1991:9).
- **The availability of data and systems:** The assets should be available to authorised people (Pritchard, 1979:13). An authorised person should not be prevented from accessing the data or objects to which he or she has legitimate access (Pfleeger, 1989:5-6; Van Zyl, 1990:2).

Louw (1990:76-77) pointed out that if these risks are not adequately controlled, it may cause a variety of secondary risks, namely business interruption; loss of, or damage to assets and information; erroneous management decisions; excessive expenditure; erroneous record-keeping; unacceptable accounting; loss of employee morale; loss of customer confidence; fraud and embezzlement or commercial espionage. Any of these risks may culminate in a measurable cost to the company, thereby directly affecting its competitive position and profits

The major risk areas can also be classified as:

- **Hardware risks:** The portability of computer equipment (for example memory, modems) and accessories (for example floppy disks) make it an attractive target for office thieves (Wong & Watt, 1990:90-93).[1]

- **Software risks:** Many systems only have a limited password system, while the password table is held in clear text (Wong & Watt, 1990:93-95).

[1] Although the works of Pfleeger (1989) and Wong and Watt (1990) are older works, they can be regarded as standard works on information security, especially regarding the basic principles of information security.

- **Network risks:** The host usually does not recognise any local intelligence of a workstation. Once the data is downloaded, the host security system cannot impose restrictions on any subsequent copying, printing, interrogation or modification of the data, or its forwarding to another workstation on the network (Wong & Watt, 1990:95-97).

- **User-related risks:** Usually the office personal computer user does not appreciate the need for security, and therefore does not practise routine backup and control procedures. Common English or Afrikaans words or names are generally used as user passwords, passwords are seldom or never changed, and computers are left unattended after log-on. Floppy disks are interchanged between work and home which aggravate the virus problem (Wong & Watt, 1990:98-100).

3.2.2 THREATS TO INFORMATION SECURITY

According to Lowe (1994:35) an information security threat can shortly be defined as the potential violation of information security. Threats can broadly be grouped into seven main categories, which are not necessarily mutually exclusive.

3.2.2.1 Insider threats

Insider threats occur when legitimate users of the system behave in an unexpected or unauthorised way (Claassen, 1994:1-12). Theft of computer services and data constitutes the largest category of information misuse (Lubbe & Amstrong, 1995:22). Haag *et al.* (1998:394) pointed out that law enforcement officials found that it is mostly insiders that tamper with information.

3.2.2.2 Outsider threats

These are threats that arise when persons who are not authorised to use the system compromise the security of the system by making use of active or passive wiretapping, interception of transmission, masquerading as an authorised user or by by-passing authentication or access control mechanisms (Claassen, 1994:1-13).

3.2.2.3 Passive threats

Claassen (1994:1-13) illustrated that passive threats occur where no modification is made to any information or the system itself, and where the operation and state of the system are not changed, for example passive wiretapping to observe information.

3.2.2.4 Active threats

According to Claassen (1994:1-13) active threats are threats, which involve the alteration of information, or change the state or operation of the system, for example a malicious change to the routing tables of a system by an unauthorised user.

3.2.2.5 Accidental or unintentional threats

Claassen (1994:1-12) pointed out that accidental threats are threats that occur with no premeditated intent, for example system malfunctions, operational blunders and software bugs (compare also Perlman, 1994:57). These are the dangers of ignorance, lack of training or insufficient documentation where files are wiped out, disks are damaged or information is corrupted (Russell &. Gangemi, 1992:14). Unintentional threats also include loss or destruction of identification cards, printout, source documents, or magnetic tape, as well as operator errors, hardware errors, crosstalk, software or programming errors (Walker & Blake, 1977:3-6). These unintentional threats can be systematised as follows:

- **Hardware failure:** Because of the complexity of computer systems and number of components, hardware failure is a real threat. A simple problem, like a faulty hard disk, or ground loops, can distort data and cause unimaginable damage, especially when it goes undiscovered (Lowe, 1994:44-46).

- **Software failure:** This aspect refers to computer program failure, that is when the program written for the computer does not perform the way everyone expected it to, because of what is commonly described as a "bug" or logic flaw in the program (Post & Anderson, 1997:670-672).

- **Human or liveware failure:** The human element can and does play a very important role in disaster situations (Martin *et al.*, 1994:367). People are able to destroy data, valuable files,

programs and procedures inadvertently. They even may damage equipment (Rilley, 1989:29-31).

- **Bumbling:** Stang (1992:5) mentioned that a very high percentage of disasters can be attributed to bumbling, otherwise known as human errors, accidents, errors of omission and errors of commission.

3.2.2.6 Environmental hazards or natural risks

The fact that computer systems is generally of a delicate electronic nature, makes it susceptible to natural phenomena, for example earthquakes, floods, fires, power surges and failures (Russell & Gangemi, 1992:14).

3.2.2.7 Intentional or deliberate threats

Intentional threats, according to Claassen (1994:1-12), may range from casual examination using easily available monitoring tools to sophisticated and specialised attacks using special knowledge of the system and software. Deliberate threats can come from outsiders and insiders. Outsiders include foreign intelligence agents, terrorists, criminals, corporate raiders, and hackers. Many security systems protects against outsiders, but totally ignore the insider threat, for example the fired or disgruntled, coerced or greedy employee (Russell & Gangemi, 1992:14-16).

Although many methods exist to deliberately threaten information security, they can basically divided into the following categories:

- **Interruption or denial of service:** Denial of service is the prevention of a legal user from performing computer or network tasks (Lowe, 1994:35). In an interruption, an asset of the system becomes lost or unusable, for example the malicious destruction of a hardware device or the erasure of a program or data file (De Ru, 1992:20; Pfleeger, 1989:3).

- **Interception:** Interception entails the observation and interception of data on the network and means that some unauthorised party has gained access to an asset, for example wire tapping or copying of data files (De Ru, 1992:20; Pfleeger, 1989:4). Interceptors often employ a network analyser to assist them (Lowe, 1994:35, 43-44).

- **Modification:** Modification is when an unauthorised party tampers with an asset for example the modification of values in a data base, the alteration of programs to perform an additional computation, or the modification of data being transmitted electronically (De Ru, 1992:20; Pfleeger, 1989:4). Modification thus entails the random changing or deletion of sensitive information (Lowe, 1994:35).

- **Fabrication:** Fabrication is when unauthorised parties fabricate counterfeit objects for a computing system, for example the adding of spurious transactions to a network communication system, or the adding of records to a data base (De Ru, 1992:20; Pfleeger, 1989:4).

From the above it is already clear that the deliberate threatening of information security encompasses not only computer crime and fraud as is often believed, but a variety forms of illegal, dishonest and unauthorised behaviour involving automatic data-processing and/or transmission of data (Anderson, 1983:21; Louw, 1990:78).

Some of the most important types of computer abuse will be discussed below:

3.2.2.7.1 Computer fraud

According to Schultheis and Sumner (1998:657) computer fraud is committed when a person gains unauthorised access to a computer and modifies or damages the computer, system or network in order to control assets or services (compare Anderson, 1983:34).

Most computer-related fraud cases proved to be the work of trusted staff, sometimes in collusion with outsiders (Rilley, 1981:32; Wong & Watt, 1990:33). The problem is aggravated by management laxity and the favourable conditions created by the computer environment, namely:

- The embezzler can operate from a distance or away from the scene of the crime.
- Hard copy records play a declining role in data processing with resulting implications for the auditor.
- Low unit, high volume crime becomes feasible, for example the salami technique where one cent is stolen from every depositor.
- International crime is difficult to prosecute and easy to commit.
- The prosecution and punishment of computer crime is not effective.

Fraud can be committed through numerous mechanisms or a combination of mechanisms such as illegal program code, fraudulent input, abused input and output, abused computer service, abused terminals, collusion, and data file manipulation (Knight, 1995:237; Lubbe & Amstrong, 1995:20-22). It was found that the most common modus operandi are fraudulent input and terminal abuse (Wong & Watt, 1990:36-42).

Unfortunately, as Anderson (1983:5) quite aptly pointed out, a significant amount of computer fraud goes undetected. It is only by chance or when the perpetrator makes a serious mistake that most cases are uncovered.

3.2.2.7.2 Computer crime

Computer crime can be classified as any person who deliberately uses a computer, computer system, computer network, or any part thereof for the purpose of devising or executing any scheme or artifice to defraud, obtain money, property, or services by means of false or fraudulent pretences or representations (Conradie, 1996:71; Pfleeger, 1989:12). Computer crime also includes any person who deliberately and without authorisation uses, alters, damages, or destroys any computer, computer system, computer network or software program, documentation or data.

Because of the growing importance and usage of computers, computer fraud and crime are escalating (Ernst & Young, 1996:12; 1997:5). The cost of computer crime in South Africa was estimated in 1986 to be R140 million (Bezuidenhout, 1988:24). According to the Ernst & Young (1997:5) survey the rand value of losses increased. In 1996 78% of respondents indicated a loss of R250 000, 17% a loss of between R250 000 and R1 million, and 5% reported losses of R1 million or more. It is clear that the situation will continue to worsen if organisations do not pay more attention to effective information security and control.

3.2.2.7.3 Hacking

Hacking involves the use of remote diagnostics to break into a computer, computer system, or computer network (Lowe, 1994:36; Wong & Watt, 1990:3). Over the years varieties of hackers have developed namely phreaks, codes-kids, cybercrooks, wares dudes and crackers. Although it is estimated that only about 1% of all hacking is done with malicious intent this phenomenon remains a costly threat to information security and can cause serious damage to information systems (Lowe, 1994:37-38).

3.2.2.7.4 Sabotage

Computer sabotage threatens the integrity and availability of information systems (Louw, 1990:78). Disgruntled internal staff commits many cases of sabotage of information technology equipment, data and systems (Wong & Watt, 1990:9,33). It is quite easy for a dissatisfied employee to destroy files and programs in a relative short span of time. It is therefore important to have good termination procedures, especially for trusted employees in senior positions, whose privileged positions could enable them to access very sensitive systems and information (Wong & Watt, 1990:11).

3.2.2.7.5 Industrial espionage

Bugging of organisations in South Africa is widely known (Rilley, 1981:33). One of the primary intentions of industrial or economic espionage is to gain information, which will give the spy or his organisation a competitive edge over the invaded organisation (Schultheis & Sumner, 1998:658-659). Computer systems contain valuable production, financial, marketing and other data and are therefore a prime target for industrial espionage.

3.2.2.7.6 Misuse of authority

According to Louw (1990:78) the principle threat of confidentiality at the application level is the abuse or misuse of authority by authorised personnel. Although an audit log can be used to produce an accurate, immutable, persistent record of relevant activity that can attest to an auditor the possible misuse of authority (what, when, whom, why, where and how), it is not impossible for an experienced person to circumvent it.

The misuse of authority is aggravated by the distributed nature of the applications, which makes the implementation of security functions more difficult. The operating system and applications do not really take each other into consideration when security is concerned. Applications are huge, complex, portable, and performance tuned, while identification and authentication are often implemented unacceptably. Applications can therefore easily be penetrated. These vulnerabilities are further aggravated by inadequate encapsulation (Lodin *et al.*, 1997).

3.2.2.7.7 Data diddling or manipulation

Data manipulation threatens the integrity of the information system and entails the altering or omission of data prior to or during the entering of the data or on the route from source to destination (Anderson, 1983:36; Louw, 1990:78; Lubbe & Amstrong, 1995:23). It is the most basic and common method used for computer crime.

The alteration of data because of abuse can take on various forms:

Replay

The reprocessing of data items, for example the interceptance of a message from one bank to another. The message is usually modified and replayed (Pfleeger, 1989:10).

Salami techniques

Automated allocation of very small amounts of money by deducting or rounding (Anderson, 1983:37; Pfleeger, 1989:10, 174-175; Lubbe & Amstrong, 1995:22). It is however a technique that is not frequently used (Parker, 1990:545).

Spoofing

Spoofing is when a computer or computer user is fooled into thinking that he is communicating with a specific computer, while he is actually communicating with an interceptor (Anderson, 1983:38). Spoofing usually involves the creation of counterfeit packets with private Internet addresses in order to gain access to private networks and information by impersonating the system that owns the address (Kalakota & Whinston, 1997:124). These programs usually trick an unsuspecting user into giving away privileges (Russell & Gangemi, 1992:86).

Superzapping

This method is derived from a well known emergency computer utility that works as a "master key" to the system and grants unhindered access to any part of the system (Stang, 1992:11). The program will bypass all controls or modify or disclose any of the contents of the computers (Anderson, 1983:39).

3.2.2.7.8 Masquerading

Masquerading occurs according to Anderson (1983:39) when an unauthorised user attempts to gain access to a system, by acting like an authorised user, using a valid password.

3.2.2.7.9 Malicious data deletion

Disgruntled employees may delete important data and cover up their tracks. It is therefore important to make simultaneous sign on for one user impossible (Wong & Watt, 1990:67-69).

3.2.2.7.10 Data corruption

Wong and Watt (1990:70) indicated that data can easily and deliberately be corrupted if the access by all employees, including technical or development staff, is not controlled carefully.

3.2.2.7.11 System lockout

It is possible for an employee to lock the total computer system by means of a secret password. It is therefore necessary to implement acceptance testing, independent authorisation, and checking of code changes. A favourite way in which disgruntled technical staff introduces illegal code (lockout passwords, salami technique) into programs is by means of the backup copies which are often not stored in a secure place. Then by using his or her expertise to crash the system, the illegal code is introduced via the backup files. The access of backup files should therefore be controlled very strictly (Wong & Watt, 1990:70-71).

3.2.2.7.12 Software modification

Software programs are often used to exploit vulnerabilities in computing systems. Programs can intercept or modify data on behalf of unauthorised users, and they can exploit service flaws in computing systems to allow system access to unauthorised users (Pfleeger, 1989:169). The most frequently used programs are:

Bombs

A Bomb is a malicious piece of code contained within a normal computer program and executes on a specific time or event with the aim of failing at a critical time, damaging of valuable information, disclosing of files or transferring of money (Denning, 1990:xiv; Louw, 1990:13; Pfleeger, 1989:7). There are basically two types of bombs, namely time bombs and logic

bombs. The time bomb is set to release a virus or worm or system attack at a specific date or time, for example the famous Friday the 13th virus. A logic bomb is set to go off when a particular event occurs for instance if a customer tries to perform an illegal copy (Russel & Gangemi, 1992:84), or when certain conditions are met (Forcht, 1994:269-270). Usually all internal evidence that there had been an illicit access to the system is destroyed afterwards (Anderson, 1983:38).

Program manipulation or Trojan Horse method

Program manipulation comprises the hidden placement of computer instructions in a program in order to conduct unauthorised functions without impact on the functioning or objective of the program (Hruska, 1992:18-22). Trojan horses usually hide in attractive programs, which tricks a user into running the program (Russell & Gangemi, 1992:83). Trojan horses are often used to modify protection levels of files, and to alter access rights (Witten, 1990:117-118). To counter this security threat computer centres must accept only source code and rather perform their own compilations before making a contributed utility public (Pfleeger, 1989:8, 169-170).

Trapdoors

This method is commonly used by programmers and comprises the inclusion of additional program coding and instructions to create a secret, undocumented entry point to a program or module (Lubbe & Amstrong, 1995:23). The designer usually inserts the entry point during code development (Anderson, 1983:37; Pfleeger, 1989:8, 170).

Data leakage

Data leakage occurs when data is removed or copied from a computer system or network without official authorisation or when data is made accessible to unintended people or programs via covert channels (Stang, 1992:5-6). Programmers can create a program that secretly communicates sensitive data. In an environment where data is extremely sensitive, a programmer should therefore not have access to the data on which the program operates after the program has been tested and implemented (Pfleeger, 1989:8, 175-177).

3.2.2.7.13 Scavenging

According to Stang (1992:11) scavenging or browsing basically involves the theft of information. The most basic form is to search a wastepaper basket for the log-on password, user

identification, discarded printer ribbons, and hand-written notes with sensitive information. Another form of scavenging is to be present when another user logs on (Anderson, 1983:36), to unerase files from disks (Stang, 1992:11), or to use sniffer programs as in the case of Carlos Felipe Salgado who stole a 100 000 credit card numbers from a database on the Internet.

3.2.2.7.14 Piggybacking and impersonation

Electronic piggybacking is a method for gaining access to a computer system where identification is verified automatically by the computer system (Lubbe & Amstrong, 1995:22). Usually an extra terminal is attached to the channel and the messages and instructions are selectively interrupted as they move between the system and the user. The user is tricked to log off by the modified messages, without really signing off (Anderson, 1983:38-39).

Impersonation is the process of one person assuming the identity of another person, for example by stealing and using another person's passwords or access codes (Lubbe & Amstrong, 1995:23; Stang, 1992:7).

3.2.2.7.15 Wiretapping

Wiretapping is the tapping of information during data transmittance over communication channels (Pritchard, 1979:72). Although called wiretapping, it is not limited to landlines, but also includes microwave and satellite interception (Stang, 1992:12).

3.2.2.7.16 Service problems

Security problems do not only involve data, but also computer service. Malicious programs can block a computer system so that legitimate users are denied access.

Theft of services

Theft of services threatens the availability of the information system (Louw, 1990:78).

Greedy programs

A program can maliciously be altered to let background computing assume a foreground position, thereby slowing or blocking all other computation (Pfleeger, 1989:177).

a) Loops

A simple example of a greedy program is one that loops indefinitely, for example input/output loops which stops the central processing unit and monopolises the entire system (Pfleeger, 1989:178).

b) Viruses

Computer viruses are the logical extensions of greedy programs, and generally fall into four categories, namely boot sector and partition record infectors[2], system infectors[3], generic application infectors[4] (Louw, 1990:29; Solomon & Kay, 1994:11) and macro infectors[5] (Holton, 1996). A virus is a small program that can "infect" other programs by modifying them to include a copy of the virus program itself, so that the infected program begins to act as a virus, infecting other programs (Kroenke & Hatch:1997:431; Russell & Gangemi, 1992:79). Eventually the entire computer system can be taken over by the viruses (Denning, 1990:286-287; Louw, 1990:1,10; Pfleeger, 1989:178).

Viruses usually spread rather quickly, because they are often planted in shared system utilities to access common data, such as electronic mail, systems news bulletins, and lists of users on the system (Pfleeger, 1989:178; Wong & Watt, 1990:11-112).

Viruses are extremely dangerous because they can be written to cover most traces of their spreading, and are often "hidden" inside larger and more complicated programs. This is the main reason why viruses are many times detected too late (Pfleeger, 1989:178-179). Some viruses also employ stealth or evasive techniques, polymorphism or mutation, and tunnelling to evade virus detectors (Perlman, 1994:58)

Computer viruses therefore represent a significant threat to the corporate computing environment, because they compromise all three aspects of information security, namely integrity, confidentiality and availability (Louw, 1990:3). The primary risk viruses expose the information system to, is summarised in table 3.1.

---

[2] Common examples of the boot infector virus that installs itself and attacks by seizing the computer's start up sequence, include the Brain virus from Pakistan, the Italian bouncing ball from Turin, the 2730 virus, the Alameda virus, the mistake virus from Israel, the New Zealand virus, Nichols virus, Cruel and search virus (Spafford *et al.*, 1990:342-345; Wong & Watt, 1990:114).

[3] An example of the system infector is the Lehigh virus (Spafford *et al.*, 1990:345-346; Wong & Watt, 1990:115).

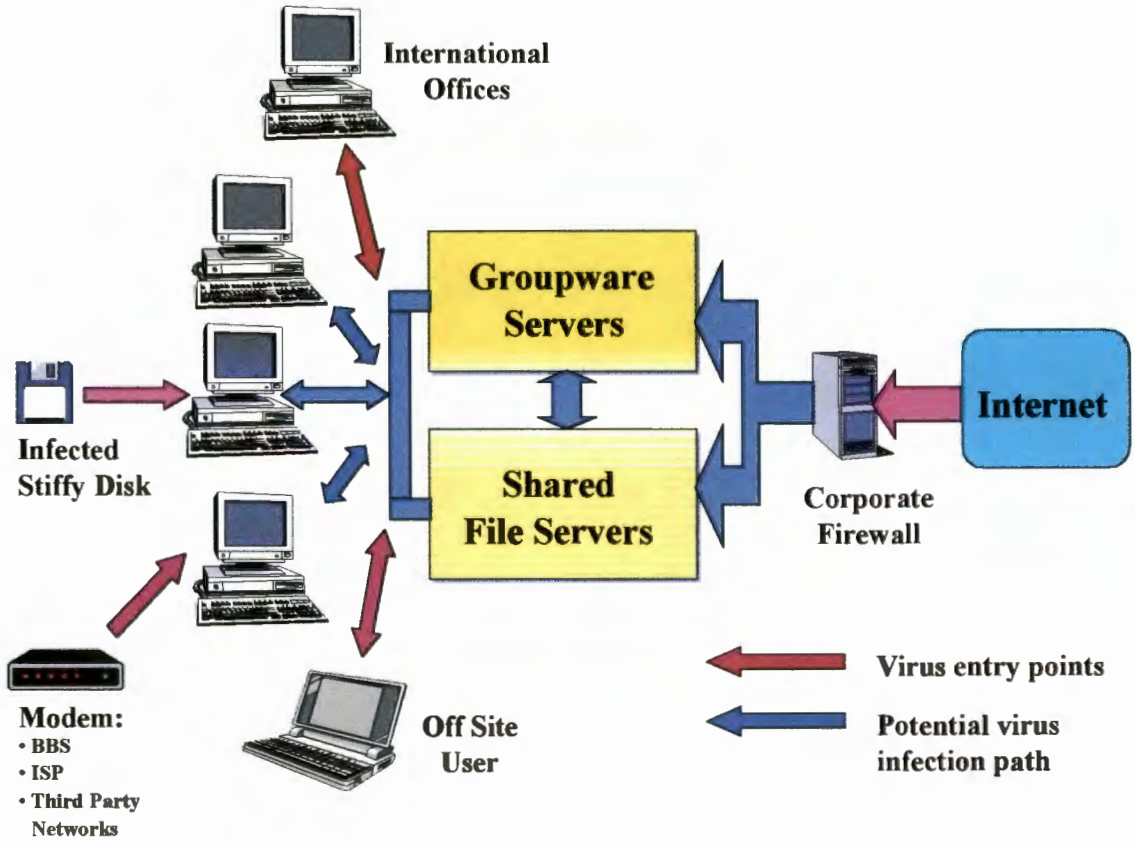
Table 3.1: Primary risks because of viruses

	Integrity	Confidentiality	Availability
Data	Change data in files; format a disk	Copy data to another file; add messages to printouts	Corrupt directories or the file allocation table (FAT); encrypt data
Systems	Damage hardware; corrupt system files; redefine keys	Write system information to a file or remote location	Lock the keyboard; slow down the system
Programs	Change programs on disk or in the random access memory (RAM)		

(Louw, 1990:82-83)

The virus threat, with the various entry points and infection paths, is illustrated in figure 3.1.

Figure 3.1: The multi-tiered virus threat



(Adapted from Anon., 1996d:1)

---

[4] The most common examples of application infectors are the 1813 or Hebrew University virus, the 1701/1704 or Hailstorm virus, and the nVIR virus (Wong & Watt, 1990:115).

[5] The most common macro viruses are the WinWord Concept, WordMacro Nuclear, and MS Word CAP virus (Orvis, 1998a and 1998b).

From figure 3.1 it is evident that the main virus entry points are via networks, infected stiffys, dial-in connections and the Internet. From the point of entry the virus goes to the server where it infects the programs.

c) Worms

Worms emerged in 1980 and are self-contained network extensions of viruses that can replicate and propagate themselves without a host carrier (McAffee & Haynes, 1989:29; Perlman, 1994:54). A worm program differs from a computer virus in that the worm seeks out new hosts across network connections to replicate itself on them, but does not cause destruction or damage the host system or its data (Louw, 1990:14; Shoch & Hupp, 1990:266-267; Wong & Watt, 1990:6). Viruses hide copies of itself inside other programs, whereas worms appear as separate and independent programs and do not change other programs (Denning, 1990:xiv; Spafford *et al.*, 1990:317). Worms use the network management mechanism of a computing system to identify free computers on the network, and to pass the worm program to the free computer (Russell & Gangemi, 1992:82). Once active, the worm keeps on finding other free computers to which it transfers a segment of itself. After the transfer the worm is embedded in a computer program. From there it is replicated and can lead to a system crash or data loss (Pfleeger, 1989:179-180).

In November 1988 Robert Morris unleashed a worm on the Internet. It targeted a back door in the sendmail binary used on Sun operating systems and made use of debugging hooks, which had not been removed from distribution software, to migrate to other UNIX systems. If the worm fulfilled its design goal, it would have constituted little more than a fascinating experiment. Unfortunately the worm contained a bug. It was intended to check for its own presence on a computer, and fail to run if a copy was already present. However, in practise the worm persistently re-infected computer after computer, bringing them to a standstill and nearly broke the Internet. This incident is documented in a technical paper, RFC 11 35, which is available on the Internet (Anon., 1998).

d) Bacteria

Although sometimes regarded as viruses, bacteria do not require a host program to infect a system. A bacterium program replicates itself and slows down the computer by acquiring as much computer time as possible. Bacteria can also fill up hard disk space (Lucas, 1997:633).

E-mail bombs

E-mail bombs fill the inbox of the company with hundreds or thousands of messages to block the use of the e-mail system (Schultheis & Sumner, 1998:660).

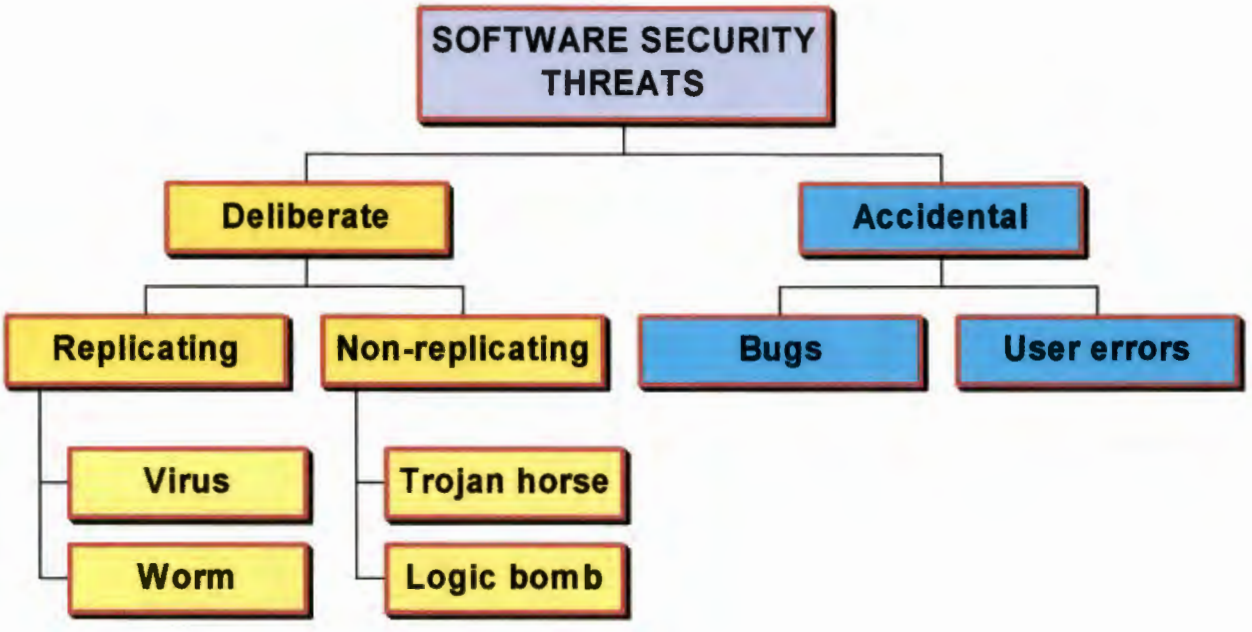
3.2.2.7.17 Electronic warfare

Various forms of electronic warfare exist to shut down the computer system of an organisation. Electronic warfare weapons include microwave or high-energy radio frequency guns (HERFs), which can shut down a computer system temporarily or permanently, and electronic magnetic pulse/transformer bombs (EMPTYs), which can erase the computer's memory (Schultheis & Sumner, 1998:660).

3.2.2.7.18 Software problems

Software security threats, which involve some of the above problems, is schematically illustrated in figure 3.2.

Figure 3.2: Software security threats



(Developed from Forcht, 1994:256-272)

Figure 3.2 indicates that there are mainly two types of software security threats, namely deliberate and accidental threats. In deliberate attacks on software use can be made either of replicating infections like viruses and worms, or non-replicating programs like Trojan horses or

logic bombs. Accidental threats consist of unintentional bugs in programs and normal user errors.

3.2.2.8 The effects of information security threats

The effects of the major information security threats that were discussed above is broadly summarised in table 3.2. Because many of the threat categories are not mutually exclusive, only two categories, namely unintentional and intentional will be used.

Table 3.2: Effects of the major information security threats

THREAT	*EFFECT*
UNINTENTIONAL	
Natural disasters (fire, floods, wind)	Computer hardware, files, and manual records may be destroyed
Electrical power (failure, spikes, surges, brownouts, blackouts)	All computer processing is halted; hardware may be damaged, or telecommunications disruptions mat occur
Hardware malfunction	Data are not processed accurately or completely
Software errors and malfunction	Computer programs do not process data accurately, completely, or according to user requirements e.g. broadcasting storms
User errors	Errors inadvertently introduced by users during transmission, input, validation, processing, distribution, and other points of the information processing cycle destroy data, disrupt processing, or produce incorrect output
INTENTIONAL	
Computer crime	Illegal use of computer hardware, software, transmission, or data results in monetary theft or destruction of valuable data or services
Computer abuse	Computer systems are used for private or unethical purposes
Vandalism and sabotage	Disgruntled employees damage computer hardware and systems

Alter (1996:652); Laudon and Laudon (1995:436); Laudon and Laudon (1997: 430-441); Mensching and Adams (1991:105-106); Menzies (1993:166-169); Robson (1997:495); and Zwass, 1992:822).

3.2.3 NETWORK SECURITY

According to Van Zyl, 1990:7-8 computer networks create a security exposure with regard to the following aspects:

- **Privacy:** Because of the many unknown users on a network the secrecy of data is threatened.
- **Data integrity:** Because more nodes and users can gain access to the system, the risk of data corruption is higher.
- **Authenticity:** It is difficult to ensure the identity of the user on a remote workstation.
- **Hidden channels:** Because of the mere amount of data transmitted on the network, it is easy to create hidden channels in the network.

In large computer networks, especially multi-location networks, there are many points on the terminal or personal computer to service host where communications can be intercepted or an intruder attack can take place. The communication links are usually ordinary telephone lines, cables, microwave links or satellite channels that can be physically intercepted through wiretap at the switch itself or at a demarcation block (where the internal and external telephone lines meet), electromagnetic emanation monitoring, active/passive invasive taps of underground cables, or interceptance of terrestrial microwave or satellite signals. Attacks also occur in an internetworking environment by subversion of a gateway (Claassen, 1994:1-10 to 1-11).

Wire tapping is a real threat to information security, especially in the case of local area networks straddling across buildings or wide area networks. Ethernet is one of the most popular topologies in the local area network arena. Because it uses broadcast technology to transmit data it is quite easy to get access to sensitive data by using a datascope, data analyser or protocol analyser. Even a personal computer connected to a spare cable access point is enough to glean useful information.

Many e-mail systems assign default passwords to new users, based on their initials, user identification or account names. The problem is that many users never change their default passwords. Sensitive information can also be accessed via the corporate electronic mail system.

Electronic data interchange (EDI) is becoming more popular, but poses some of the generic threats according to Sokol (1995:101-108), namely:

- Errors, for example human and computer errors.
- Unauthorised access.

- Unauthorised modification, for example fraud and viruses.
- Unauthorised destruction of information, for example malicious damage by employees or hackers.
- Unauthorised removal or copying of information, for example theft or industrial espionage.
- Unauthorised disclosure, for example the leaking of information to a competitor or revealing of information internally.
- Poor information system design, development and maintenance.
- Temporary unavailability, for example equipment malfunction and failures; software failures; environmental disorders (power cuts, voltage surges, static electricity discharges) and labour disputes.
- Prolonged unavailability, for example disasters (earthquakes, floods, fires, lightning, explosions, and burst water pipes).

Van Zyl (1990:6-7) stated the following reasons why networks experience the above mentioned security problems:

- **Sharing:** The possibility for unauthorised access is greater in a network because of sharing.
- **Complexity of the system:** Many operating systems are insecure. Together with the complexity it creates security risks.
- **Unknown perimeters:** The growth of networks is practically unlimited. A person on a specific network can gain access through a guest to another network.
- **Several points of attack:** The more nodes there are in a network, the more points of attack are created.
- **Unknown path:** The implementation of computer technology lead to distributed systems and many alternative communication channels. The result is that the path is often unknown.

3.3 SUMMARY

It is evident that security problems will increase because of the dramatic growth in information technology. Computer crime and fraud will become more sophisticated and popular, as organisations become more and more dependent on information systems.

The resultant escalation in the three primary risks of integrity, confidentiality and availability can mainly be attributed to the following aspects:

- Unauthorised access to the database, computer centre or network.
- Incomplete recording of data and ineffective validation tests at system or communication level.
- The presence of inadvertent human errors.
- Insufficient separation of duties in the computer environment to prevent fraud or misuse of assets.
- Unauthorised modifications to application programs or the system.
- The absence of an audit and transaction trail.
- The absence of balancing and reconciliation of the database and printouts.
- Ineffective methods of fault handling.
- Absence of a disaster recovery plan.
- Absence of an information control policy.
- Insufficient information security control by management.

If the various information security threats as discussed above and based on the above mentioned shortcomings are not addressed by senior management, it can lead to a variety of information security problems and computer crimes, which have been discussed in this chapter. The major information security threats currently experienced are external threats, internal threats, accidental threats, hardware misuse, computer fraud and crime, masquerading, pest programs, bypasses, active misuse, passive misuse, inactive misuse, and indirect misuse.

The next chapter will look at various countermeasures for these information security threats.

Smart thieves who want to get ahead will have to take up programming

Anonymous

CHAPTER 4

SOLUTIONS TO INFORMATION SECURITY PROBLEMS

4.1 INTRODUCTION

The previous chapter elucidated many and varied potential threats facing the valuable information resource. Security in computer systems is thus important so as to ensure reliable operation and to protect the integrity of stored information. Faults in the implementation of critical components can be exploited to breach security and penetrate a system. These faults must be identified, detected, and corrected to ensure reliability and safeguard against denial of service, unauthorised modification of data, or disclosure of information.

It is unfortunately not possible to build a completely secure information system because of the extent of the task, problems with cryptographic methods, insider abuse, and accessibility. Although not possible to eliminate the threats and problems discussed in chapter three, it is possible to limit and prevent it by means of effective management of information security and adequate control measures.

The aim of information security is to minimise the impact of security threats and exposures and thus to minimise business disruption, fraud, embezzlement, competitive disadvantage, lost of assets and information, faulty management decisions, overspending, lost of profit, faulty record keeping, unacceptable accounting procedures, and commercial espionage.

This chapter will therefore concentrate on various ways to minimise the impact of security threats, as well as control measures to limit the consequences of the threats.

4.2 ASPECTS OF INFORMATION SECURITY

Because of the complexity of modern information systems, information security is usually divided into a few basic areas, namely hardware, software, data processing, data transmission and personnel. It is, however, important to follow a total systems approach to obtain the

optimum level of information security (Lowe, 1994:47). It is necessary that an organisation should adopt a consistent approach to security, regularly review the sensitivity of applications, set down control policy and guidelines, and determine areas where additional security provisions should be considered, properly cost-justified if necessary. Aspects that should be considered are:

4.2.1 RISK ANALYSIS

Pfleeger (1989:457) stated quite clearly that security planning begins with risk analysis, which is a process to determine the exposures and their potential harm. An asset, a threat, together with the vulnerability that exists between them, forms a risk. The whole objective of information security is to minimise these risks by implementing specific countermeasures. These risks need to be identified (risk analysis) and protected against (risk management) (Von Solms, 1993:2).

The risk characteristics of individual computer systems should be considered with special regard to the sensitivity and value of the data being handled. The data should be examined regarding its possible misuse or disclosure, either internally or externally, to employees, the public, close competitors, or interested third parties such as suppliers and customers. The opportunities and possible consequences of the data being accessed, disclosed, modified or destroyed illegally, or service being denied, both accidentally and deliberately, should be reviewed, starting from the point of data creation, to processing, and eventually to transmission and output distribution. Eventually the business implications and system security requirements should be established (Wong & Watt, 1990:101). Because risks are only potential events, not certainties, care must be taken not to overestimate or underestimate the risks (Laudon & Laudon, 1998:626).

Risk analysis is an orderly process and consists of the following basic steps according to Pfleeger (1989:458-465):

- Identification of assets, for example hardware, software, data, people, documentation and supplies.
- Determination of vulnerabilities, for example effects of natural and physical disasters, outsiders, malicious insiders, and unintentional errors.
- Estimation of the likelihood of exploitation.
- Computation of the expected annual loss.

- Surveying of applicable controls and their costs, for example cryptographic controls, secure protocols, program development controls, program execution environment controls, operating system protection features, identification, authentication, secure operating system design and implementation, database reliability controls, database inference controls, multilevel security controls, personal computer controls (procedural, physical, hardware, and software), network access controls, network integrity controls, controls on telecommunications media, physical controls, and physical devices.
- Projection of the annual savings of controls.

4.2.3 RISK MONITORING

According to Wong and Watt (1990:107) a good security journal should be implemented with the following reporting facilities, with relevant abstracts issued to the manager, security officer or person responsible for information security:

- Security violations, including details of attempts to use incorrect passwords to access the system (successfully or unsuccessfully), authorised users attempting to gain illegal access to other user's files, or trying to write to files when only read access was allowed.
- An audit trail of user and work station activities, namely date and times of start and finish of each session, network connection point, user identity, application, software utilities and files accessed, read or written to, and the number of pages printed or bytes copied

4.2.4 RISK CONTROL

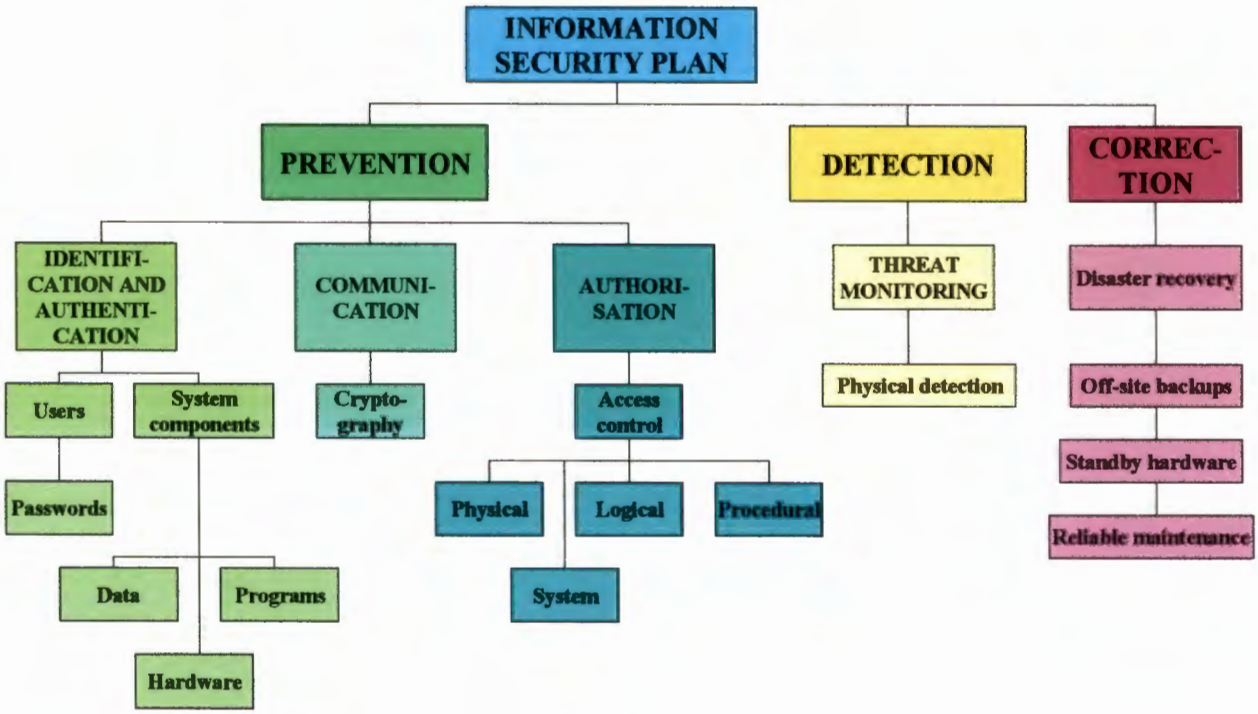
Trickett (1972:14-15) stated that information security risk control basically entails five elements, namely:

- **Setting of standards:** Before a control system can be implemented, it is necessary to establish standards of information security.
- **Measurement of performance:** It is essential that the actual performance of information security controls be measured.
- **Comparison of the actual performance against the standards:** The actual measured performance of the control system is compared against the predetermined standards and the deviation is analysed.

- **Corrective action:** The manager is required to analyse the causes of the deviations and to develop controls to restore the desired level of information security.
- **Evaluation of the effectiveness of the corrective action:** After the implementation of corrective action, it is essential that the effectiveness of the new controls be evaluated to ensure the desired information security level is restored.

To implement the elements as mentioned above, various methods of control exist, for example determent, prevention, detection (tracking), recovery, rectification, reporting and response (Bezuidenhout, 1981:42). These methods of control are schematically presented in figure 4.1 and discussed below.

Figure 4.1: Methods of control



4.2.4.1 Prevention

Lubbe and Amstrong (1995:24) adequately pointed out that absolute information security is impossible to achieve, but well-planned and well-instituted prevention is a good second. It is important to prevent first, detect later, and then finally correct. The conclusion is that all points of penetration prevention and detection including before (software analysis, integrity reviews,

testing, programming standards), during (checksums, table integrity), and after (table status, audit trails) penetration need to be considered (Lodin *et al.*, 1997).

Although expensive, the main aim is to prevent fraud from occurring, or at least to reduce the frequency of fraud incidents and to contain the size of the loss sustained. Preventative controls include logical access control according to the least privilege principle, program passwords and keywords, segregation of sensitive duties, and security awareness training. Part of prevention is also determent controls to discourage any unauthorised access, for example by means of a security profile, control over physical keys, and security personnel (Wong & Watt, 1990:80-82).

The use of a system that provides for strong user authentication, access control, and integrity protection (for example incorporating the Secure-Sockets-Layer (SSL) on Windows 95 or Windows NT servers) for unclassified but sensitive data on a private (isolated) network or collection of networks is of great importance (Tabibian, 1995:75). The system must also support the secure connection of the private network to an external Internet, as well as dial-up network connections to the private network, via a firewall and secured links, with strong user authentication and encryption of traffic. Either commercial off-the-shelf (COTS) software or custom software can be used to provide these services (Avolio & Ranum, 1997).

4.2.4.1.1 Virus-prevention

Kephart (1997) stated that computer viruses are one of the first forms of artificial life to have had a measurable impact on society. Currently, viruses are a relatively manageable nuisance. However, two alarming trends are likely to make computer viruses a much greater threat. First, the rate at which new viruses are being written is high, and accelerating. Second, the trend towards increasing interconnectivity and interoperability among computers will enable computer viruses and worms to spread much more rapidly than they do today. To address these problems, use can be made of an innovative new immune system for computers and computer networks that takes much of its inspiration from nature. Like the vertebrate immune system, the system develops antibodies to previously unencountered computer viruses or worms and remembers them so as to recognise and respond to them more quickly in the future. However, a risk of an auto-immune response, in which the immune system mistakenly identifies legitimate software as being undesirable, do exist. At the same time nature's technique of fighting self-replication with self-replication, which has been shown by theoretical studies to be highly effective, can be employed.

Even with a protection strategy in place, employees cannot always be relied on to check and clean their disks. A solution is to make use of a program like Disknet, which throws a security net around a file server with mission-critical data by not allowing infected or foreign disks to write anything to the hard drive or network drive (Bowen, 1995:98).

Another basic method of protecting computer systems against viruses can be viewed generally as the problem of learning to distinguish self from other. This method of change detection is based on the generation of T cells in the immune system (Forrest & Perelson, 1997).

Perlman (1994:57) and Holton (1996) suggested the following steps to prevent virus attacks (also compare Anon., 1990:5-6):

- Establish a corporate virus policy that should spell out clear guidelines and standards.
- Train personnel, because a policy without a necessary awareness program and training to recognise the early warning signs of viruses can be futile.
- Enforce password management procedures by instructing employees to take password selection seriously.
- Control the uploading of programs from the micro to the server or mainframe.
- Test new or upgraded software in an isolated computer environment. The separation of test and production machines is a good idea.
- Back up data and programs on a regular basis and store them offsite.
- Establish an effective disaster recovery plan.
- Purchase software from reputable sources and do not permit employees to download freeware or anti-virus software from the bulletin boards or the Internet. Use of foreign software obtained from external organisations without prior approval should be prohibited.
- Make use of signature scanning, file checksumming and virus guards for desktop computers, Internet browsers, e-mail, servers, networks, GroupWare, and gateways.

Louw (1990:4, 85-86) and Van Dyk (1990:32-37) emphasised that a strategic approach to the virus problem is necessary for long-term success. The management emphasis should centre on awareness, good judgement and contingency planning. Virus security should therefore include prevention, detection and recovery aspects. Brothers (1990:359-364) suggested that to protect information against viruses the methods of write-protection, limited machine and media access,

and back-ups should be used. The use of anti-viral software, and diskless terminals or PCs can also be considered (Spafford *et al.*, 1990:331-333). Wong and Watt (1990:98-100) argued that it is good practise to forbid external diskettes to be used on the organisation's computer system unless they are screened.

4.2.4.1.2 Firewalls

As the number of businesses and government agencies connecting to the Internet continues to increase, the demand for Internet firewalls - points of security guarding a private network and data from intrusion by enforcing access control - has created a demand for reliable tools from which to build them (Ranum & Avolio, 1997; compare Reichard, 1995:84).

Connecting to the Internet exposes some subset of the enterprise network resources, called the zone of risk, to Internet-based attacks from any of millions of Internet users. According to Angell and Heslop (1995:46) one way to reduce this exposure is to reduce the zone of risk to a small number of extremely secure hosts. These secure hosts are collectively referred to as a firewall. An Internet firewall allows enterprise network administrators to implement strict access controls, including strong authentication methods such as token authentication, between the Internet and the enterprise network (Robinson, 1997). Numerous variations of firewalls exist and include simple traffic logging systems, Internet protocol (IP) packet screening routers (packet-filtering gateways), hardened firewall hosts, and proxy application gateways. Unfortunately, as pointed out by Kalakota and Whinston (1997:126-133), firewalls are not impenetrable and must be part of a consistent overall organisational security architecture to deter network penetration (Laudon & Laudon, 1998:639).

Different categories of firewalls can be identified:

Packet filtering firewall

Ever-increasing numbers of Internet protocol (IP) router products are offering packet filtering as a tool for improving network security. Chapman (1997), however, warned that when used properly, packet filtering is a useful tool for the security-conscious network administrator, but its effective use requires a thorough understanding of its capabilities and weaknesses, and of the quirks of the particular protocols that filters are being applied to.

By using existing information in packet headers, routers can provide system administrators a facility to manage network connections between computers. Host address, network number, interface, direction, protocol, and port number, are parameters that may be used to implement an access control policy (Corbridge *et al.*, 1997).

Laudon and Laudon (1998:639) suggested that one way to restrict access is to prevent certain packets from entering or leaving an organisation through its gateways by using efficient mechanisms for screening the Internet protocol (IP) packets that flow through a gateway.

Application gateway

Schauer and Wolfhugel (1997) stated that information is the lifeblood of the computer age, and network connectivity is crucial to day-to-day business. As needs for both connectivity and security increase, it becomes necessary for organisations to build and manage secure Internet gateways. Connecting a private, corporate network to the Internet is not acceptable without some form of secure gateway acting as a firewall between the two networks, to prevent miscreants and unwelcome visitors from accessing hosts on the private network. In the case of a software or hardware vendor, source code, computer aided design (CAD) diagrams, and other product-specific information must be kept secret. Hospitals and insurance companies that maintain confidential information, or pharmaceutical research labs with patent applications, cannot afford to take chances with data theft. A break-in over the network could do incalculable damage in a very short time. One way of preventing break-ins is to make use of several gateways between the corporate network and the Internet, with a high degree of access while maintaining excellent security. Gateways are usually composed of multiple machines acting together, and a specially configured packet-screening machine that provides discretionary transmission control protocol/Internet protocol (TCP/IP) access control. Ranum (1997) emphasised that software must be configured across the gateways to provide transparent USENET, secure mail transfer protocol (SMTP mail), file transfer protocol (FTP), and name service, while preventing direct connections between internal machines and external machines. Special software is usually used to restrict traffic to a particular application, such as e-mail or Novell GroupWise (Laudon & Laudon, 1998:639).

Circuit–level gateway

According to Laudon and Laudon (1998:639) a circuit level gateway connects an outside discretionary transmission control protocol/Internet protocol port to an internal destination such

as a network printer. It acts as an intelligent filter to distinguish a valid transmission control protocol or user datagram protocol (UDP) session.

Proxy server

A proxy server maintains replicated copies of Web pages for easy access by a designated class of users. It thus allows outside visitors to access this information while keeping them away from more sensitive information (Laudon & Laudon, 1998:639).

Stateful inspection

Laudon and Laudon (1998:639) stated that stateful inspection entails technology that derives information from the state of transmission and applies it to the organisation's business rules. The state information is then stored to provide a context for examining messages from identical sources.

4.2.4.1.3 Assured pipelines

Reichard (1995:84) mentioned that for a higher level of security than firewalls, expensive assured pipelines could be used. Assured pipelines use more sophisticated methods to prevent access. Unlike the firewall, which only looks at the header of a packet, an assured pipeline looks at the entire request for data and then determines whether the request is valid or not.

4.2.4.2 Detection control or tracking

Early detection of potential abuse can serve to reduce corporate losses. Effective monitoring resulting in a high risk of detection would serve as a determent to potential perpetrators.

Kumar (1997) reasoned quite correctly that computer and network systems are vulnerable to attacks. Abandoning the existing huge infrastructure of possibly insecure computer and network systems is impossible, and replacing them by totally secure systems may not be feasible or cost effective. Some computer security breaches can just not be prevented using access and information flow control techniques. These breaches may be a consequence of system software bugs, hardware or software failures, incorrect system administration procedures, or failure of the system authentication module. Intrusion detection techniques, which involves the tracing of

information to ensure correct and authorised processing of transactions, can have a significant role in the detection of computer abuse in such cases.

According to Kumar (1997) intrusions can generally be divided into six main categories:

- Attempted break-ins, which are detected by atypical behaviour profiles or violations of security constraints.
- Masquerade attacks, which are detected by atypical behaviour profiles or violations of security constraints.
- Penetration of the security control system, which is detected by monitoring for specific patterns of activity.
- Leakage, which is detected by atypical use of system resources.
- Denial of service, which is detected by atypical use of system resources.
- Malicious use, which is detected by atypical behaviour profiles, violations of security constraints, or use of special privileges.

Although there are six categories of intrusions, Sundaram (1998) pointed out that the techniques of intrusion detection can be divided into only two main types:

Anomaly detection. Anomaly detection techniques assume that all intrusive activities are necessarily anomalous. This means that if a "normal activity profile" could be established and a "current activity profile" for a system maintained, all system states varying from the established profile by statistically significant amounts could, in theory, be flagged as intrusion attempts. Three of the major approaches to anomaly detection systems are statistical approaches, predictive pattern generation and the use of neural networks

Misuse detection. The concept behind misuse detection schemes is that there are ways to represent attacks in the form of a pattern or a signature so that even variations of the same attack can be detected. This means that these systems are not unlike virus detection systems - they can detect many or all known attack patterns, but they are of little use for as yet unknown attack methods. An interesting point to note is that anomaly detection systems try to detect the complernent of "good" behaviour. Misuse detection systems try to recognise known "bad" behaviour. Some of the systems used for misuse detection are expert systems, keystroke

monitoring, model based intrusion detection[1], the state transition analysis technique and pattern matching.

Ko *et al.* (1997) showed that a common element in many attacks is that a single user will often attempt to intrude upon multiple resources throughout a network. Detecting the attack can become significantly easier by compiling and integrating evidence of such intrusion attempts across the network, rather than attempting to assess the situation from the vantage point of only a single host. To solve this problem, use can be made of an approach for distributed recognition and accountability (DRA) that consists of algorithms which "process", at a central location, distributed and asynchronous "reports" generated by computers (or a subset thereof) throughout the network. The highest-priority objectives are to observe ways by which an individual moves around in a network of computers, including changing user names to possibly hide his/her true identity, and to associate all activities of multiple instances of the same individual to the same network-wide user.

The use of an integrity checker for intrusion detection, like the program Tripwire, is important for any system administrator who operates sites employing modern variants of the UNIX operating system (Kim & Spafford, 1997a). Tripwire uses interchangeable "signature" routines to identify changes in files, and is highly portable, configurable tool (Kim & Spafford, 1997b). It keeps a database of inode information and message digests of file and directory contents, based on a user-designed configuration file. When rerun, Tripwire will compare the stored values against the configuration flags and warn the operator of any deviations (changes, additions, and accesses). Tripwire is extensively documented, has been ported to over thirty varieties of Unix, and is highly recommended by most people who use it (Kim & Spafford, 1997c).

Misuse intrusion detection, according to Kumar and Spafford (1997) has traditionally been understood in the literature as the detection of specific, precisely representable techniques of computer system abuse. Pattern matching is well disposed to the representation and detection of such abuse. Each specific method of abuse can be represented as a pattern and many of these can be matched simultaneously against the audit logs generated by the operating system kernel. Using relatively high level patterns to specify computer system abuse relieves the pattern writer from having to understand and encode the intricacies of pattern matching into a misuse detector.

---

[1] To determine significant variations in transaction patterns computer modelling are often used. The variations are further investigated for

Patterns represent a declarative way of specifying what needs to be detected, instead of specifying how it should be detected. A model of matching, based on coloured petri nets, was specifically designed for misuse intrusion detection.

Other intrusion detection systems that are well known are advanced security audit trail analysis on Unix (ASAX) (Habra *et al.*, 1997a; 1997b; Mounji, 1997), IDIOT (Crosbie *et al.*, 1997), graph-based intrusion detection system (GrIDS)[2] (Staniford-Chen *et al.*, 1997) and state transition analysis tool for UNIX (USTAT)[3] (Ilgun, 1997).

Frank (1997) indicated that intrusion detection systems (IDSs) have previously been built by hand. These systems have difficulty successfully classifying intruders, and require a significant amount of computational overhead making it difficult to create robust real-time intrusion detection systems. Artificial intelligence (AI) techniques can reduce the human effort required to build these systems and can improve their performance. Learning and induction are used to improve the performance of search problems, while clustering has been used for data analysis and reduction. Artificial intelligence has recently been used in intrusion detection for anomaly detection, data reduction and induction, and the discovery of intruders that created "private" communication services undetectable by normal means.

Another solution used in intrusion detection is a combination of work in the fields of artificial life and computer security. Autonomous agents, which are built by using genetic programming, are used (Crosbie & Spafford, 1997).

4.2.4.3 Correction

The last aspect of risk control, namely correction, according to Bezuidenhout (1988:51-52), entails various aspects, namely recovery, rectification, report and response.

---

possible fraud abuse (Wong & Watt, 1990:57-58).

2 GrIDS collects data about activity on computers and network traffic between them. It aggregates this information into activity graphs, which reveal the causal structure of network activity. This allows large-scale automated or co-ordinated attacks to be detected in near real-time. In addition, GrIDS allows network administrators to state policies specifying which users may use particular services of individual hosts or groups of hosts. By analysing the characteristics of the activity graphs, GrIDS detects and reports violations of the stated policy. GrIDS uses a hierarchical reduction scheme for the graph construction, which allows it to scale to large networks (Staniford-Chen *et al.*, 1997).

3 USTAT is a real-time intrusion detection tool that makes use of audit trails and keeps track of only those critical actions that must occur for the successful completion of the penetration. This approach differs from other rule-based penetration identification tools that pattern match sequences of audit records (Ilgun, 1997).

Recovery: Recovery controls are a result from detection controls and ensure the correct reprocessing and repair of the processing process.

Rectification: Corrective controls are a result of either preventative or detection controls. In the first instance it includes procedures for the rectification of transaction errors and in the second instance faulty task procedures or unauthorised transaction processing.

Reporting: Reporting controls are a result of detection controls and are usually in the form of error reports, variance reports and error messages on the computer screen.

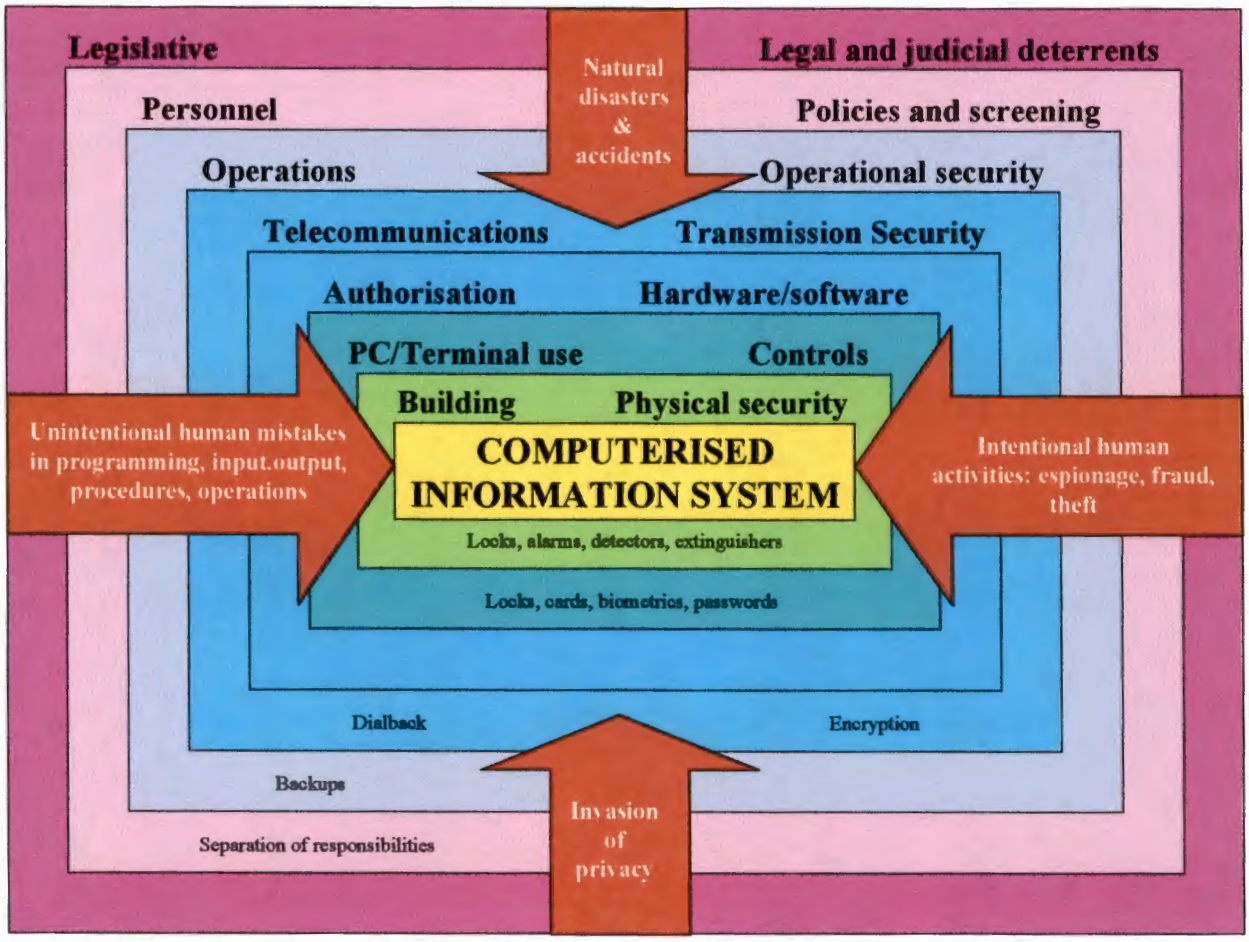
Response: Although adverse publicity is a problem, it is necessary to prosecute because it will act as a deterrent to possible intruders.

4.3 INFORMATION SECURITY CONTROLS

Information security control is one of management's fundamental responsibilities because of the significant capital and operating investment in information technology (Lucas, 1997:617-618). Effective manual and automated controls are needed to ensure information security and to minimise errors, fraud, computer crime, and destruction of valuable information (O'Brien, 1998:546).

The various layers of control in order to deter or limit the information security threats are illustrated in figure 4.2:

Figure 4.2: Layers of control



Adapted from Hussain and Hussain (1992:161-171)

The layers of controls necessary to ensure the quality and security of information and to limit the impact of natural disasters, to prevent intentional and unintentional human activities, and to deter the invasion of privacy, begins with legislative control measures, which are usually outside the jurisdiction of the organisation. However, the organisation can implement administrative, operational, transmission, information systems, and physical controls. These controls will be explained in more detail below.

Although the various information security controls will be organised and discussed in seven categories, the categories are not absolute and controls often overlap. Information security controls will thus be discussed in the category where the major security role is fulfilled.

4.3.1 ADMINISTRATIVE CONTROLS

Not all controls can be imposed by the computer system. Some controls must be applied by administrative procedures, for example standards of program development (design, documentation, language, coding style, programming, testing, and configuration management), security audits, separation of duties, background investigation of employees prior to hiring them and an investigation of employees on a regular basis (Pfleeger, 1989:190-191; Rorbye, 1993:26).

Laudon and Laudon (1998:640) define administrative controls or management controls, as it is often called, as formalised standards, rules, guidelines, policies, and control disciplines to ensure that the organisation's information security controls are properly executed and enforced.

4.3.1.1 Security policies, procedures and guidelines[4]

The results of the risk analysis of the computer systems should be used to derive a suitable security policy, which stipulates the corporate position regarding the security of information, as well as indicates how staff are accountable for their actions regarding the use of system resources, and the access, disclosure, modification and destruction of information (Fitzgerald, 1994:11; Wood, 1995:667). Usually the information security policy serves three main purposes, namely to define the information security requirements, to allocate responsibilities, and to contribute directly to control (Pottas, 1995:80). It is, however, important that policies and procedures are formalised in writing and authorised by the appropriate level of management. Responsibilities and accountabilities should be clearly stated (Laudon & Laudon, 1998:640).

Wong and Watt (1990:101-103) argued that guidelines should be available to all computer users to implement the security policy, for example guidelines concerning equipment and software purchase, facilitation of maintenance, networking to the host computer, restriction of hardware usage (for example business use only), and connection to other systems.

Computer users should be given clear guidelines on what type of data may be downloaded from the host, and may be taken home to work on or to process. Guidelines should also be given when to use encryption and authentication techniques to protect the secrecy and integrity of sensitive data.

Users should be clearly briefed on their responsibility for the protection of hardware, software, data and other resources, as well as their responsibility for data integrity, for example error detection and correction in data entry. Departmental managers should be issued with guidelines on individual responsibility for control, supervision, and monitoring of normal operations, and taking corrective action for any security breaches.

Operational procedure guidelines should be provided to end users regarding logging requirements for processing activities and sensitive events, regular backup and copying, as well as expedient reporting of faults, suspected security breaches and access violations. Guidelines should also be provided on the testing and documentation of end user programs.

4.3.1.2 Personnel controls

Information security is a fundamentally human issue (Cunningham, 1989:165), and therefore the most sophisticated information security technology will not be effective unless the human element has been adequately addressed (Wood, 1995:667). Possibly the weakest link in the security system is the people who have direct or indirect access to the system (Witten, 1990:105). According to Wong and Watt (1990:33) computer experts have pointed out quite correctly that seventy to eighty percent of information security breaches are inside jobs, mostly by disgruntled or dishonest employees (compare also Alexander, 1995:30-31).

Personnel security therefore involves personnel controls (job rotating practise, dismissal and resignation procedures, employment and selection procedures, training and awareness of 1information security, handling of personnel who may be a security risk), organisation controls (supervision procedures, documentation of standards and procedures, allocation of responsibilities with regard to resources and assets, job descriptions and procedures for the responsibility with regard to the execution of work assignments) and control of outside parties involved in the information environment (Bezuidenhout, 1988:45; Rilley, 1981:37-38).

However, the area of personnel security is the most difficult to address. This is probably the reason why management often neglects this aspect and rather prefers to believe that security

---

[4] This aspect will be discussed more thoroughly from a management perspective in chapter 5.

breaks come from outsiders. To assist the other security measures, attention will have to paid to the following aspects:

4.3.1.2.1 Selection

Selection and security clearance, especially for personnel of the information technology department, is of the utmost importance. Aspects that should be addressed within ethical limits are background, general alliances, integrity, political alliances, behavioural patterns, personality, financial steadfastness, employment history, and references (Du Toit, 1992:62-64).

4.3.1.2.2 Employment

Du Toit (1992:64) emphasised that when a prospective employee passed the selection process, an employment contract should be drawn up and signed. This contract should have a confidentiality agreement section that should at least include the following information:

- Personal security responsibilities.
- Disciplinary action when security measures are not adhered to.
- Any contractual obligations that the employee may have when leaving the organisation.
- Rules in connection with publication of any material that involves the organisation.

4.3.1.2.3 Security awareness and attitude of employees

According to Wong and Watt (1990:107-108), the attitude of employees with regard to information security is probably one of the most important factors for the successful implementation of the information security policy. This is the reason why continual security training and motivation are so important.

Most computer users dislike any control measures, which they perceive to be counter-productive in their work. It is therefore necessary to convince them of the importance of information security. Good security awareness will only come with constant reminders, in the form of regular training sessions, news bulletins, posters, and personal contacts from the corporate information technology security function.

Users should be encouraged to follow appropriate security procedures, to report any suspected security breaches, and to appreciate that any successful attempts at illegal access or sabotage

could directly affect their own office or work performance and productivity, as well as the well-being of the whole organisation.

Du Toit (1992:65-66) reasoned that it is a good idea to compile a complete information security manual, which includes the confidentiality agreement that was signed by the employee. Information security should form an integral part of an employee's job description. However, employees should be brought to the point where they are convinced that it is in their best interest to be security conscious.

The inclusion of security objectives in the business plan can also further active participation in the promotion of information security. Middle and senior management can be measured according to these objectives during performance evaluation.

4.3.1.2.4 Segregation of functions

To minimise the risk of errors or fraudulent manipulation of information or assets, this classic form of control entails that job functions should be segregated. According to this control the ability of any one individual to carry out sensitive tasks for a business transaction from beginning to end is reduced. Employees responsible for operating systems should not be the same people who can initiate transactions that change the assets held in these systems. For example, the function responsible for placing orders for materials should be separated from the function which receives the materials and certifies their acceptance of the quantity of delivery (Wong & Watt, 1990:44-45).

Laudon and Laudon (1998:640) pointed out that it is best to divide the responsibilities for input, processing and output among different employees. Within the information systems department is also a good idea to separate the duties of programmers and analysts from those of computer equipment operators.

It is however true that network computing has to a great extent broken down the separation of tasks. A new approach where every user is personally accountable for a list of duties is therefore necessary. Systems managers should minimise the amount of trust between users and audit all work (Stang, 1992:71).

4.3.1.2.5 Supervision

To ensure that the controls for an information system are functioning as intended and to detect weaknesses, correct errors, and identify deviations from standard procedures, supervision should be instituted (Laudon & Laudon, 1998:640).

4.3.1.2.6 Security inducive environment

To create an environment where the information security risk is minimised, a good moral, competency, openness, loyalty and integrity should be maintained by creating a framework for employees where they can experience job satisfaction, quality of work life and growth.

Aspects that will further information security are task rotation, limiting of excessive overtime and limiting of authorisation (Du Toit, 1992:66-67). Stang (1992:72) rightly pointed out that it would also be inducive to provide regular security training and to incorporate information security in the employee performance and appraisal system.

4.3.1.2.7 Termination of service

Clear termination of service procedures should exist and be implemented to ensure that all documents, magnetic media, access cards, keys and other information are obtained from the employee. Employees should sign a contract before leaving, stating that they would not disclose any information. Passwords and user numbers should immediately be changed (Du Toit, 1992:68).

4.3.1.2.8 Contract and maintenance personnel

It is extremely important that external contract and maintenance workers, as well as consultants sign the confidentiality agreement. Access of maintenance personnel to sensitive information should be barred (Du Toit, 1992:67-68).

4.3.1.2.9 *Quis custodiet ipsos custodes?*

Even in systems where information security is tightly controlled, the problem remains of who will guard the guards themselves? Despite all technical means to ensure information security, eventually people will have to be trusted. Mutual trust is one of the cornerstones of information security (Witten, 1990:106-107).

4.3.2 PHYSICAL CONTROL

Physical controls involve protection outside the computer system and usually include facilities such as guards, locks, and fences. Probably one of the most important preventative measures is not to have file servers distributed around offices, but to house them in a secured and controlled server room (Boyle, 1996:1).

4.3.2.1 Physical security

According to Hoffman (1973:44) physical security generally refers to countermeasures available to protect tangible assets and is the first line of defence for any computer system or installation. Ideally offices with computer systems should always be locked up when unattended. Tapes and diskettes not in use should be kept in a secure cabinet or safe. To deter the theft of computer equipment, security cables to thread the monitor, keyboard and printer together can be used. Equipment cover locks for work stations are available to deter tampering inside the cabinet and to reduce the risk of office users attempting to remove computer parts for use at home (Wong & Watt, 1990:104).

Physical security comprises access control to the network, program documentation, computer centre and backup store. Physical security facilities include locks on doors, guards at entry points, backup copies of important software and data, and a well planned computer centre or server room (Bezuidenhout, 1988:44; Pfleeger, 1989:15).

4.3.2.1.1 Concentric boundaries of control to protect assets against unauthorised access

Du Toit (1992:33-34) and Forcht (1994:63) indicated that to protect information assets physical security can be organised according to concentric boundaries, which each requires a different type of control.

- **The outer boundary:** Vehicle control, vehicle identification, security personnel.
- **The building boundary:** Control of all material or equipment entering or leaving; positive identification of individuals; automatic access control system; control of visitors. Special care should be taken of user materials, carriers, communication components and printers (Stang, 1992:70).
- **The computer centre boundary:** Stricter access control.

- **The computer or server room:** Very limited access; safeguarding of magnetic media; careful selection of personnel.

4.3.2.1.2 Physical access control

Linked closely to physical security are access considerations. Buildings should be designed to facilitate access control. Different levels of access to sensitive and computer areas should be planned very carefully (Rilley, 1989:36). Hardware and software access devices, call-back devices, passwords, encryption, firewalls and audit trails can be implemented (Lowe, 1994:56-59). Access control remains one of the very effective control measures of physical security and often entails the following aspects:

- Identification of personnel through magnetic employee identification cards, personal identification numbers, passwords, lock combinations and/or any other access algorithm. Automatic or electronic access control has the benefit of accurate logs of all entries and exits. A more expensive alternative is the use of fingerprints, handprints, retina patterns, neural network face recognition, thermal facial readers, voice recognition, signature recognition, keystroke patterns, passive cranial scan, skin cell printing, blood and saliva testing or any other biometric control system (Cloete, 1995:39-50; Russell & Gangemi, 1992:246-252; Post & Anderson, 1997:676).
- Visitors must be under supervision of an authorised employee (Du Toit, 1992:34-37).
- Access control systems should not restrict the flow of traffic (Anon., 1989:3).
- Guard patrols and television surveillance (Forcht, 1994:46).

4.3.2.1.3 Physical security vulnerabilities

To manage the problem of physical security four vulnerabilities need to be addressed, namely natural disasters, human intrusion, and interception.

<u>Natural disasters</u>

Schultheis and Sumner (1998:656) emphasised that computer facilities and valuable data should be protected against fire, floods, earthquakes and other natural disasters by means of a fire control system (smoke and heat detectors; fireproof walls) and a water warning system.

Human intrusion

To address the human intrusion vulnerability, attention will specifically have to be paid to theft prevention. Personal computers and floppy disks are easily carried away. According to Pfleeger (1989:444-446) and Russell and Gangemi (1992:246-248), there are mainly three approaches to prevent theft of these items, namely to prevent access and portability or to detect exit.

- **Access control:** The oldest access control is a guard who keeps an accurate record of everyone who has entered the facility. The second oldest access control is a lock. The problem is that a lock provides no record of access, and there are difficulties of lost and duplicated keys. More modern access control devices employ cards with radio transmitters, magnetic stripes, and cards with electronic circuitry that makes them difficult to duplicate. Biometric control based on the unique physiological, behavioural, and morphological characteristics of every person, can also be implemented and probably provide the best form of access control.

- **Preventing portability:** The simplest way to prevent theft is to lock the room containing a computer. Use can also be made of cables, lockable cabinets or fibre optic cable that sounds an alarm if the cable is cut or broken.

- **Detecting exit:** Because it is absolutely impractical to chain every piece of equipment or media down, use can be made of security code tags or radio transmitters that are sensed by a detector mounted by the exit of the premises.

Interception

To counteract interception vulnerabilities, controls regarding the disposal of media, protection against emanations and port protection will have to be instituted.

Disposal of sensitive media

When disposing of draft copies, care should be taken to dispose both of the hard and magnetic copies. Magnetic data should be overwritten several times, using different patterns each time, because the erase or delete command often just changes the directory pointer, leaving the sensitive data still recorded on the medium. To prevent sensitive residual data on disk, the magnetic media should either be degaussed properly or the data should positively be overwritten

several times. The most secure and much faster way is to use a degausser that generates a magnetic flux and realign all magnetic charges (Pfleeger, 1989:446-447).

Protection against emanations

Computer screens, printers, disk drives and central processing units give off emissions that can be detected from a distance. Essentially there are two approaches to prevent the emission of sensitive information, namely enclosing the device and modifying the emanations. Enclosing the device in a copper conductive case will defuse the emissions. Because this approach is not always practical, it is much better to modify the emanations by adding spurious signals (Pfleeger, 1989:447-448).

Port protection

Dial-in modem ports are a real threat to information security. Security controls include dial-back connections, complex authentication schemes, silent modems, and a complete log of calls, rejected communications, and operator actions (Pfleeger, 1989:448-450).

4.3.2.2 Environmental control

Computers are extremely vulnerable to poor quality of the power supply, which affects their proper working and results in hardware failure and data corruption. Therefore large voltage or frequency fluctuations, power spikes or frequent outages should be avoided through the installation of devices aimed at smoothing out the power supply and delivering an uninterrupted power supply (O'Brien, 1998:554; Zwass, 1992:830).

Static electrical charges can build up in office personnel and could damage the circuit boards or memory. Anti-static mats should be provided to minimise the risk. Reducing the presence of smoke and dust to a low level will prolong the life of equipment and magnetic media (Wong & Watt, 1990:103-104).

Tackett *et al.* (1995:621-622) also mentioned that the environment should be kept as stable as possible by controlling of the temperature and humidity.

4.3.2.3 Hardware controls

Hardware controls ensure that the hardware is physically secure and can only be accessed by authorised people. It also monitors for equipment malfunction by means of parity checks or the check for altering of bits within bytes; validity checks or the monitoring of the structure of on-off bits within bytes; and echo checks, which verify that the hardware devices are performance ready (Laudon & Laudon, 1998:637).

4.3.2.4 Software controls

Software controls or program security are necessary to ensure the security and reliability of software. Software controls regulate the use of systems software and prevent unauthorised access of software programs, system software, and computer programs (Laudon & Laudon, 1998:636).

According to Lodin *et al.* (1997) the three major reasons for penetrations are:

- The software change cycle is more frequent (due to the market being more money driven).
- There is more and larger software to be subverted.
- Software maintenance becomes an issue.

To counter attacks on information security, controls such as operating system controls and program security controls can be considered.

4.3.2.4.1 Operating system and program security controls

These controls comprise limitations enforced by the operating system to protect each user from all other users. Use can be made of trusted software (functional correct, enforced integrity, limited privilege, and an appropriate security level); mutual suspicion between programs; confinement of suspected programs; compartmented information; and an access log to list who accessed which computer objects, when, and for what amount of time (Pfleeger, 1989:14, 187-190).

Unfortunately the UNIX operating system was developed for use in non-hostile environments like research laboratories and universities, and therefore never intended to have a high degree of security. As a result, the sharing of files, data, devices, and storage volumes is relatively simple and unhindered by a strong protection mechanism. UNIX thus offers only rudimentary security

features, such as identification number; password control and ageing; overwriting of residual memory data; read or write-only access; non-display of password on the screen; and encryption of the password file. However there are also a number of well-documented serious flaws in the range of security features provided. The "super-user" function, that can perform basically any operation in the system, is very powerful and therefore the object of many system attacks. Another problem is that a user sharing access to a system program can obtain high security rights if the system program runs in "setuid" mode. Directories, input/output devices and even parts of memory are all files to UNIX and therefore accessed with the same structure. File access permission is checked only once, when the file is opened. By changing the characteristics of the file or device after it has been opened, a user can obtain unlimited access permission. Secure systems like the Honeywell SCOMP, UCLA secure UNIX, and kernelised VM/370 are available (Pfleeger, 1989:287-288).

According to Laudon and Laudon (1998:636-637) program security controls prevent unauthorised changes to programs that are already in use.

4.3.2.5 Network security

The connection of computers by means of a network increases the risk of breaks in security. The network therefore has to be protected from illegal and improper use (Elliot & Starkings, 1998:268; Lowe, 1994:19-20). The network must thus ensure integrity of data, secrecy of data, and availability of service. This is, however, extremely difficult because of sharing; complexity of the system; unknown perimeters; many points of attack; and unknown paths from one host to another. Networks are therefore exposed to a lack of privacy; data corruption; unauthorised access; and the construction of covert channels for data flow (Pfleeger, 1989:364-374).

Network and terminal (or personal computer) security include the documentation of the use of the network; protection of network control programs; protection of data lines; procedures to prevent the avoidance of the network control system; automatic log off procedures if not in use for a pre-specified time; and the implementation of a physical and logical security system with regard to terminals or personal computers. Workstation or terminal controls include the physical protection of workstations to prevent unauthorised use (Stang, 1992:74).

Lowe (1994:20-22) pointed out that the three main focal points of network security in a client/server environment are the end-user's applications running at the client computer, the transmission of data and the administrative tasks being performed at the server.

Concerning network security it is further necessary to distinguish between security services and security mechanisms.

4.3.2.5.1 Security services

Authentication

It was indicated by Claassen (1994:2-2) that authentication entails the authentication of a communicating peer entity and the source or origin of the data. The peer identity authentication service confirms the identity of the connected entity during the transfer phase to prevent masquerading or unauthorised replay of previous connection messages. The data origin authentication service determines if the source of the data is really the claimed peer entity.

Access control

Claassen (1994:2-2) further stressed that access control provides protection against unauthorised use of resources, for example reading, writing, deletion of an information resource or execution of a program. For access control, use can be made of port protection, for example automatic call back; differentiated access rights; and silent modems. Methods of user authentication include passwords; the exchange of secret protocols; passphrases; tokens or smart cards; and personal characteristics (Pfleeger, 1989:375-410).

Data confidentiality

According to Claassen (1994:2-2 to 2-3) data confidentiality protects data from unauthorised disclosure and entails connection, connectionless, selective field, and traffic flow confidentiality. To protect the data, symmetric encryption (secret key encryption) or asymmetric encryption (public key encryption) can be used (Von Solms & Eloff, 1997:9-10).

Data integrity

Von Solms and Eloff (1997:11) pointed out that data integrity refers to the assurance that only authorised people may change the contents of the data or software, and that data integrity therefore concerns the integrity of all user data over a connection and detects any modification,

insertion, deletion or replay. It mainly comprises connection integrity with or without recovery, selective field connection integrity, connectionless integrity, and selective field connectionless integrity (Claassen, 1994:2-3).

Non-repudiation

According to Von Solms and Eloff (1997:5,12) non-repudiation or non-denial involves the enforcement of accountability for transactions in a computerised environment. Non-repudiation can take place with proof of origin or delivery. In the case of proof of origin, the recipient of data is provided with the proof of the origin of the data and in the case of proof of delivery the sender is provided with proof of delivery of the data (Claassen, 1994:2-3). Favourite non-repudiation controls are digital signatures, public key encryption, certification authorities, certificates, and digital identities (Von Solms & Eloff, 1997:65-87).

4.3.2.5.2 Security mechanisms

Several security mechanisms may be incorporated in the network security to provide some of the services described above. Some of these mechanisms mentioned by Claassen (1994:2-3 to 2-5), Etheridge and Simon (1992:153-155) and Schultheis and Sumner (1998:287) are:

- Encipherment - encryption techniques can be used to provide privacy, authenticity, integrity, and limited access to data. Encryption can be applied between two hosts or between two applications.
- Terminal security.
- Access control mechanisms.
- Positive identification of users.
- Internal procedures.
- Logical access (log-on codes, passwords).
- Document authorisation control.
- Digital signatures.
- Data integrity mechanisms.
- Authentication exchange mechanisms.

- Traffic padding mechanisms.
- Routing control mechanisms.
- Notarisation mechanisms.
- Trusted functionality.
- Security labels.
- Event detection.
- Security audit trail.
- Security recovery.

One of the popular developments in network security is to remove the disk drives from personal computer workstations and to rather use the random access memory as a virtual disk (Wong & Watt, 1990:95-98).

4.3.2.6 Communication security

Communication security, according to Russell and Gangemi (1992:17), is the protection of information while it is being transmitted by telephone, network cabling, microwave, satellite, or any other means. Not only networks, but also the communication links between network hosts intensify security concerns. Pfleeger (1989:416) pointed out that the two most common communication vulnerabilities are noise (loss of integrity) and active and passive wiretapping (loss of secrecy). Drummond (1997:27) indicated that the four basic requirements for secure communications are usually regarded as non-repudiation of delivery/receipt, electronic signature, message confidentiality (encryption), and content integrity. To achieve these requirements on the Internet, the best strategy according to Stross (1996:255-257) is to encrypt the data at application, data or protocol level. Use can be made of the Secure Hypertext Transport Protocol (S-HTTP) that is based on public-key encryption and ensures confidentiality, authenticity, integrity, non-repudiability, and replay security (Kalakota & Whinston, 1997:148; Von Solms, 1996:18).

To reduce noise, organisations can make use of dedicated or direct lines, which do not pass through the normal switching network, so that extra noise and distortion due to switching circuitry is eliminated. Cyclic redundancy checks are also valuable (Pritchard, 1979:10).

The most common communication mediums at the moment are twisted pair cables and coaxial cables. Unfortunately both are subject to passive and active wiretapping. Passive wiretapping entails just listening, while active wiretapping is injecting something into the communication by cutting into the cable. Another security problem is inductance, where the electromagnetic field is detected by electronic circuitry. Other increasing mediums include microwave and satellite links. Microwave is a very insecure medium, because signals travel through the air and are available to anyone who wants to pick the signals up. This security risk is aggravated by the problem with precision of aim. Satellites have an even greater potential of interception, because of the same problem with signal spreading over a wide area of several hundreds of kilometres.

Probably the most secure medium at the moment is optical fibre. Optical fibre offers two important security advantages. Firstly, the entire optical network must be tuned carefully each time a new connection is made, therefore making it almost impossible to tap an optical system without detection. Clipping just one fibre in a bundle will destroy the balance in the network. Secondly, optical fibre carries light energy, which does not induce a magnetic field, thus making inductive tap impossible. The security threat, however, remains, because it is still possible to tap the system at repeaters and splices (Pfleeger, 1989:424-430).

Claassen (1994:2-3) listed several mechanisms that can be used to improve the security of the transfer of data via satellite, microwave or wires:

- Encipherment.
- Digital signatures.
- Access control mechanisms.
- Data integrity mechanisms.
- Authentication exchange mechanisms.
- Traffic padding mechanisms.
- Routing control mechanisms.
- Notarisation mechanisms.

Communication security are very much dependant on standards for the use of encryption[5] and decryption techniques. By transforming data so that it is unintelligible to the outside observer, the value of an interception and the possibility of a modification or a fabrication are minimised (Christoffersson, *et al.*, 1988:1-2; compare Gericke, 1987:9). A secure system is a system where an interceptor cannot recover a plaintext message from its ciphertext, regardless of the amount of effort (Pfleeger, 1989:14, 64-66). Scott (1996:3) aptly demonstrated that modern encryption processes usually allow for more than 2^{128} variations, therefore making it highly unlikely that an attacker could randomly guess the key value used to modify the transformation. To simplify encryption and to overcome the problem of regular changing of cryptographic keys, De Ru (1992:195-206) suggested the use of an expert system.

According to Scott (1996:2-6) cryptographic theory is thus mainly used for:

- Secrecy and the protection of privacy when using public networks.
- Authentication of the source and recipient.
- Authentication of the content of any message.
- The guarantee of delivery.

4.3.3 PROCEDURAL CONTROLS

Procedural controls or logical security ensure accuracy and integrity of computer and network operations according to O'Brien (1998:554-555) and entail the following aspects:

4.3.3.1 Logical access control

To prevent the unauthorised access to data by means of trap doors, Trojan Horses, Salami attacks and other techniques, as discussed in the previous chapter, management should implement cost effective control measures. Logical security therefore entails the protection of software and sensitive data, and aims at limiting access to information to authorised and

---

[5] A discussion of the various encryption techniques, their design and analysis are beyond the scope of this dissertation. For a detailed discussion of monoalphabetic and polyalphabetic substitution ciphers, transpositions (permutations) and fractionated Morse, see Pfleeger (1989:26-62). For a discussion of the three important public encryption algorithms, namely the Merkle-Hellman knapsack, the Rivest-Shamir-Adelman (RSA) and the Data encryption Standard (DES) algorithms, see Pfleeger (1989:90-122), as well as Christoffersson *et al.*, 1988:23-38. See also Christoffersson *et al.* (1988), De Ru (1992:180-193), De Soete (1993:33-49), Maurer and Schmid (1994), Pritchard (1979:93-111), Scott (1996:10-91) and Stinson (1994) for a general discussion of cryptography.

identified users (Long, 1994:451). Sensitive data that should be secured from inadvertent deletion, overwriting or editing by unqualified or unauthorised people, usually are financial reports; sales plans; personnel data; designs; and drawings. A document management system, which is strictly controlled by an administrator, should be set up. This document management system should have the following security features as stipulated by Alton (1995:56):

- **Check-out/check-in:** For a user to retrieve a document from a secure, central location, the document should be checked out. Other users should be able to see when the document was checked out and by whom.
- **Single-user control:** A secured document must only be editable by one user at a time.
- **Clear authorisation and access rights:** The administrator must be able to set up several levels of security.
- **Maintaining of data integrity:** The system must be able to maintain data integrity through any potential disaster, for example loss of electrical power.

Especially microcomputers have access control difficulties mainly because of the low degree of protection in the architecture. Network hosts again need to be continually reassured of the authenticity of the other hosts on the network. Therefore it is important to use extensive access control, stored file encryptors and network penetration detectors. Authentication devices, for example smart cards, challenge-response systems or biometric devices are of great use (Pfleeger, 1989:450-454).

Most access control mechanisms are thus either hardware or software-based, to restrict a user from gaining illegal access to the system. Safe keeping of passwords is essential, and users should be discouraged from storing passwords in one of the workstation's programmable function key memories. If possible, central control of regular password changes should be enforced and users should be advised on the risk of adopting common words or names as passwords. The system should log off the user after two or three failed attempts to enter the correct password. Managers should automatically be notified by the computer system and investigation instituted to account for the incident before allowing the workstation to be reconnected to the network. User passwords should be at least eight characters long and should comprise both letters and digits, uppercase and lowercase to deter simple guessing (Forcht, 1994:231; Husain & Parker, 1996:119). The password table should be encrypted with a one-way

mathematical logarithm, and passwords should not be displayed on the monitor or stored in journal files (Rorbye, 1993:43; Wong & Watt, 1990:104-105).

The compilation of access rules and security profiles to control the actions of users is a considerable task and are usually left to the discretion of the security administrators. To simplify this task of generating and maintaining information security profiles, use can be made of a conceptual model named MAPS (model for automated profile specification) as aptly illustrated by Pottas (1995:1-172).

4.3.3.2 Logical access control types

McCleod (1998:575) indicated that three main types of controls, namely user identification, user authentication, and user authorisation are usually used to exercise logical access control.

4.3.3.2.1 User Identification

Positive identification is usually obtained through the use of user-identification and one or more passwords according to Von Solms and Eloff (1997:7). McLeod (1998:575) added that identification could also include the user's location, such as a telephone number or network entry point. However, as pointed out by Du Toit (1992:47-48), more modern developments include the use of slim cards and biometrical identification.

The most common identification (and sometimes also authentication) mechanism is a password. Although passwords usually are relatively secure, human practise sometimes degrades its quality. Care must however be taken that the login sequence notifies a user of a failure only after accepting both the user name and the password, so that the unauthorised user would not know whether it is the user name or the password that is unacceptable. Although inconvenient, employee logins can also be limited to their specific work hours (excluding vacation and business trips) and terminals (Pfleeger, 1989:226-228).

Because passwords themselves are not very secure, specific care should be taken (Witten, 1990:109-113). There are for instance only 18 278 ($26^1 + 26^2 + 26^3$) passwords of length three characters or less. At an assumed rate of one password per millisecond on an average computer, all passwords can be checked in 18.278 seconds. Four characters would take 475 seconds (7.9 minutes) and five characters would take 12 356 seconds (3.43 hours). A password of 100 characters would however present a formidable task, and even a supercomputer capable of

testing one million keys per second would require centuries to find the correct one (compare Prosise, 1996:119).

Passwords should therefore be as long as possible; nonguessable; refrain from meaningful words or actual names; include alphabetic and numeric characters; include upper and lower case; be changed regularly; and should not be written down or disclosed to any person (De Ru, 1992:52-59, Mandell, 1990:174; compare Pottas, 1990:65-66). Systems should force users to change their passwords regularly. Identification procedures can also intentionally be made slow to discourage penetrators and must not allow more than three failed logins (Pfleeger, 1989:232-235; Rorbye, 1993:43-44). De Ru (1992:73-99) added that to improve the effectiveness of passwords, systems generated passwords; pronounceable but meaningless passwords; password phrases; cognitive passwords; password algorithms; word association; secondary passwords; and the use of an expert system password mechanism can be considered.

The password list should also be carefully protected by strong access controls and encrypted password files (Pfleeger, 1989:230-231; Wong & Watt, 1990:54).

4.3.3.2.2 User authentication[6]

Once identification of the person has been established by something they know, users verify their right to access by providing something they have, for example a smart card or token, or an identification chip. Authentication can also be accomplished by providing something they are, such as a signature, voice or speech pattern (McCleod, 1998:575).

To assist authentication, Denning (1990:198) recommended the use of much more secure physical devices, like handprint or fingerprint detectors, voice recognisers, retina scanners, voice verification or signature dynamics. This type of authentication is very difficult, if not impossible, to forge because it uses physical characteristics of authorised users. Unfortunately the cost of these devices limit their use to mainly high security situations (Pfleeger, 1989:236).

---

[6] A full discussion of authentication techniques falls without the scope of this dissertation. For the various authentication techniques, secret key protocols (e.g. Wide-Mouth Frog, Yahalom, Otway-Rees, Needham and Schroeder, Kerberos, and KriptoKnight), public key based protocols (e.g. CCITT X.509 and Selane), and Hybrid protocols (e.g. station to station protocol and SPX) see Claassen (1994: 5-1 to 5-30). For a general discussion see Beth *et al* (1994), Chen (1994), Jiwa *et al.* (1994), Hardjono and Seberry (1994), Preneel *et al* (1993:87-131) and Van Tilburg (1993:71-86).

4.3.3.2.3 User authorisation

Authorisation, or logical access control, usually follows once the user has been identified and authenticated, and controls the access rights the authenticated user has to different resources by means of an access control list (Von Solms & Eloff, 1997:8-9). Access rights are awarded according to the classification of the information, the job description of the person, and his/her position (Du Toit, 1992:46-47). Important according to Stang (1992:70) is, however, that logical access controls should provide the ability to grant and revoke authorisation over all accesses and access levels.

4.3.3.3 Access violations

Illegal attempts to gain access to the computer system by guessing passwords in order to log on to the system and associated data files should be carefully monitored. One effective way to detect hacking is to display the last log-on time and date on the screen after a user has successfully logged on to the system (Wong & Watt, 1990:54-55).

4.3.3.4 Unusual circumstances

Be careful for unsupervised work, especially if the individual regularly volunteers to work after office hours or over weekends. Unusual circumstances should thus be reviewed regularly (Wong & Watt, 1990:55-56).

4.3.3.5 Data control

All data are not equally sensitive. It is therefore necessary to use data classification to accommodate the different security requirements for each class.

4.3.3.5.1 Data classification

The aim of classification of data is to ensure that all employees become aware of the importance of specific data for the survival of the organisation. Possible classes are public or unclassified, company or internal use only, private, confidential, high security (Du Toit, 1992:49-50).

4.3.3.5.2 Methods for classification of information

According to Du Toit (1992:51) information is usually classified according to specific factors by using a matrix. The factors include form (for example final form), subject (for example marketing), type of information (for example strategic), timeliness (for example archive), cost of exposure (for example high) and risk of exposure (for example high).

4.3.3.5.3 Reclassification

The sensitivity of certain information may change over time, for example financial statements. It is therefore necessary to determine a date of reclassification for all classified information (Du Toit, 1992:51-52).

4.3.3.5.4 Ownership of information

It is important to appoint an owner for every piece of information. The owner has the right to award access rights to his information (Du Toit, 1992:52).

4.3.4 OPERATIONAL CONTROL

These controls mainly apply to the maintenance work of the information systems department and ensure that programmed procedures are consistently and correctly applied to the processing and storage of data. Operational controls include controls over the set-up of computer processing jobs, operations software and computer operations, as well measures taken by users to prevent and recover from errors, for example backup and recovery procedures (Stang, 1992:73).

Laudon and Laudon (1998:637) stated that controls over operations software should include manual procedures to prevent and detect errors, recovery procedures, procedures for the disposition of magnetic tapes, and the maintaining of an activity log to record hardware malfunction, abnormal endings and operator actions.

4.3.4.1 Control of amendments

Appropriate authorisation procedures should be established and enforced to control any changes made by technical staff on live systems and data, for example system passwords; closed user group membership; reconstitution of routing tables for data transmission; user passwords; access

privileges or profiles to various databases; changes to the program library on system utilities or application programs; as well as modification of live business data or transactions on application databases. Similar controls should be applied to the modification of physical access control data (Wong & Watt, 1990:46-47).

4.3.5 INFORMATION SYSTEMS CONTROL

Information systems controls are necessary protective methods and devices to prevent and limit security threats; to reduce vulnerability; and to ensure the accuracy, validity, integrity and security of information system processing activities and resources (O'Brien, 1998:546; Pfleeger, 1989:3). The processing of data can be sub-divided in input and capturing (terminals and scanners), communication (networks and modems), processing and output (terminals, printers, optical and magnetic media).

Important systems controls to eliminate and prevent fraud and errors according to Carden, (1976:80) and Laudon and Laudon (1998:640) are:

- The completeness and correctness of the input and processing of data must be ensured. Supporting documentation must be valid en authorised. A clear transaction audit trail must be available where possible.
- Accuracy of input, which entails the accurate capture and recording of data.
- Data should be authorised or checked with regard to the appropriateness of the transaction to ensure validity.
- Input controls to ensure the correctness, completeness, security and auditability of data. Input control is absolutely necessary, because it is the place where the most intentional and accidental errors are made. Errors and fraud is not only applicable to data, but also to the updating and modification of master files. A common saying amongst the computer fraternity, namely "garbage in, garbage out" is here very much applicable (O'Brien, 1998:547). If controls are not instituted on input data, there are possibilities that bad decisions will be made on bad information.
- Processing control ensures the correctness of the processing and entails the efficiency of the system programs, strict control over processing procedures and the reliability of the apparatus. The efficiency of the system programs are greatly dependent on the testing

procedures during system development, as well as the way in which system programs are protected against incidental or intentional corruption.

- Control over information storing media, for example hard disk drives in the data processing area; databases; data administration; optical and magnetical media; and physical handling.
- Output controls control the obtainment, access, restriction and correctness of documents, reports and display. The output from production reports destined for management should also be carefully controlled. Audit trails are absolutely essential (Rilley, 1981:36).
- Maintenance controls to ensure that data continues to remain correct and current.
- Access to application systems and databases must be controlled by means of a complex system of access keys.
- The successful management and control of personal information, information on people, corporate information and sensitive information depends greatly on the ownership of data. Methods whereby data ownership are allocated, controlled and classified are thus of the utmost importance.
- Systems integrity and control must be ensured by making a specific person responsible for direct reporting to the chief executive officer to guarantee that systems are developed according to pre-determined standards, systems are operated according to specified methods, access to information are controlled, and that the overseeing and changing of access passwords are done on a continuous basis.

Information systems control measures can usually be classified in a few main groups:

4.3.5.1 Origin of data controls

Source document controls involves procedures for the control of documentation- and user procedures. Source document design includes pre-printed documentation with numbers, transaction identification, cross references and transaction order capturing control. The storage of source documents must be limited and clear responsibilities must be assigned with reference to the storage and transporting of resource documents.

Authorisation controls include the separation of tasks with regard to data preparation and the approval of source documents.

The aim of data processing input preparation is control over the preparation for data capturing by means of clear transaction identification, user supervision over input, batch and transaction transmittal control.

The retention of source documents must be according to statutory requirements and must be available in case of disaster recovery. Source document error handling must be controlled and handled according to determined procedures.

4.3.5.2 Input and capturing controls

Input controls check data for accuracy, correctness and completeness when it is entered into the system. This is often done by means of passwords, security codes, encryption, formatted data entry screens, audible error signals, templates for key-driven input devices, pre-recorded forms, pre-numbered forms, and control totals and logs (O'Brien, 1998:547-548).

To check against any omission or loss of records during data entry or data capture, computer users should be encouraged to use record counts and financial totals, as well as to print out a transaction listing, and use it to check against original source documents by sampling techniques. Other control checking could include the provision of general utilities to perform range and limit checks, completeness tests, check digit verification, valid account code tests, and the use of control totals and hash totals (Wong & Watt, 1990:105-107).

According to O'Brien (1996:582), the following input controls should be implemented:

- When batch processing are used, procedures must be established for the control and handling of transaction documents.
- Terminal data capturing controls involves the logon procedures, user application access, and access to data.
- Transaction data validity controls include transaction verification techniques, for example validity testing routines and validity of passwords.
- Input balancing controls the capturing of transactions according to control numbers and error detection procedures.
- Transaction capturing error handling includes the error correction procedure and recapturing van corrected data.
- Other measures that can be used are security codes, error signals and control totals.

4.3.5.3 Input authorisation controls

It is important the input should be properly authorised, recorded, and monitored. Source documents should be serially numbered, grouped into batches, and logged (Laudon & Laudon, 1998:641).

4.3.5.4 Data conversion controls

Input should be properly converted into errorless computer transactions as it is transcribed from one form to another. Transaction errors can be minimised and even eliminated by keying input transactions directly into the computer terminals or by using scanners (Laudon & Laudon, 1998:641).

4.3.5.5 Edit checks

Various routines should be established to edit input data for errors before it is processed. The editing procedure which are most frequently used are reasonable checks, format checks, existence checks, dependency checks, and check digits (Laudon & Laudon, 1998:642).

4.3.5.6 Processing controls

Processing controls ensures that data are complete and accurate during updating, calculations and logical operations and mainly involves hardware controls, software controls, run control totals, computer matching, and programmed edit checks.

Computer integrity processing controls firstly include transaction identification by means of transaction codes and the monitoring of computer generated transactions. Integrity processing and logical control secondly entails anticipating controls, mathematical and arithmetical correctness, exception reporting, file control totals, and file completion controls.

Computer processing of error handling controls involves error reporting, error correction and recapturing of corrected data.

4.3.5.6.1 Hardware controls

Hardware controls are according to O'Brien (1998:548-549) special checks built into the hardware to verify the accuracy of computer processing, for example malfunction detection

circuitry, redundant components (for example multiple read-write heads), and special-purpose microprocessors and associated circuitry to support remote diagnostics and maintenance.

4.3.5.6.2 Software controls

O'Brien (1998:549-550) describes software controls as controls, which ensure that the right data are processed by checking internal file labels, establishing checkpoints during the processing of a program, and system security monitors.

4.3.5.6.3 Run control totals

Run control totals reconcile the input control totals with the totals of items that updated the files and thus controls the updating process. The computer compares the totals, for example total amount of transactions processed or totals for critical quantities, for discrepancies (Laudon & Laudon, 1998:642).

4.3.5.6.4 Computer matching

Computer matching, as pointed out by Laudon and Laudon (1998:642), is used to check for the consistency of data and matches input data with information on master or suspense files and reports unmatched items.

4.3.5.7 Output controls

Output controls are developed to ensure that the results of computer processing are accurate, correct and complete, and distributed only to authorised users. It typically includes control totals, control listings, prenumbered output forms, and security codes (O'Brien, 1998:550-551). Documents in there final form should also be classified and clearly marked accordingly.

According to Bezuidenhout (1988:52-57) and Laudon and Laudon (1998:643) the most frequently used controls are:

- The balancing of output totals with input and processing totals.
- Regular reviews of computer processing logs to ascertain that all the correct computer jobs were executed properly for processing.

- Audits of output reports to ensure that totals, formats, and critical details are correct and reconcilable with the input.
- Formal documentation and procedures regarding authorised recipients of output reports, cheques, or other critical documents.
- Data processing, -balancing and -reconciliation controls by means of the reconciliation of transactions and reports and the monitoring of process flow and task control.
- Output distribution includes the handling of outputs, distribution of reports, control over the number of copies and the channelling of the information to decentralised workstations.
- Record retention controls include methods for the retention and destruction of records by the user.
- Output error handling controls, including error reporting, error correction and recapturing of the faulty transactions.

4.3.5.8 Communication controls

Security and control of communications is of specific importance for organisations that are involved in electronic commerce and electronic data interchange (EDI). It is essential that commerce-related data of buyers and sellers are kept private when transmitted electronically. Stang (1992:74) pointed out that the aim is thus to protect the transmission of data against passive (non-modifying) or active (modifying) intrusion. Control measures that are used widely during electronic data interchange, are physical access controls; logical access controls; environmental controls; development and maintenance controls; application controls; business continuity controls; operations controls; personnel controls; encryption; authentication and message integrity checks (Laudon & Laudon, 1998:644).

The following communication controls are quite widely used to enhance information security:

- Message capturing controls include the protection of communication equipment, message transmittal identification and communication system user control.
- Message transmittal control involves the control of communication lines, automatic call back methods, validity testing, echo control, message interrupt functioning, encryption techniques, multipurpose modem control, backup modems and lines.

- Message receive and acknowledge controls include validity testing, line usage record, phone in modems, error capturing en rectifying procedures.

4.3.5.9 Storage and extraction controls

O'Brien (1998:551) stresses the importance that files, computer programs and databases should be protected against unauthorised use and processing accidents by using security codes, passwords, backup, and file retention procedures. Storage controls that can be considered are:

- File handling controls, including file and program library operations procedures.
- Access control by means of file and program classification, data base control tables, passwords, program interface control tables and file labels.
- File maintenance control over master file modifications, as well as critical file control.
- Back up procedures with regard to separate computer copies of master files, contingency and disaster recovery planning.
- File error handling controls including error reporting, rectification and recapturing of files.

4.3.5.9.1 Database security and control[7]

Although some fine controls have been developed in the field of database integrity and secrecy over the last ten years, there are still more security concerns than there are available controls. Two major security problems are the inference problem and the multilevel problem. The inference problem entails the inferment or derivation of sensitive data from non-sensitive data, while the multilevel problem refers to differentiated security (Pfleeger, 1989:299, 319-331).

Secure relational and object-oriented databases are essential because information is a valuable asset and needs protection against unauthorised access. According to Olivier (1991:9-10, 26-29) three important aspects need to be addressed in a database environment:

- **Secrecy:** Measures taken to ensure that information is not disclosed to unauthorised parties. Implementation strategies for multilevel secure databases include trusted filter or trusted

[7] For more detailed information regarding database security, see the papers in Biskup *et al.* (1994) and Thuraisingham and Landwehr (1993).

front-end approach, the balanced assurance approach, and the monolithic or uniform assurance approach.

- **Integrity:** The prevention of unauthorised changes and additions to the databases. Integrity measures include, amongst others:
  - Disallowment of unauthorised users to modify or add information.
  - Controls to limit an authorised user's ability to modify or insert information where the new values are inconsistent with other information in the system or the new values are incorrect.
  - Inhibition of the flow of unreliable information to locations where it can be accepted as reliable.
  - Ensurement that physical phenomena (for example power failures and natural disasters) do not cause inconsistencies or other integrity problems in the system.
  - Ensurement that all information is accurate and insulated against accidental and deliberate change (compare also Alexander, 1995:30).
- **Availability**: The assurance that data will be available to authorised users when needed. Measures to ensure availability of a service include aspects such as:
  - Ensuring that the measures for secrecy and integrity do not hamper authorised users.
  - Ensuring that other users (authorised and unauthorised) do not monopolise the system to such an extent that an authorised user is denied service.
  - Establishing facilities and procedures to ensure that work can continue despite physical phenomena.

Based on the three above mentioned and well-known aspects of information security, the following requirements should usually be met to secure the databases:

- **Physical database integrity:** The data should be immune to physical problems, for example power failures.
- **Logical database integrity:** The structure of the database should be intact, in others words when the value of one field is changed it should not influence the other fields.
- **Element integrity:** The data in every element should be accurate.

- **Access control:** A user should have access only to data for which he has authorisation. Different users should be limited to different access rights.
- **User authorisation:** Every user should be identified positively before access is granted.
- **Availability:** Conflicts about access to certain data should be solved to make the data available to users.

It is however important that the implementation of security features should not negatively influence the use of the database. Security measures should therefore be flexible, should not limit the accessibility, and should be cost effective (Du Toit, 1992: 53-54).

4.3.6 IMPLEMENTATION OR SYSTEMS DEVELOPMENT CONTROLS

According to Laudon and Laudon (1998:635) implementation controls audit the systems development process at various points of development to ensure that the process is properly controlled and managed.

4.3.6.1 In house development

When systems are developed in house by an organisation, special attention to information security should be paid. Aspects such as identification, authorisation, access control, integrity, recovery of data and auditing should be build into the system. All security procedures should be clearly documented (Du Toit, 1992:56-58).

4.3.6.2 Distributed development

Many organisations have moved from centralised application development to distributed development. Although this practise offer many benefits, for example diminished backlogs, user satisfaction and the spreading of cost, there are some drawbacks. These drawbacks include the use of non-standard software, software that is difficult to support, software that contain bugs, and software that has trap doors, logic bombs or time bombs.

Laudon and Laudon (1998:636) and Stang (1992:73-74) therefore emphasised the necessity to implement the following controls:

- Develop documentation requirements. Appropriate technical and user documentation is a frequently neglected aspect, which should be carefully controlled
- Develop procedures for modifying code.
- Maintain all source code.
- Thoroughly test new applications.
- Ensure that all code and programs are backed up and clearly labelled.

4.3.6.3 Acquired software

Rorbye (1993:26) emphatically states that only authorised software from reputable sources that meets organisational standards should be acquired. To prevent virus infection, software should be purchased from reputable sources in sealed packages and should always be checked before instalment. A backup copy of the software should be stored off-site. To prevent booting up from infected diskettes, a boot read only memory (ROM) can be installed in every terminal. Games and private software, as well as shareware and public domain software, downloaded from bulletin boards, should be prohibited. Use should be made of the various protection products focusing on virus detection, infection prevention, and infection identification (Wong & Watt, 1990:117-125).

4.3.6.4 Program development controls

Programmers have many ways that they can subvert a system to their own advantage. It is therefore important to apply controls during program development (design, writing and testing) to ensure the quality and integrity of the code to be produced. Oné of the most important controls is to avoid programming by individuals and to rather make use of team software engineering, peer design reviews, peer code reviews, configuration management, and program verification to eliminate the possibility of trapdoors, Trojan horses, salami attacks, viruses, worms, and other program flaws. Management should use exigent code reviews throughout code development as a way of ensuring security of the programs produced. However, no level of source-level verification or scrutiny will protect an organisation from using untrusted code. It is therefore of the utmost importance that the people who wrote the software can be trusted (Thompson, 1990:97-104).

Once a program has been developed, it is important to compare an image copy bit by bit against the audit copy for illegal code. Any discrepancy should be checked for illegal insertion of unauthorised code changes. An easier way is to calculate a hash total or cryptographic checksum. The built in control function would initiate a repeat calculation from time to time to check the current value of the hash total or cryptographic checksum against the previous value obtained. If the two values differ, the possibility of illegal code changes exists (Wong & Watt, 1990:58).

According to Pfleeger (1989:14, 180-187) application system development and maintenance control further include procedures for change control and management, logical access control to application systems, data and programs, standards for system design with specific reference to system security, project management methodology, programmed controls, documentation, testing of the system and maintenance.

Rilley (1981:37) stated that clear and well-structured documentation is compulsory during program development to make it possible for another person to take over in the case of a departed employee.

4.3.7 CONTROLS OF THE LAST RESORT

4.3.7.1 Natural disasters and disaster recovery

Du Toit (1992:40-41) pointed out quite correctly that natural disasters like fire, lightning, wind, floods and earthquakes cannot always be prevented. Their damage can however be limited by means of carefully planned fire systems, lightning conductors, water channels and construction of the building to specific standards, as well as a complete and tested disaster recovery plan.

4.3.7.1.1 Types of disasters

Floods

Floods can come from two sources, namely rain, tides and waves (natural) and broken water pipes (artificial). Therefore it is important to plan for controls against floods from rising water and falling water (such as leaking roofs). Care must be taken to identify the most important media beforehand for urgent removal. Volumes can be marked with coloured labels. Locating the computer centre or server room above ground level or placing the building on a slight

elevation can also prevent the threat of rising water. To prevent damage from descending water (burst water pipe, roof leakage, or sprinkler system) every computer system should have an available plastic cover.

Fire

Fire is more serious than water, because of the time limit for reaction. It is therefore imperative that computer centres should have a plan to shut down the network in an orderly fashion. The plan should include individual responsibilities for all personnel and computer users. Carbon dioxide extinguishers or automatic gas systems should be used in stead of water. The careful placement of the computer centre or server room, absence of windows, fire resistant doors, and non-flammable full height walls can prevent a fire from spreading from adjacent areas to the computer centre or server room.

Electrical power

With a direct power loss, all computation ceases instantaneously. To minimise disruption through power failure, use can be made of battery backup via an uninterruptible power supply (UPS) or standby generator, depending on criticality and usage of individual computer systems. Another problem with power is its cleanness from drops and spikes (surges) due to heavy machinery or lightning. This problem can be overcome by installing surge suppressors on every computer, printer or other connected component.

Heat

Computer systems are very sensitive to heat, which can lead to unpredictable performance of components and computations and seriously shortens the life span of electronic components. Heat should therefore be monitored and controlled very carefully (Pfleeger, 1989:438-442).

4.3.7.1.2 Disaster recovery planning

Disaster recovery planning includes the duplication of critical network components, data, media, as well as the testing of recovery procedures. Attention should be paid to the following aspects in a disaster recovery plan:

Backup

Bowen (1994:36) argued that to prevent accidental or malignant erasure or modification of mission-critical data, there should be standard backup procedures as part of the total strategy to protect information. Because it is essential to the survival of any organisation, complete backups in which everything on the system is copied, including system files, user files, scratch files, and directories, should be made on a regular basis (Du Toit, 1992:42). Erwin and Blewett (1996:529-536) recommend that selective backups, in which only files that have been changed since the last backup are saved, should at least be done on a daily basis. It is also important to regularly test the backup routines to see whether they still perform their functions.

Off-site backup

The back up procedures for data and the safe storage of the backup copies are important for disaster recovery. A backup copy is of no use if it is destroyed in the same crisis. Because it reduces risk, it is a good idea to keep the newest backup copies at an off-site facility or remote secure location to limit accidental corruption of data, and to enable recovery from a disaster (Du Toit, 1992:42-43). Backup copies of software, application programs and system documentation should also be stored off-site.

Even a vault or secure storage place in another part of the building is better than keeping the backups at the same place than the computer system. Backups can also be stored with a security company that specialises in storing information from several organisations in encrypted form. This is known as televaulting (Haag *et al.*, 1998:394).

Hardware

There should be control and advice on the acquisition or purchase of computer equipment, to ensure there is adequate spare capacity for internal backup and future expansion. Full compatibility should be maintained of the various equipment and software in use to facilitate changeover, in case some work stations may be out of service during routine maintenance and repair, or in the event of fire or water damage to an office.

Alternative processing facilities

Various types of alternative processing facilities that can be used in the case of a disaster exist:

Cold site

Du Toit (1992:44) describes a cold site or shell as an empty computer facility with power, cooling and communications available, where a computer system can be installed to begin instantaneous operation. Usually a computer centre can have identical equipment installed and resume operation from a cold site within a week of a disaster.

Warm site

According to Du Toit (1992:44) a warm site is a recovery centre fully equipped with compatible data processing and communications equipment. However, occupancy is limited and a concurrent disaster could occur with another user.

Hot site

If applications are absolutely critical to the business of an organisation or if very specialised equipment is being used, a hot site may be more appropriate. A hot site is a solely owned computer facility with an installed and ready-to-run compatible and fully configured computer system, all necessary programs, peripherals, telecommunication lines, power supply, and sometimes even skilled personnel ready to operate on a short notice (Du Toit, 1992:45; Post & Anderson, 1997:75). Alternative backup apparatus with the necessary capacity and compatibility are therefore critical for important programs (Pfleeger, 1989:442-444). Although expensive, an off-site electronic vault to which mirror copies of vital data are send over high speed communication links in real time or near real time, is the ideal.

The ultimate is of course a complete and synchronised decentralised centre with resource programs, processing programs, data files, contingency plans, network programs, documentation, and communication facilities.

Up site

A mobile computer room, either containerised or mounted within a trailer, equipped with computer hardware, which can be delivered to the affected site.

Vendor agreement

This alternative relies on an agreement with a hardware vendor to provide a compatible backup at the time of the disaster, but compatibility and security may be problems.

Reciprocal arrangements

An inter-company arrangement can be made where each other's work is processed during a disaster, but may not be available when needed.

Personnel

Staff responsibilities should be agreed on and documented. The following personnel teams, lead by the recovery co-ordinator, can be selected to ensure that all actions are co-ordinated in accordance with the disaster recovery plan:

Table 4.1: Disaster recovery personnel teams

Tasks	Suggested Members
Management team	
❖ Implementation of the recovery plan ❖ Co-ordination and liaison with all users and specialist teams ❖ Monitor and report progress	❖ Financial director ❖ Personnel director ❖ Information technology manager
Facilities Team	
❖ Preparation of any existing or alternative data-processing site facilities	❖ Operations supervisor ❖ Personnel manager ❖ Security manager ❖ Buildings manager
Hardware Team	
❖ Acquisition of new or replacement hardware ❖ Refurbishment of existing hardware	❖ Hardware engineer or technical support person
Telecommunications Team	
❖ Establish or re-establish telecommunications network	❖ Data communications manager or technical support person
System Software Team	
❖ Provide a working version of the current operating system	❖ Analyst programmers ❖ Systems analyst or ❖ Technical support person
Operations Team	
❖ Provide a working installation and operate alternative site equipment	❖ Operations manager ❖ Network administrator
Data Entry Team	
❖ Establish data entry services	❖ Data entry supervisor
Salvage and Restoration Team	
❖ Evaluate damage ❖ Minimise further losses ❖ Recover all salvage	❖ Facilities manager

Table 4.1 (continued)

Tasks	Suggested Members
Transportation Team	
❖ Organise all transportation needs for personnel	❖ Transport manager
Administration Team	
❖ Service all personnel functions and supply consumables	❖ Administration manager

In addition to the size of the organisation, factors such as management style, skill levels available, and business activity, will all contribute to the decision as to the number and composition of the above mentioned teams (Wong & Watt, 1990:261-265).

The disaster recovery plan

An extensive disaster recovery plan will have to be completed probably at considerable expense and effort. Because of the continually changing business and computing environment, the disaster recovery plan will have to be updated regularly to maintain the viability of the plan.

In order to succeed, senior management must take responsibility for one of their most valuable assets, and therefore agree to properly fund the contingency planning exercise. To ensure effectiveness the plan should at least be tested biannually to ensure its practicality and usefulness. The results should be presented to senior management in a written report (Wong & Watt, 1990:270-277).

4.3.7.1.3 Contingency Plan

A tried and tested contingency plan is necessary to allow an organisation to resume operations within the minimum time period after a disruption or disaster. The contingency plan, which includes disaster recovery, is part of the information security plan and involves three steps according to Haag *et al.* (1998:330-331):

- Identification of functions or processes that are critical to the success of the company, as well as the information technology systems that support those functions and processes.
- Estimation of the cost of unavailability of critical information and formulation of the information unavailability cost curve.

- Development of a disaster recovery cost curve to determine the balance between the cost of unavailability and the cost of recovery.

4.3.7.1.4 Insurance

For the sake of insurance claims in case of a disaster, it is helpful if inventory forms are kept, stating the computer models, where equipment is located, who is responsible for the equipment, any modifications made to the computer or its software, who uses the system, and who has technical knowledge. These inventory forms should be copied and stored off-site for ready access in an emergency (Wong & Watt, 1990:108-109).

4.3.8 SYNERGY

According to Claassen (1994:1-9) the aspects of security can be expressed mathematically to illustrate the relationships of the various components of information security. The formula of Claassen (1994:1-9) can be adapted to include all seven control measures discussed above. The new mathematical formula then expresses information security as a multiplative function of the seven control measures of information security:

$S = f(A \times P1 \times P2 \times O \times IS \times I \times LR)$

where

S = total information security
A = administrative controls
P1 = physical controls
P2 = procedural controls
O = operational controls
IS = information systems controls
I = implementation or systems development controls
LR = controls of the last resort

Each element of the mathematical equation may be thought of as varying between 0 and 1 and represents a weighted value of 0 in the case of no security controls and 1 in the case of maximum security controls.

It is quite obvious that if any of the aspects of information security in the equation is awarded a 0 because of a lack of security controls, total security will be 0. Synergy regarding all aspects, facets and control measures is thus of the utmost importance for the success of information security. To be really effective, information technology staff with security responsibilities in the company need to work closely with all key players, including departmental managers, physical security personnel, as well as the users using the equipment. Between them they have to ensure that the various security products and control procedures in use are well understood and consistently applied (Wong & Watt, 1990:110).

4.4 SUMMARY

Although it is not possible to build a completely secure information system and to eliminate all threats and problems, it is possible to minimise the impact and business disruption by following a total systems approach by paying attention to risk analysis, risk monitoring and risk control.

The three major methods of control are prevention, detection and correction. Because absolute security is impossible, prevention is of the utmost importance and entails virus-prevention and the use of firewalls and assured pipelines. Just as important is the early detection of potential abuse. Two main techniques are used, namely anomaly and misuse detection. Correction involves recovery controls, rectification of errors, reporting of errors and prosecution.

Various information security controls can also be implemented, for example administrative, physical, procedural, operational, information systems, systems development and last resort control measures. Synergy between the various components of information security is a necessity.

Information security controls ensure that valuable business data files are not subject to unauthorised access, change, or destruction. On-line and real-time systems are particularly vulnerable and should be protected by the physical restriction of terminals, the use of passwords, limited access, and a multilayered information security system. It is important that top management take responsibility for information security and control, but also involves all personnel.

However, to be successful and effective it is important that these information security control measures are managed properly. This is the topic of the next chapter.

CHAPTER 5

THE MANAGEMENT OF INFORMATION SECURITY

5.1 INTRODUCTION

No combination of products or procedures can completely safeguard the information assets of an organisation. Although many of the vulnerabilities can be eliminated and the effects of threats minimised, the management of information security plays an important role.

Information security management is concerned with the procedures and operations, which are needed to support and control the security aspects of information, namely integrity, secrecy, and availability. It mainly entails the provision of security services and mechanisms as discussed in the previous chapter, as well as the reporting on security services, mechanisms and security-related events. Security management thus includes for example the distribution of information on access rights, the setting of administratively-imposed security selection parameters, the reporting of both normal and abnormal security events or audit trails, and service activation and de-activation.

In the previous chapters the vulnerability of information security and the implementation of certain measures to limit this vulnerability were discussed. In this chapter the emphasis will be placed on the management of information security. The chapter will thus concentrate on various management aspects, for example responsibility for information security; the corporate information technology security policy, objectives, standards and guidelines; the determining of security requirements; a control strategy; the formulation of a information security control framework; an information security management model; and the optimum level of security with regard to cost vulnerability and accessibility.

5.2 A STRATEGIC PERPSPECTIVE

Du Toit (1992:23-24) pointed out that before information security can be implemented effectively, it is necessary for top management to acknowledge the strategic importance of

information systems to retain a competitive advantage. Before top management realises the strategic importance of their information resource, they will not allocate adequate funding, nor pay information security the necessary attention. It is obvious that the real value of the information will determine the extent of the security on the cost/benefit scale.

5.3 THE RESPONSIBILITY FOR INFORMATION SECURITY

Pritchard (1979:16) correctly pointed out that because information is of corporate importance, it is clear that the ultimate responsibility for information security within an organisation rests with senior management and not only the information technology department. Sharratt (1974:11-12) again argues that the responsibility for information security rests with the information technology department. Research has however shown that to effectively implement an information security plan, the continuous involvement and support of senior management is imperative (Du Toit, 1992:25-30).

5.3.1 THE INFORMATION SECURITY MANAGER

There is no doubt that in a relatively large organisation with heavy use of information technology facilities, a specific person should be tasked with the management of the information security function (Von Solms, 1993:6). According to Du Toit (1992:146-147) and Wong and Watt (1990:128-134) the information security manager is responsible for the following aspects of security:

- Planning of the corporate information technology security policy.
- Security of the data centre, server room, communication network and terminals.
- Liaison with all computer users.
- Motivation of personnel with regard to information security.
- Production, implementation and enforcement of security standards, controls and procedures.
- Regular risk analysis, monitoring and security reviews.
- Regular log reviews.
- Implementation and administration of access control equipment and software.
- Control of encryption and authentication devices.

- Control of the security of all files in the media library.
- Contingency planning and computer insurance.
- Advice on all levels in the organisation on information security matters.
- Studying of the most recent literature on information security.
- Reporting to top management.

Six high-level main processes for information security management by the security information manager can be identified:

5.3.1.1 Research and knowledge

The information security manager should be actively involved in research efforts to continually identify new threats, and develop new techniques as technology changes. He should keep abreast of changes in hardware, software, management, potential threats, social and legal issues (Von Solms, 1993:28-29).

5.3.1.2 Policy and information security organisation

The most effective way for senior management to show their total commitment to information security is to issue a corporate information security policy document. The information security manager is responsible for the creation and maintaining of a security library storing all information security policies, standards, procedures, newsletters, professional and product literature (Von Solms, 1993:30-32).

5.3.1.3 Education and liaison

The information security manager should provide regular security awareness programs, through the use of posters, bulletins, videotapes, multimedia, employee sign-on agreements, and e-mail. All employees should be aware of the information security problem and the possible consequences of security breaches.

Close co-operation and continuous liaison of the information security manager with security bodies, like physical security, personnel security and law enforcement, as well as service

suppliers, the telephone company, insurance underwriters and legal counsellors should be established (Von Solms, 1993:32-34).

5.3.1.4 Contingency planning

Contingency planning is an attempt to ensure a high level of integrity, security and availability at all times. Therefore it is imperative to install appropriate countermeasures to limit security risks and the results of disasters. The information security manager should continually assess these risks. He should also institute an effective and tested disaster recovery plan (Von Solms, 1993:34-37). Most of these aspects were dealt with in chapter 4.

5.3.1.5 Measuring and reporting

The information security manager should evaluate the information security controls on a regular basis to ensure that an acceptable level of security is maintained. The results of this evaluation should be reported to the top management on a continual basis (Von Solms, 1993:37-39).

5.3.1.6 Operational management

Von Solms (1993:39) also pointed out that the information security manager and his department should review and monitor all security risks, vulnerabilities, countermeasures and logical access control on a constant basis.

Without doubt, the advent of the personal computer has complicated the role of a central security manager or administrator from the information technology department who centrally controls all physical and logical access to computer facilities, systems and data. If an personal computer workstation is only allowed read-access to the host system data by the central access control facility, the latter will be unable to prevent the former from storing in local memory, the data which is downloaded from the host and displayed on the personal computer's screen. Once this is done, there will be very little the host system can do to prevent the local workstation from manipulating the data. The data can thus be copied to the hard disk or diskette, sent to a printer to produce a hard copy or sent to another personal or host computer.

5.4 CORPORATE INFORMATION TECHNOLOGY SECURITY POLICY, OBJECTIVES, STANDARDS AND GUIDELINES[1]

To facilitate the enforcement of good information technology security in an organisation, it is fundamental that management and all employees know and understand the corporate stance on information security. This is usually spelled out in the following documents:

5.4.1 CORPORATE INFORMATION SECURITY POLICY

A security policy is a formal management recognition of the information security requirements of the organisation to ensure integrity, confidentiality, availability, resilience, and accountability of the system and its data. The document contains a high-level policy statement from senior management regarding the information security, and consists of several sections, namely goal, policy statements, definitions, scope, structure, responsibilities, and tangent issues.

According to Du Toit (1992:78-79, 95) and Wong and Watt (1990:135-137) the corporate information security policy should:

- State clearly how different types of information should be treated, for instance secret, confidential, personal, or public information.
- Stipulate the security responsibility of management and employees regarding the access, processing, dissemination, disposal, and general handling of each security category of information.
- State the respective security roles of management, the information owner, the information technology department and the computer user.
- Define the responsibilities for the formulation of control guidelines, monitoring procedures, feedback and review mechanisms, the administration of the security function, as well as guidelines for surveillance, investigation and reporting activities.
- Refer to the application of risk analysis and risk control practises and techniques.

---

[1] Security policies, procedures and guidelines were briefly discussed in 4.3.1.1 as part of administrative controls.

- Give examples of control measures to protect the availability, secrecy, integrity and access to the different categories of information. This could include encryption techniques, password control, and authentication checks.
- Address other aspects such as personnel policy, data ownership and data users responsibilities, control of the flow of information, security of stored data, monitoring of information security and audit trails, and contingency planning.

Du Toit (1992:97-99) also indicated that the general principles for the protection of a business can be helpful with the compilation of a policy document, namely in-depth business protection (more than one protection measure), early warning of potential threats, sufficient management information for decision making, cost effectiveness, and risk prioritisation.

Because of the constant change in technology, it is important that the policy statement should be reviewed and adapted regularly.

5.4.2 SECURITY OBJECTIVES

Depending on the size of the organisation, the objectives of information security can comprise one or more documents to put the information security policy in perspective. The purpose of the objective document is to serve as an expansion of the policy document. It usually expands on the policy statements, explains the reasons behind it, as well as states the objectives of the statements. It also functions as a link between the policy statement and the procedures and standards document (Du Toit, 1992:80-82,117-128).

5.4.3 SECURITY PROCEDURES, STANDARDS AND GUIDELINES FOR IMPLEMENTATION

To allow the information security policy to be properly implemented, detailed guidelines and procedures should be issued, as well as standards to measure the success of the implementation. This document specifies the obligations of every employee, procedures and standards to standardise methods of work, and provides guidance for the implementation of information security (Du Toit, 1992:83-84, 129-140). Although several guidelines can flow from one policy statement, the guidelines should not be too voluminous and should be properly explained during

security training sessions or workshops. The guidelines should be clear enough to the employee in order to contribute to meeting the information security objectives.

5.4.4 A STANDARD INFORMATION SECURITY DOCUMENT

Eventually a standard information security document should be published and distributed to all employees. This document should address the following topics and aspects[2]:

Table 5.1: Important topics and aspects of the standard information security document

Topic	Aspects
Security policy	◆ General structure of the document ◆ Application control ◆ Host system security ◆ Operational security ◆ System development ◆ Network and communications ◆ End user computing ◆ Office security and office system security ◆ Physical security ◆ Contingency planning ◆ Computer insurance
Risk analysis and control	◆ Frequency
Hardware concerns	◆ Access – unattended micros, timelocks if the keyboard is inactive, password changes ◆ Theft ◆ Environmental damage – electrical power; smoking, eating and drinking; static electricity ◆ Magnetic media – floppy disks, hard disks ◆ Media declassification or destruction ◆ Electromagnetic emanations ◆ Hardware modifications ◆ Trusted, authorised technicians
Data concerns	◆ Classification ◆ Labelling – external classification labels on micros, floppy disk labels, files, encryption ◆ Securing data media – lock floppy disks, removable hard disks, backups, clearing memory. ◆ Data transmission
Human concerns	◆ Personnel ◆ Senior management support ◆ Education and training of employees ◆ Participation of all employees ◆ Rewarding of staff efforts

[2] Most of these aspects of information security were fully covered in chapter 3 and 4 and are therefore not discussed again.

Table 5.1 (continued)

Topic	Aspects
Logical security	◆ Software concerns and security ♦ Software vulnerabilities ♦ Operating system weaknesses ♦ System access control (password management, log-in procedures) ♦ Privilege control (information driven access control, user separation, special privileges) ♦ Logging ♦ User identification and authentication – passwords, power up ♦ Software attacks – trapdoors, Trojan horses, worms, viruses ♦ Communication attacks – encryption ◆ Software development and change control ♦ Computer viruses and worms ♦ Development process ♦ Change control process ♦ Computer operations ◆ Information and data security ♦ Intellectual property rights ♦ Data privacy ♦ Data criticality ♦ Data integrity ◆ Communications security ♦ Establishment of access paths and systems ♦ Encryption ♦ Dial-up computer communications ♦ Download of data ♦ Electronic mail systems ♦ Tele-commuting ♦ Internet connections
Managerial security	◆ Administrative security ♦ Training and awareness ♦ Reporting of security problems ♦ Control selection ◆ Personnel security ♦ Discipline and termination ♦ Reliance on people ♦ Background checks ◆ Organisational structure - responsibility for information security ♦ Management role ♦ Line management role ♦ Information security department role ♦ Information technology department role ♦ Ownership and user responsibilities
Physical security	◆ Physical access security ♦ Building access control (locks and barriers, access records, handling of visitors) ♦ Access control to computer facilities ♦ Hardware security (drive locks, cable traps, universal lock down)

Table 5.1 (continued)

Topic	Aspects
Microcomputer security	◆ Classification of data ◆ Hardware security ◆ Software security ◆ Data security ◆ Responsibilities
Network security	◆ Responsibilities ◆ System access control ♦ Identification and authentication - end-user passwords or other forms of identification ♦ Password system set-up ♦ Log-in/log-off process ♦ Levels of network access – network supervisor, administrative users, trusted users and vulnerable users ◆ Accountability – link all activities on the network to user identity ◆ Audit trails to determine if a security breaches have occurred ◆ Object reuse – secure resources for the use of multiple users ◆ Data exchange – secure transmissions over communication channels ◆ System privileges ♦ Limiting system access ♦ Process for granting system privileges ♦ Process for revoking system access ◆ Viruses, worms and Trojan horses ◆ Data and program back-up ◆ Encryption ◆ Portable computers ◆ Remote printing ◆ Privacy ◆ Logs and other system security tools ◆ Physical security
Internet Security	◆ Information movement ◆ Information protection ◆ Privacy ◆ Resource usage ◆ Access control ◆ Reporting security problems
Internal auditing	◆ Intervals ◆ Extent

(Compare chapter 3 and 4, as well as Stang, 1992:207-212 and Wong & Watt, 1990:137-138)

5.5 DETERMINING THE SECURITY REQUIREMENTS

An important part of the management of information security is to determine the security requirements of an organisation's information system. To determine the security requirements, the following tasks will have to be performed:

5.5.1 BUSINESS RISK ANALYSIS[3]

The aim of a business risk analysis is to determine the extent of business dependence on the computer system and information. Key questions that should be asked are amongst others, the importance of the computer system and information for operational efficiency; business profits; customer satisfaction; management control; and competitive advantage. Other aspects that will have to be covered are communication, data encryption, and electronic data interchange.

5.5.2 EVALUATION OF BUSINESS AND TECHNOLOGY THREATS

Based on the results of the business risk analysis, the business and technical environment will have to be evaluated to determine the possibility of the various business risk exposures to materialise. Areas to be covered include the hardware platform, system configuration, available hardware and system security features, general data flow, network typology and architecture, network management and control, and physical environment.

From chapter 3 it is evident that the potential threat or security breach from the following elements should be evaluated:

- Disloyal or careless technical staff or maintenance engineers.
- Discontented or negligent employees in position of trust, including ex-employees or temporary contractors.
- Outside hackers.
- Trade union activists.
- Radical pressure groups.
- Criminals.
- Unethical business associates or competitors.
- Inquisitive journalists.
- Other subversive elements.

---

[3] This aspect was fully covered in chapter 4 and will not be covered in full again.

Various possible forms of attack, as discussed in chapter 3, should also be considered, namely:[4]

- Abuse of privilege by trusted users, ex-users, service and technical staff to commit fraud or sabotage the system in an act of revenge.
- Planting of illegal trap doors, logic time bombs, Trojan horses, computer viruses, or worms.
- Theft of computer equipment, software or data.
- Sabotage of computer equipment, data lines, network circuits, software, data files, and security files and techniques.
- Natural disasters.
- Hacking from internal and external sources.
- Active and passive wire-tapping or electronic eavesdropping on cable risers, lines, circuits, and junction boxes.
- Monitoring of radio frequency signals from computer screens, printers, power leads and connecting cables, or intercepting data from microwave and satellite transmissions (compare also Parker, 1990:547).
- Others forms of abuse or perpetration specific to the operating environment (compare also Wong & Watt, 1990:146-149).

5.6 DETERMINING OF A CONTROL STRATEGY

In the light of the business dependence on the computer system and information, as well as the evaluation of the technical and physical environment, an information security and control strategy should be developed. By closely examining every area of potential exposure in descending significance, the most effective way of dealing with the threats can be determined.

According to Wong and Watt (1990:149-151) the following control objectives could be considered:

- Risk prevention.

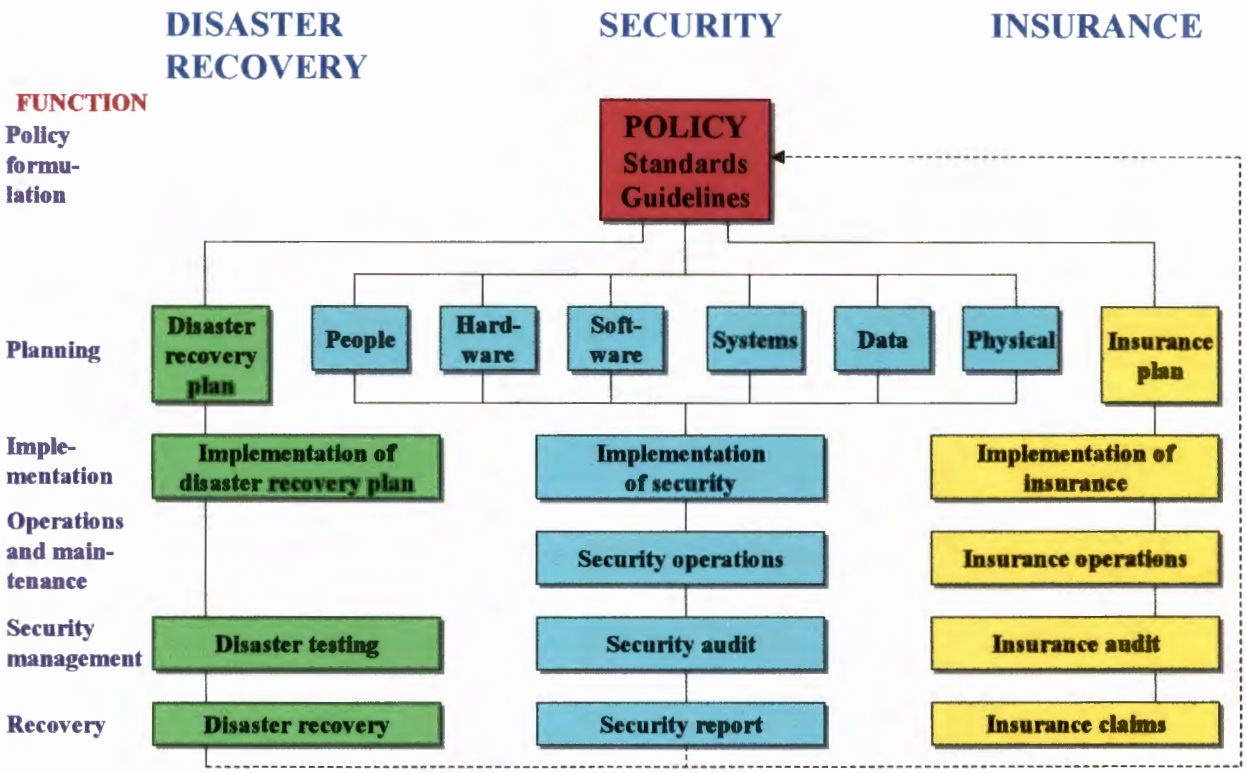
[4] The various security threats and forms of attack were fully discussed in chapter 3.

- Risk reduction.
- Risk detection and response.
- Recovery.

5.7 FORMULATION OF AN INFORMATION SECURITY AND CONTROL FRAMEWORK

This aspect comprises a set of detailed control guidelines and standards for the implementing of information security as stipulated in the security strategy and policy. A slightly simplified version of this framework is presented in figure 5.1.

Figure 5.1 Information security and control framework



Adapted from Louw (1990:79-80), Lowe (1994:127) and Menzies (1993:170).

As can be seen in figure 5.1, there are two dimensions to the framework. The first is the process of information system security and control, which is divided into six functions: policy formulation, planning, implementation, operations and maintenance, monitoring, and recovery. The second is the scope of information systems security and control, which is divided into three broad areas: security and control, disaster recovery, and insurance.

The process of information system security and control begins with the formulation of an information system security and control policy that is consistent with both the company's overall security policy and its information system policy. This policy must then be translated into plans, which will form a subset of both general security and information system plans. The next phase is the implementation of these plans. Once the plans have been implemented, the organisation moves into the operations and maintenance phase. To ensure that the security and control measures continue to operate effectively, they must be monitored or "audited". Finally, if the security and control measures fail, the company must both recover from the situation and enter a new policy formulation or planning phase.

Each of these elements will now be briefly described.

5.7.1 POLICY FORMULATION

Effective policy formulation according to Louw (1990:79) requires four things to be achieved in the following order:

- Firstly, the awareness and involvement of senior management. Without this, neither adequate funding nor consistency with broader corporate policy can be guaranteed.
- Secondly, an assessment of both the importance of information system security to the firm, and the magnitude of the information system risks it faces.
- Thirdly, the level of information system security and control expenditure must be determined, based on a cost/benefit analysis of various security and control programmes.
- Fourthly, the establishment of an infrastructure of standards and contracts with which to guide and support the planning function.

The processes of policy formulation, planning and subsequent stages should encompass all three areas of information system security and control, namely insurance, disaster recovery, and security and control.

5.7.2 INFORMATION SECURITY AND CONTROL PLANNING

Louw (1990:80) argued that information security and control planning comprises six elements:

5.7.2.1 People

People interact with information systems in many ways, and various groups of people have to be considered:

- Firstly, there are people who manage the system and its security. A security committee is needed to co-ordinate the six functions of policy formulation, planning, implementation, operations, monitoring and recovery. The committee should have close links with both the information systems steering committee (or its equivalent) and the corporate security function.
- Secondly, there are the people who use the system, including the company employees. A computer security awareness program for these people should be seriously considered.
- Thirdly, there are outsiders who, as a consequence of connectivity and the transitive flow of information, are able to interact directly or indirectly with the system.

5.7.2.2 Hardware

Hardware security involves limiting of physical access to computers, choosing hardware that is appropriate for the level and type of security desired, and having backup hardware available.

5.7.2.3 Software

Software security encompasses system software and applications software. Issues, which must be addressed, include the nature and extent of systems programming, the use of security software, the nature of application programs, and the sourcing of software.

5.7.2.4 Systems

Systems considerations include input controls, processing controls and output controls. The type of operating system used, and the nature and degree of intra-system and inter-system connectivity utilised must also be examined.

5.7.2.5 Data

Data and information security issues include controlling access to data; controlling data creation, alteration and deletion; data storage; data encryption; classification of information; audit trails; backups; and data erasure.

5.7.2.6 Physical

Physical security is a specialised field that encompasses considerations as diverse as physical access to systems and air conditioning.

5.7.3 DISASTER RECOVERY PLAN

However, despite all the security controls a disaster can happen. As was pointed out in chapter 4 natural disasters like fire, lightning, wind, floods and earthquakes cannot be prevented, but their damage can be limited to a great extent by means of disaster recovery plan (4.3.7.1). Therefore all organisations should formulate a disaster recovery policy, standards and guidelines. This usually culminates in the disaster recovery plan, which is implemented and regularly tested for effectiveness (4.3.7.1.2).

5.7.4 INSURANCE PLAN

If damage occurs during a disaster or security break, the policies and guidelines, which are formalised in the insurance plan, are followed to submit the necessary claims. It is important that the insurance stipulations are followed very closely (insurance operations) and that the plan is audited regularly to ensure realistic insurance values.

The framework encompasses not only the prevention of computer abuse, but also the other types of information security risks discussed earlier. Therefore, using the framework to deal with a specific problem such as computer abuse will often cause other problems to be mitigated to some extent (Louw, 1990:81).

5.7.5 FRAMEWORK CONTROLS

To establish the above mentioned information security framework the following controls that were discussed in chapter 4 can be considered:

- **Organisation controls:** Management and employee security responsibility; the need to know; security classification of documents, files and data; security awareness and training; safe custody of information and physical assets; access control of premises; personnel liaison on security matters; procedures for the handling and disclosure of information; personnel security procedures.

- **Server area controls:** Physical environment; access control; operational control (for example on project documentation); use of powerful utilities; batch and on-line operation; system software and technical support; magnetic file library; software library versions; change control; system maintenance; document and information despatch; and emergency back-up procedures.

- **Network management:** Operational procedures and usage reports; access control (for example the protection of master control terminals, cable risers, and network management area); backup and recovery; software implementation; change control; system maintenance; access security on the public switched network.

- **Access security:** Operating system and application access control facilities; database administration.

- **Operational control of applications:** Application software; message control; validation of transactions; file version control; retention and backup.

- **Message security:** Message authorisation; date and time-stamping; address and content validation; authentication; delivery; accountability for total received, partial loss of contents, drop-outs or line faults; control of integrity during system recovery or retransmission.

- **Data confidentiality:** Encryption of messages and files; backup for encryption systems; key management; passwords and test keys.

- **End user responsibility and custody:** Security of workstations; clerical control procedures; code of good practice; segregation of duties; dual control.

- **Liability and legal issues:** System or network service liability; service agreement with users and outside vendors; insurance cover; legal requirements.

- **General guidelines for controls implementation:** The assurance of data and system integrity (detection and prevention of unauthorised usage; control of physical and logical access; restriction of user privilege; data validation techniques; secure delivery of messages; personnel security procedures such as segregation of duties, dual controls, job rotation); protection of data confidentiality (classification of messages and data; level of access control, for example passwords, user identification, test keys, encryption, authentication keys); limiting liability (control responsibilities of all parties involved; insurance cover for possible losses); back-tracking of events (system auditability; logging); assurance of network functionality (self-checking routines and procedures with positive feedback); operational resilience and system redundancy (use of dual processors, communication circuits, mirror copies of databases; automatic switching and swapping of processors, input and output devices and controllers, lines and circuits; dynamic reconfiguration of lines, nodes, transmission routing, links, port connections and work stations; simultaneous creation of image copies in transaction processing journals); and fallback and recovery (operational backup and contingency provisions; off-site storage; emergency procedures).

5.8 INFORMATION SECURITY IMPLEMENTATION

The next step will obviously be the implementation of the information security policy, guidelines, standards, procedures, controls and techniques. A disaster recovery plan, information security plan and insurance plan should also be implemented. As was pointed out in chapter 4 the best way of doing this is by assigning the task to specific individuals, who will determine priorities, assess impacts on the existing set-up, determine resources required and manage the various projects.

A possibility is to follow an architecture approach. Fitzgerald (1994:11-13) pointed out that an architecture approach implies a proactive understanding of how information is used throughout the organisation and its corresponding security requirements. Thus the following two aspects should be attended to:

- Continuity of computing services (the availability aspect of security) by the establishment of strict maintenance service standards, the provision of redundant support services, strict change control standards, strict back up procedures, and training of employees.

- Control of access to information (the confidentiality and integrity aspects) through logical access control and user accountability. Authentication can be obtained through passwords or third party authentication software.

5.9 INFORMATION SECURITY AUDIT

Lucas (1997:630) stressed the important fact that to ensure that information security countermeasures conform to the security policy, guidelines, framework and requirements, as well as to ascertain that the information security controls that have been established are effective, it is necessary to perform regular security audits.

This is done by a comprehensive and systematic audit, which consists of a series of controlled tests that should be conducted to check the functionality and performance of individual controls, as well as their associated operational control procedures, and monitoring and reporting procedures for security breaches.

A management information system audit (MISA) identifies all the various controls that govern individual information systems and assesses their effectiveness. The audit usually includes operations, physical facilities, telecommunications, control systems, information security objectives, organisational structure, personnel, manual procedures, and individual applications. All control weaknesses are listed and the probability of occurrence and impact estimated (Laudon & Laudon, 1998:646-647). Lodin *et al.* (1997) also mentioned application auditing, which addresses the protection of data and the accountability for reading data (privacy) and writing data (integrity). The disaster recovery plan should also be tested for functionality.

Most computer frauds involve exploiting weaknesses or loopholes in input and output controls. It is therefore necessary to implement a tamperproof local audit trail. Ample audit trails should be provided for computer systems to stress and locate areas of errors and unusual activities. Exception reports should be monitored and reviewed regularly for system irregularities. It should not be possible to turn the system log off (O'Brien, 1998:557-558).

The final test to evaluate the information technology security function is to make a concerted attempt to penetrate security systems and to show certain security flaws or system loopholes.

5.10 AN INFORMATION SECURITY MANAGEMENT MODEL

To manage information security effectively the following model, which consists of five different security levels for the operational security environment (OSE), can be considered according to Von Solms (1993:52-59):

5.10.1 THE CURRENT OPERATIONAL SECURITY ENVIRONMENT

The current operational security environment is the collection of all information services together with all countermeasures installed at any specific point in time as determined by a risk analysis. Introducing more countermeasures can raise the current operational security environment (Von Solms, 1993:54).

5.10.2 THE IDEAL OPERATIONAL SECURITY ENVIRONMENT

The ideal operational security environment is the ideal security situation so that no information security risk will be able to materialise. This ideal operational security environment is determined by top management and specified in the corporate information security policy document. The ideal operational security environment is difficult to achieve because of the cost factor (Von Solms, 1993:55).

5.10.3 THE PRESCRIBED OPERATIONAL SECURITY ENVIRONMENT

The prescribed operational security environment represents a set of countermeasures determined by external factors, for example insurance companies or business partners (Von Solms, 1993:56).

5.10.4 THE BASELINE OPERATIONAL SECURITY ENVIRONMENT

Although an organisation may be confronted by a prescribed operational security environment, the management may for certain reasons (for example financial) decide to accept a lower or

higher operational security environment than defined by the prescribed operational security environment (Von Solms, 1993:57-58).

5.10.5 THE SURVIVAL OPERATIONAL SECURITY ENVIRONMENT

In any organisation, some information services are of vital importance and should be restored immediately in the event of a disaster. These critical information services, together with the countermeasures to restore them, constitute the survival operational security environment (Von Solms, 1993:58-59).

5.11 THE OPTIMUM LEVEL OF SECURITY

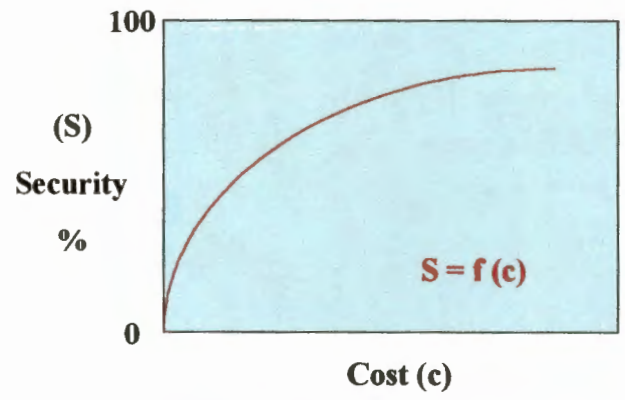
Numerous threats that the information resource is subject to, as well as the countermeasures available to management, have been discussed in chapters three and four. Information systems can make exhaustive use of the control mechanisms discussed above, but will greatly depend on the economic and operational feasibility. It is not always possible to implement maximum security, but rather to opt for the optimum level of information security (Rilley, 1981:43). The optimum level of security is a function of three factors, namely cost, accessibility and vulnerability.

5.11.1 SECURITY/COST RELATIONSHIP

There are different techniques available to determine the optimum point when considering cost versus benefit and benefit versus risk. One such a technique is the well-known cost-benefit analysis to determine the most effective controls without sacrificing operational efficiency or cost. Considerations that should be taken into account usually are the importance of data and the level of risk (Laudon & Laudon, 1998:644-646). Eventually a security budget should be determined, based on the value and sensitivity of the data processed, or the criticality of the system in use, and not the equipment value.

The security/cost relationship is illustrated in figure 5.2.

Figure 5.2: Security/cost relationship

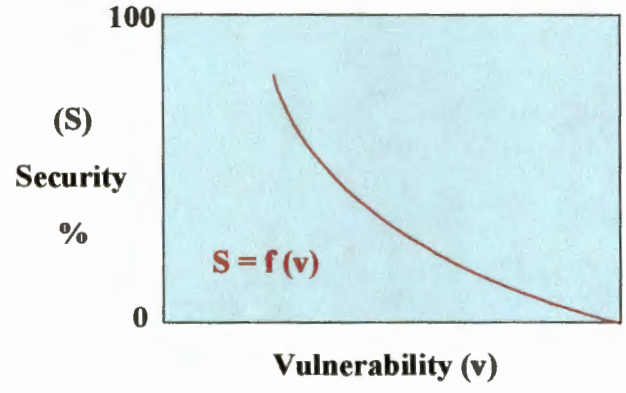


From this illustration it is evident that higher information security induces higher cost, but with diminishing marginal returns. Perfect information security is unattainable and must be matched against the point of diminishing returns for an organisation's particular situation (Applegate *et al.*, 1996:481).

5.12.2 SECURITY/VULNERABILITY RELATIONSHIP

The second technique to determine the optimum level of information security takes the relationship between information security and vulnerability of assets into account. This relationship is illustrated in figure 5.3.

Figure 5.3: Security/vulnerability relationship

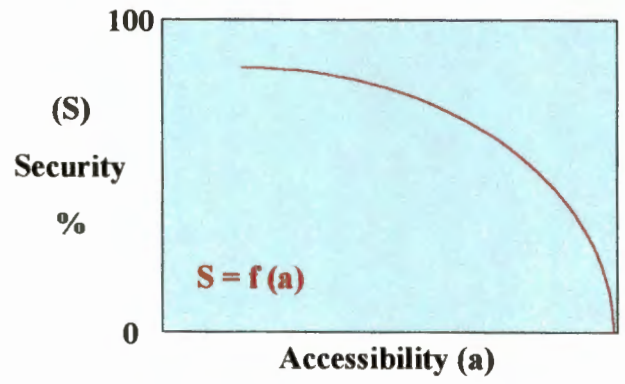


From this graph it is clear that higher security leads to a lower vulnerability to information security risks and threats. The relationship is such, that initially a little security reduces the vulnerability quite substantially (Applegate *et al.*, 1996:481).

5.11.3 SECURITY/ACCESSIBILITY RELATIONSHIP

The last consideration to determine the optimum level of information security is the relationship between information security and accessibility. This relationship is illustrated in figure 5.4.

Figure 5.4: Security/accessibility relationship

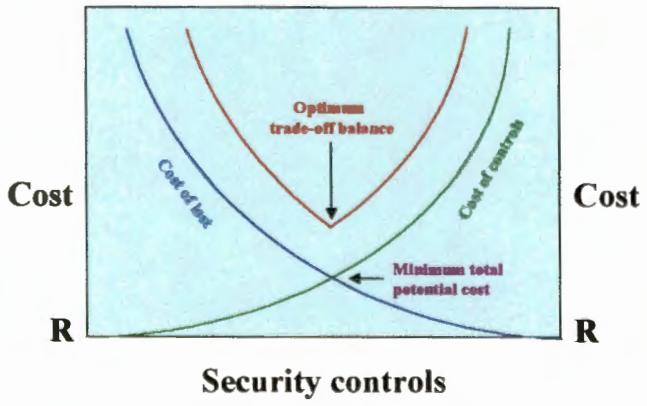


This third graph illustrates that the level of access control and user efficiency is an inverse one, which means that as information security increases, accessibility and efficiency decreases to such an extent that employees will circumvent security (Sundaram, 1998). The only safe computer is a disconnected one, but a useless one. Information security is therefore a trade-off between computer accessibility and restricting its misuse and abuse.

5.11.4 OPTIMUM SECURITY

The optimum level of security can be found when all the above mentioned relationships are simultaneously taken into account. This is illustrated in figure 5.5.

Figure 5.5: Optimum security



Adapted from Robson (1997:493)

The eventual security system will also have to take the cost of the potential loss into account. From the illustration it is evident that as more information security controls are implemented, the potential losses decrease, until the cost of potential losses and controls reach a minimum (Badenhorst, 1989:170-171).

5.12 SUMMARY

No combination of products or procedures can completely safeguard the valuable information resource. Information security needs to be management very carefully. This management

process starts with top management that should realise the strategic importance of their information systems and take responsibility for information security by adequately budgeting for it and by appointing an information security manager.

To enable all employees to understand information security, management should clearly formulate a corporate security policy, security objectives, procedures, standards and guidelines. To determine the security requirements of the organisation a thorough audit of the corporate information security infrastructure should be undertaken. The audit includes an analysis of the confidentiality and criticality of computer resources, an assessment of all the various information security threats, risks and vulnerabilities, as well as an investigation of the available countermeasures, safeguards and controls.

Once the audit is completed a control strategy is determined and a control framework formulated. Thereafter the necessary organisational, personnel, systems and other countermeasures and safeguards are implemented. To determine the effectiveness of the control measures and to enforce the implemented safeguards the security manager and his personnel do regular information security audits, and if necessary maintenance work to ensure the required level of information security.

Although numerous control mechanisms exist it is not always possible to implement maximum information security, but rather to opt for the optimum level of security, which is a function of three factors, namely cost, accessibility and vulnerability.

CHAPTER 6

EMPIRICAL RESEARCH

6.1 INTRODUCTION

The empirical research regarding the information security at Kynoch Fertilizer (Pty) Ltd was done by means of a field study of which three structured questionnaires on information security were an important component. The aim of the field study was to determine the state of information security at the central region of Kynoch Fertilizer (Pty) Ltd.

The objective of this chapter is to set out the background to the design of the questionnaires, as well as the processing of the data and the results of the field study. The development of a questionnaire to gather data for the empirical research is of the utmost importance. Therefore specific attention will be paid in this chapter to the development procedure, structuring and distribution of the questionnaire.

The second part of the chapter will be devoted to the results obtained, as well as a discussion of the results.

6.2 DEVELOPMENT OF THE QUESTIONNAIRES

It is of critical importance that the questions of the questionnaire must be related to the aspects under investigation and the objectives of the study as a whole. The questionnaires were therefore developed by a process, which included the following steps:

6.2.1 OBJECTIVES

The first aspect that needed clarification before the designing of the questionnaire, were the objectives of the research. It was necessary to distinguish between the objectives of the research and the objective of the questionnaire. One of the secondary objectives of the research is to determine the overall state of information security at the central region of Kynoch Fertilizer

(Pty) Ltd, for example strategy, policy, security plan, structures, implementations and controls, and to measure it against the ideal information security situation (compare chapter 1). The objective of the questionnaire was to collect information regarding the state of information security at Kynoch Fertilizer (Pty) Ltd.

The purpose of determining the state of information security at Kynoch Fertilizer (Pty) Ltd is to identify the vulnerabilities and gaps in information security to eventually protect the valuable corporate asset of information. From the literature study (chapters 3 to 5) it became evident that the trend toward global connectivity and the virtual office is creating new security risks. It was also established that information security risks and threats are on the rise, which certainly puts more pressure on management to improve information security and to minimise problems when they occur.

The empirical study will thus try to determine:

- The awareness at Kynoch Fertilizer (Pty) Ltd of the ever-increasing information security risks.
- The effectiveness of the currently implemented security solutions, tools, and available human resources.
- The security concerns and problems at Kynoch Fertilizer (Pty) Ltd.

6.2.2 IDENTIFICATION OF THE POPULATION

Because the focus of the study is on information security at the central region of Kynoch Fertilizer (Pty) Ltd, the questionnaires were limited to the central region and more specifically the head office and plants in Potchefstroom. Three groups were targeted for the distribution of the questionnaires, namely general computer users, departmental and functional heads, and business process support personnel. The population was stratified[1] in order to determine three important perspectives, namely that of the general employees, management and the information technology personnel. The stratification also ensured that general computer users did not have to answer management or specialised information technology questions. In all three groups the units of analysis (Huysamen, 1994:38) were the computer users at Kynoch Fertilizer (Pty) Ltd.

[1] For stratification of the population, see Huysamen (1994:40-41) and Lind and Mason (1994:211-212).

When questionnaires are used, careful attention must be paid to the choice of population and the sample. Care must be taken that the sample is representative of the population in order to receive valid results and make valid deductions (Lind & Mason, 1994:10). Another problem with questionnaires is the poor response, which limit the usefulness of deductions, because of the danger of generalisation of the results as representing the total population (Van der Merwe, 1992:67).

To overcome the first mentioned problem, to make the results more scientifically justifiable, and because the population of computer users at Kynoch Fertilizer (Pty) Ltd is a finite population (Rayner, 1969:26-27), it was decided to use the whole population[2] for all three groups of computer users and not to make use of sampling techniques. If it were kept in mind that the average response to questionnaires is about forty percent, a sample would be too small to make valid deductions (Huysamen, 1994:149-150). A total of 121 computer users were thus identified as the population.

The second problem was limited by emphasising the importance of the study by means of an introductory letter explaining the importance and relevance of the study (annexure A) and by endorsement of the questionnaire by senior management and the business process support manager.

The population for the purposes of determining the state of information security at Kynoch Fertilizer (Pty) Ltd is presented in table 6.1.

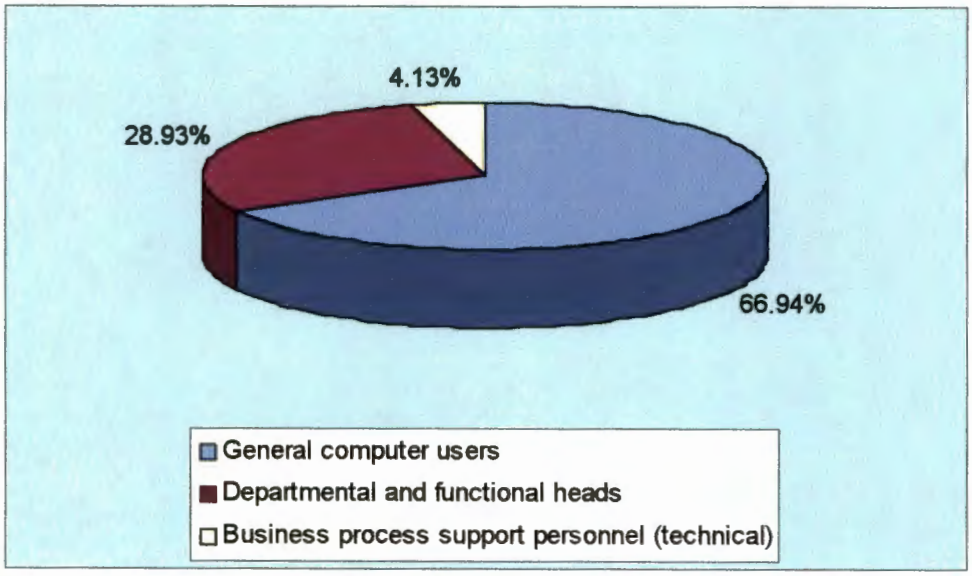
Table 6.1: Composition of the computer user population

Group	Number	Percentage of total personnel component
General computer users	81	24.85%
Departmental and functional heads	35	10.74%
Business process support personnel (technical)[3]	5	1.53%
Total	**121**	**37.12%**

[2] Berenson and Levine (1996:3) define the term population as "the totality of items or things under consideration" and Lind and Mason (1994:7) as "a collection of all possible individuals, objects, or measurements of interest."

The population of computer users is graphically illustrated in figure 6.1.

Figure 6.1: The computer user population



From table 6.1 and figure 6.1 it is evident that the largest target group for the empirical research is the general computer users at Kynoch Fertilizer (Pty) Ltd (66.94%) and that the business support or information technology department is relatively small (4.13%).

A break down of the computer user population according to the various departments is presented in table 6.2.

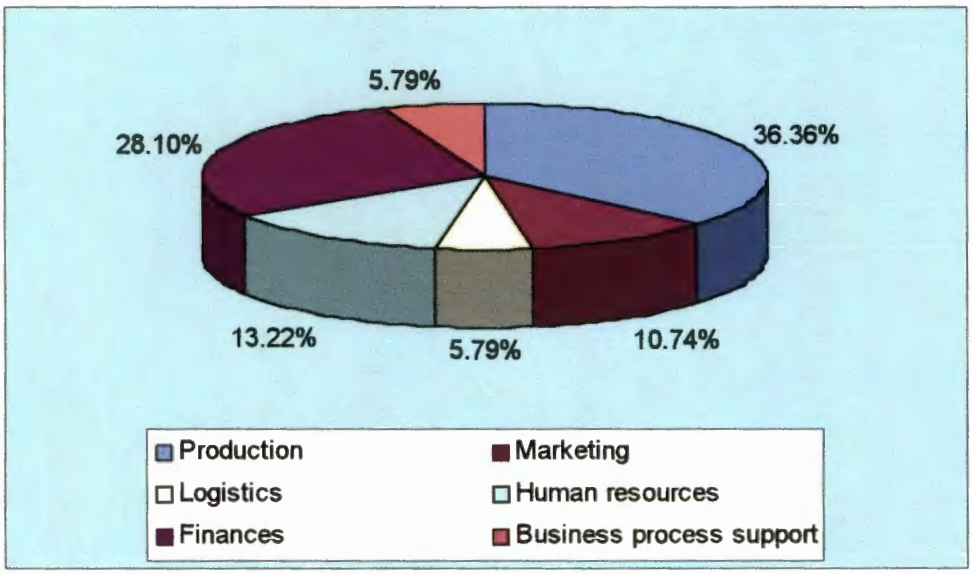
Table 6.2: Computer users according to functional department

Department	Computer users	Percentage of total department personnel
Production	44	35.48%
Marketing	13	11.30%
Logistics	7	38.89%
Human Resources	16	72.73%
Finances	34	85.00%
Business Process Support	7	100.00%
Total	**121**	**37.12%**

[3] The two secretaries of the business process support department were regarded as general computer users because they would not be able to answer specialised information technology questions regarding information security.

The computer users according to the functional department where they are working are graphically illustrated in figure 6.2.

Figure 6.2: Computer users according to functional department



From table 6.2 and figure 6.2 it is clear that although the production department has the largest number of computer users (36.36%), the percentage of the total departmental employees is relatively low (35.48%). The lowest computer usage percentage of the total departmental employees is however the marketing department (11.30%) and the highest is business process support (100%) and finances (85%).

6.2.3 LITERATURE STUDY

An extensive literature study (chapters 3 to 5) was conducted to become familiar with the concept, present situation, issues and problems regarding information security and control. The most important aspects of information security that were identified in the literature study were used to design the questionnaire. These aspects were translated into questions to correspond with the aim of the study.

6.2.4 PILOT STUDY

The need for a pilot study was identified. Personal interviews were held with various computer users and business process support personnel in order to determine the problems and issues regarding information security and control.

Based on the theory of chapters three to five and the unique circumstances of Kynoch Fertilizer (Pty) Ltd (chapter 2), preliminary questionnaires were formulated and tested at Kynoch for clarity of concepts and questions (Berenson & Levine, 1996:22). The testing was done by means of a pilot study amongst five computer users and by submitting the questionnaires to the manager of the business process support department. Recommendations were added and various improvements were made.

To ensure that the questionnaires were practically feasible, the following general guidelines, as stipulated by Huysamen (1994:129-132), were followed when the questionnaires were designed:

- Questions were kept as simple and unambiguous as possible to ensure accurate responses.
- Questions were formulated in words and concepts with which the respondents were familiar (compare also Daellenbach, 1994:102). One of the main objectives of the pilot study was to ensure the clarity of terminology.
- Open-ended questions were limited because it requires a higher level of education on the part of the respondents and respondents are often unwilling to exert the special effort required by open-ended questions. The possibility of obtaining inappropriate responses is also much greater with open-ended questions. Thus open-ended questions were only used where there are too many possible responses, and to determine whether any important aspect of information security had been omitted.
- Double questions were avoided.
- The respondents' literacy level and field of experience were taken into account.
- Leading and loaded questions were avoided.

6.2.5 REFINED QUESTIONNAIRES

After the pilot study, the preliminary questionnaires were refined to eliminate obscurities and possible problems, as well as to suit the specific situation and circumstances of Kynoch

Fertilizer (Pty) Ltd. Mostly only semantic changes were made to the questionnaires to accommodate the terminology used by Kynoch employees.

The refined questionnaires were again submitted to the business process support manager at Kynoch Fertilizer (Pty) Ltd for his comment and recommendations in order to ensure that the empirical research will meet the expectations of senior management at Kynoch Fertilizer (Pty) Ltd. Certain small adjustments were afterwards made to the questionnaires.

6.2.6 FINAL QUESTIONNAIRES

The final questionnaires were then designed and furnished to all computer users at Kynoch Fertilizer (Pty) Ltd according to a list of the relevant units of analysis. The final questionnaires are attached as annexures B, C and D.

6.3 THE STRUCTURE OF THE QUESTIONNAIRES

Three different questionnaires, each consisting of different sections, were used:

- A general questionnaire for all ordinary computers users – sections A and B.
- A management questionnaire for departmental and functional heads – sections A, C and E.
- An expert questionnaire for business process support personnel – sections A, B, D and E.

Each section was introduced by a heading to simplify the completion of the questionnaires (see annexures B, C and D).

The five sections of the questionnaires will now be discussed.

6.3.1 SECTION A

The seven questions in this section were aimed at obtaining biographical data of respondents and thus included questions concerning the demographic en personal particulars of users (see annexures B, C and D).

In order to encourage honest responses, the respondents were not required to identify themselves. Due do the size of the management and business process components, questions which could give away the identity of the respondent were avoided. The relevance of the

applicable data was aimed at compiling profiles of the various respondents in order to interpret the rest of the obtained data in context.

6.3.2 SECTION B

Section B consisted of two major parts. The first nineteen statements measured the general perception of five main aspects of information security at Kynoch Fertilizer (Pty) Ltd. (see annexures B and D).

The second part, which consisted of eighteen statements and five questions, concerned seven aspects of microcomputer or workstation security (see annexures B and D).

6.3.3 SECTION C

Section C also measured the general perception of computer security and microcomputer or workstation security, but a few managerial questions were added (statements 20-22). The first nineteen statements, as well as the last eighteen statements and five questions are exactly the same as those of section B (see annexure B).

6.3.4 SECTION D

Section D was specifically aimed at information technology personnel in order to obtain more technical detail about the information security at Kynoch Fertilizer (Pty) Ltd. The one hundred and sixty-two statements and six questions thus concentrated on seventeen major aspects of information security (see annexure D).

6.3.5 SECTION E

The aim of this section was to evaluate the current information security level at Kynoch Fertilizer. Respondents were thus asked to rate eleven aspects of information security (see annexures C and D).

The section concluded with five open-ended questions regarding information security vulnerabilities, threats and risks.

6.3.6 SCALES

In all sections use was made of survey questionnaires, which are particularly suitable for obtaining biographical particulars, typical behaviour, opinions, beliefs and convictions (Huysamen, 1994:128-133). In section B, C, D and E a four point summated or Likert scale was used to gather the relevant data (Huysamen 1994:124-126). A four-point ordinal measurement scale was selected to avoid neutrality and to force respondents to take a definite viewpoint. A larger scale would make the distinction between the various responses very difficult, and sometimes even artificial.

In section B, C and D the respondent was asked to offer his or her opinion of information security at Kynoch on a continuous four point scale ranging from "strongly disagree" to "strongly agree".

Only four open-ended questions and one yes/no question were asked to obtain information on increases in security risks, virus attacks and any other general observations regarding information security.

In section E respondents were asked to rate the level of information security at Kynoch Fertilizer (Pty) Ltd on a continuous scale from "very poor" to "very good". Section E concluded with five open-ended questions concerning vulnerabilities, threats, risks and security countermeasures.

6.4 DATA COLLECTION

6.4.1 THE PROCESS OF DATA COLLECTION

For the purpose of this study, elements of survey-based feedback were used as a diagnostic approach. The main tool for the collection of data was the three questionnaires. The clarity of the questionnaires was tested by means of semi-structured interviews (Huysamen, 1994:145) and a pilot study amongst the target population. After the finalising of the questionnaires it was delivered by hand to all computer users at Kynoch Fertilizer (Pty) Ltd. It was accompanied by a cover letter explaining the purpose of the study (annexure A).

After the questionnaires were received back all responses were carefully scrutinised for completeness, consistency and errors (Berenson & Levine, 1996:31) and to eliminate

questionable data (Steyn *et al.*, 1994:3). Because the questionnaires were completed anonymous, it was not possible to validate responses by recontacting the individuals. Unusual or inconsistent questionnaires were thus not taken into consideration when the data was processed.

After the processing of the questionnaires, results were checked with Kynoch employees and the business process support manager in order to correctly interpret the information and to get explanations for specific observations. For this, use was made of a convenience sample.

6.4.2 DISTRIBUTION OF QUESTIONNAIRES

A list of all computer users, departmental and functional heads, and business process support personnel were obtained from the business process support department. Because it is relatively well known that the response rate to questionnaires is often below 50% (Huysamen, 1994:148-150), it was decided to deliver the questionnaires in person to ensure the maximum response. A low response rate restricts the usefulness of a survey because it is uncertain to which extent a biased and consequently unrepresentative sample has been obtained (Huysamen, 1994:149-150). The personal delivery of questionnaires also eliminated the possibility that someone, who did not form part of the three targeted groups, answered the questionnaire.

To further increase the response rate and to limit non-response error and bias (Berenson & Levine, 1996:43) all questionnaires were followed up by telephone before the return date. After the return date questionnaires were personally collected (Huysamen, 1994:150).

6.5 RESPONSE

Out of the total of 121 questionnaires distributed, 56 questionnaires were received back, which means a 46.28% total response rate. The response rate for the three respective groups is presented in table 6.3.

Table 6.3: Response rate

Group	Total number of computer users	Number of respondents	Percentage
General computer users	81	34	41.98%
Functional and departmental heads	35	18	51.43%
Business process support personnel (technical)	5	4	80.00%
Total	**121**	**56**	**46.28%**

From table 6.3 it is evident that the best response was amongst business process personnel (80%), which could probably be ascribed to the fact that it is a relatively small department and that the survey was done under its auspices. The management group also had a slightly better return rate (51.43%) than the general computer users (41.98%).

The percentage of respondents in each of the three groups is graphically illustrated in figure 6.3.

Figure 6.3: Respondents according to group

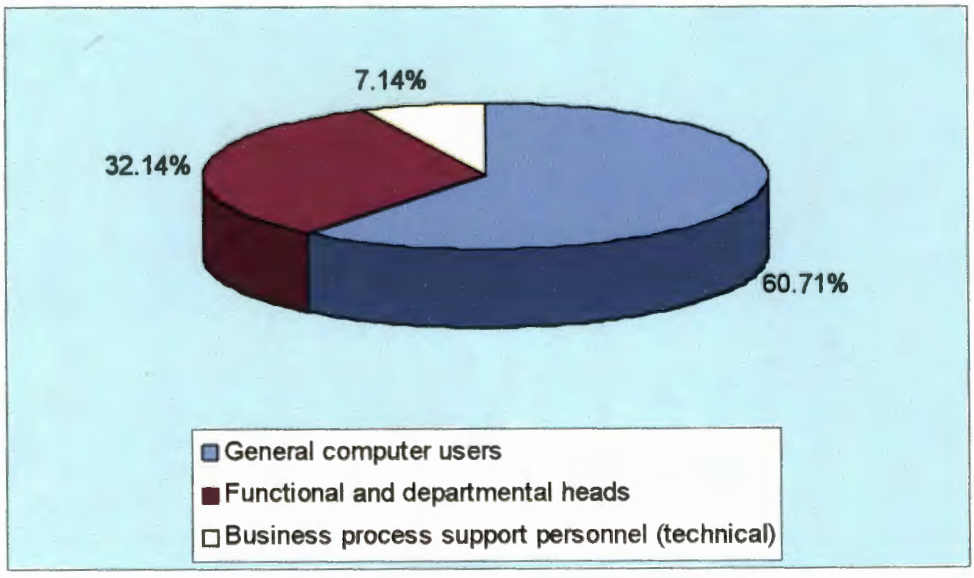


Figure 6.3 shows that 60.71% of the 121 respondents were general computer users, followed by 32.14% from the management cadre, and 7.14% technical business process support personnel.

If these results are compared to the stratification of the population as illustrated in figure 6.1 above, it is quite evident that the respondents are fairly representative of the composition of the population.

The differences in the composition of the population and the composition of the respondents according to the three groups are presented in table 6.4.

Table 6.4: Differences between the composition of the population and respondents according to groups

Group	Population	Respondents	Difference
General computer users	66.94%	60.71%	-6.23%
Departmental and functional heads	28.93%	32.14%	3.21%
Business process support personnel (technical)	4.13%	7.14%	3.01%

From table 6.4 and figures 6.1 and 6.3 it can be established that the respondents are quite representative of the three chosen groups. It is also evident that the business process personnel and management responded better than the general computer users group. This can probably be ascribed to greater responsibility and/or previous experience with questionnaires.

The response rate according to functional departments is presented in table 6.5.

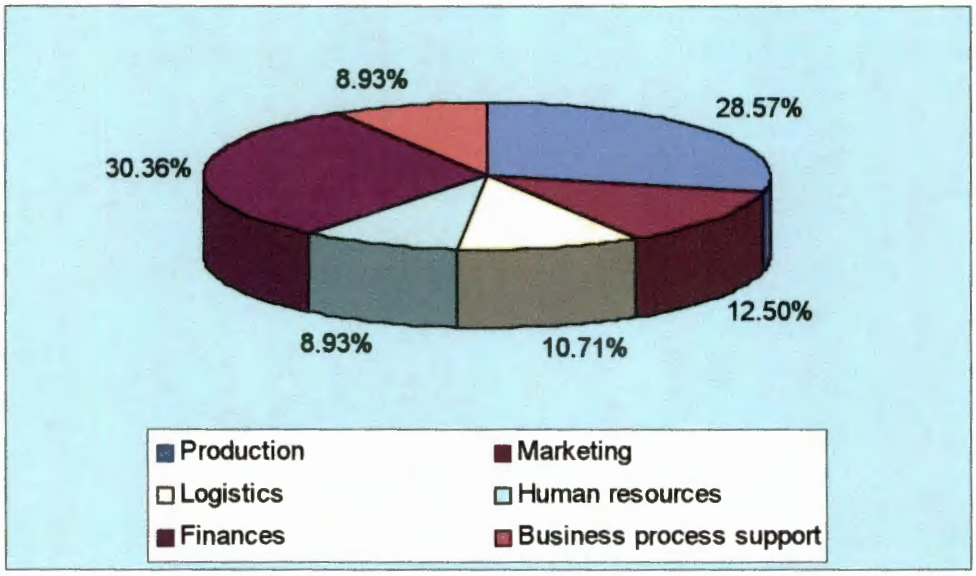
Table 6.5: Response rate according to functional departments

Department	Number of computer users	Number of respondents	Percentage
Production	44	16	36.36%
Marketing	13	7	53.85%
Logistics	7	6	85.71%
Human resources	16	5	31.25%
Finances	34	17	50.00%
Business process support	7	5	71.43%
Total	**121**	**56**	**46.28%**

Table 6.5 shows that the highest response rates came from logistics (85.71%) and business process support (71.43%), and the lowest from human resources (31.25%) and production

(36.36%). The low rate of 36.36% of production can probably partly be ascribed to the fact that the production plant was closed for maintenance work at the time of the completion of the questionnaires. The percentage of respondents according to functional department is illustrated in figure 6.4.

Figure 6.4: Respondents according to functional department



From figure 6.4 it can be seen that the largest number of departmental responses came from finances (30.36%) and production (28.57%), and the smallest from human resources (8.93%) and business process support (8.93%).

If this is compared to the composition of the population of the various departments in figure 6.2 above, it is evident that the respondents are again fairly representative of the departmental composition of computer users at Kynoch Fertilizer (Pty) Ltd.

The differences between the composition of the population and the respondents according to functional departments are presented in table 6.6 below.

Table 6.6: Differences between the composition of the population and respondents according to functional departments

Functional department	Population	Respondents	Difference
Production	36.36%	28.57%	-7.79%
Marketing	10.74%	12.50%	1.76%
Logistics	5.79%	10.71%	4.92%
Human resources	13.22%	8.93%	-4.29%
Finances	28.10%	30.36%	2.26%
Business process support personnel (technical)	5.79%	8.93%	3.14%

From table 6.6 it can be deducted that the logistics and business process support departments responded better than the production and human resources departments.

6.6 RESULTS OF THE EMPIRICAL RESEARCH AND ANALYSIS

6.6.1 PROCESSING OF THE DATA

The responses included nominal data (responses to the demographic questions), as well as ordinal data on a four-point scale. The processing of the data was done by means of the Statistica for Windows 4.5[4] program. In the processing of the data the major emphasis was on descriptive statistics, which is defined by Berenson and Levine (1996:3) as "those methods involving the collection, presentation, and characterisation of a set of data in order to describe properly the various features of that set of data." Descriptive statistics was thus used to organise and summarise the masses of numerical data that have been collected (Lind & Mason 1994:5-6).

Contingency analysis was used to establish whether the demographic variables had an effect on the nominal data collected. A frequency distribution analysis and analysis of variance was used to identify the major information security problems that users experience, and to investigate the variation in the interval scaled variables. Because of the exploratory nature of the research and

[4] StatSoft, Inc. (1995), 2300 East 14th Street, Tulsa, OK, 74104-4442, (918) 749-1119, fax: (918) 749-2217, e-mail: info@statsoftinc.com, WEB: http://www.statsoftinc.com.

also because most of the data are generally ordinal or nominal[5] in nature, the degree of statistical analysis of the results were limited to tabulations and graphical presentations. Open-ended questions were classified and listed (Berenson & Levine, 1996:31).

In order to evaluate the respective statements and questions, the following statistical procedures were performed:

- The processed data was presented as a frequency distribution to facilitate certain calculations, namely the mean, standard deviation and levels of confidence, as well as to make the process of data analysis and interpretation more manageable and meaningful (Berenson & Levine, 1996:62). According to Lind and Mason (1994:22) a frequency distribution is "a grouping of data into categories showing the number of observations in each mutually exclusive category" and is thus an indication of how many respondents assigned a specific value to a question or statement. Histograms[6] were used to portray the frequency distributions graphically for easier interpretation.

- The arithmetic mean, which is the most commonly used average or measure of central tendency (Berenson & Levine, 1996:106), was calculated for each question or statement. The arithmetic mean is calculated by summing the responses received from all respondents, divided by the quantity of times which the item occurred (n) (Berenson & Levine, 1996:106). It pinpoints a centre of the values of a specific set of data (Lind & Mason, 1994:58, 72-74).

- The 95% confidence intervals, which states the range within which the total population parameter is expected to lie (Berenson & Levine, 1996:344-348; Lind & Mason, 1994:225-228).

- To determine the representativeness and reliability of the mean the standard deviation as measure of dispersion was calculated for each question. The standard deviation is the deviation from the arithmetic mean and thus indicates the clustering of values around the mean (Berenson & Levine, 1996:120-124). The lower the value of the standard deviation, the larger is the similarity of the respondents' answers on the specific questions. The higher the value of the standard deviation, the smaller is the similarity between responses received on

---

[5] For the terms ordinal and nominal see Lind and Mason (1994:12-14).

[6] Berenson and Levine (1996) explain histograms on page 70 to 71 and Lind and Mason (1994) on page 35 to 37.

specific questions (Lind & Mason, 1994:85-89). When approximately two-thirds of observations were between the mean plus or minus one standard deviation, the mean was regarded as a reliable average (Berenson & Levine, 1996:295).

- However, when a few extremely large and extremely small items are encountered in a set of data, the mean might not be an appropriate measure of central tendency (Lind & Mason, 1994:62). To overcome this problem and to determine the shape or symmetry of the frequency distribution the degree of skewness of the distribution was determined. If a distribution is positively skewed (right-skewed) the mean is higher than the median and was influenced by a few extremely high values. If the distribution is negatively skewed (left-skewed) the mean is lower than the median and was influenced by a few extremely low values (Berenson & Levine, 1996:127). If a distribution is highly skewed the mean is probably not a good average to use. The coefficient of skewness generally lies between –3 and +3, with 0 as indication that a frequency distribution is symmetrical with no skewness (Lind & Mason, 1994:79-81,102-103).

- Correlation analysis was done to determine the strength of the association between the various variables of the biographical data (Berenson & Levine 1996:714). According to Lind and Mason (1994:328-329), correlation analysis can be defined as "a group of statistical techniques used to measure the strength of the relationship (correlation) between two variables." The strength of the relationship between two variables is usually measured by the coefficient of correlation, whose values range from –1 (perfect negative correlation) to +1 (perfect positive correlation) (Berenson & Levine, 1996:732). Only coefficients of correlation with a 95% level of confidence were taken into account.

- Throughout the statistical analysis the number of respondents were determined by the number of people

In the event of missing data use was made of the casewise deletion technique which resulted in a variation of the valid number of respondents (valid N). Only cases that did not contain any missing data for any of the variables selected for the statistical analysis were included in the analysis. This is especially important in the case of the calculation of correlations. Although use could have been made of mean substitution of missing data (replacing all missing data in a variable by the mean of that variable) in order to eliminate missing data in the data file, it was decided against because mean substitution artificially decreases the variation of scores. This

decrease in individual variables is proportional to the number of missing data, which means that the more missing data, the more "perfectly average scores" will be artificially added to the data set. The second reason is that mean substitution substitutes missing data with artificially created "average" data points and may thus considerably change the values of correlations.

6.6.2 PRESENTATION OF THE RESULTS

The results of the empirical study are reported in tabulated form, and where applicable, also in diagram form.

The various sections of the questionnaire will be discussed as follows:

- Firstly, the biographical questions as answered in section A of all three questionnaires will be discussed.
- Secondly, the responses of the general employees, departmental and functional heads, as well as the business process support personnel, will be discussed in logical groupings at the hand of sections B and C. The three additional questions contained in section C will also be discussed.
- Thirdly, the responses of the business process support specialists will be discussed in logical groupings at the hand of section D.
- Fourthly, the ratings by the departmental and functional heads, as well as the business process support personnel, will be discussed in logical groupings at the hand of section E.

The results will be discussed in terms of three main aspects:

- The topic of the statement or question.
- Results obtained – the results will be presented in tables, frequency distributions and graphs.
- Deductions – certain tendencies will be pointed out. Conclusions will however be left for chapter 7.

6.6.2.1 Results of section A: Profile of the respondents

The biographical and demographic information in section A consisted of seven aspects of which five were qualitative variables and two quantitative variables (Lind and Mason, 1994:11). The results of these questions are summarised in the following tables and figures.

6.6.2.1.1 Age

The age of respondents was measured according to six categories. A frequency distribution of the age of respondents at Kynoch Fertilizer (Pty) Ltd is presented in table 6.7.

Table 6.7: Age distribution of respondents

Category	Count	Cumulative count	% of total cases	Cumulative % of total cases
Under 20	0	0	0.00	0.00
20-29	6	6	10.71	10.71
30-39	24	30	42.86	53.57
40-49	21	51	37.50	91.07
50-59	3	54	5.36	96.43
Above 60	2	56	3.57	100.00
Total	**56**	**56**	**100.00**	**100.00**

From table 6.7 it is evident that more than 50% of respondents are under forty years of age. The largest number of respondents falls into the 30 to 39 and 40 to 49 years age category (80.36%). There are no respondents under the age of twenty and only two above 60 years.

6.6.2.1.2 Gender category

The gender of the respondents is presented in figure 6.5.

Figure 6.5: Gender distribution of respondents

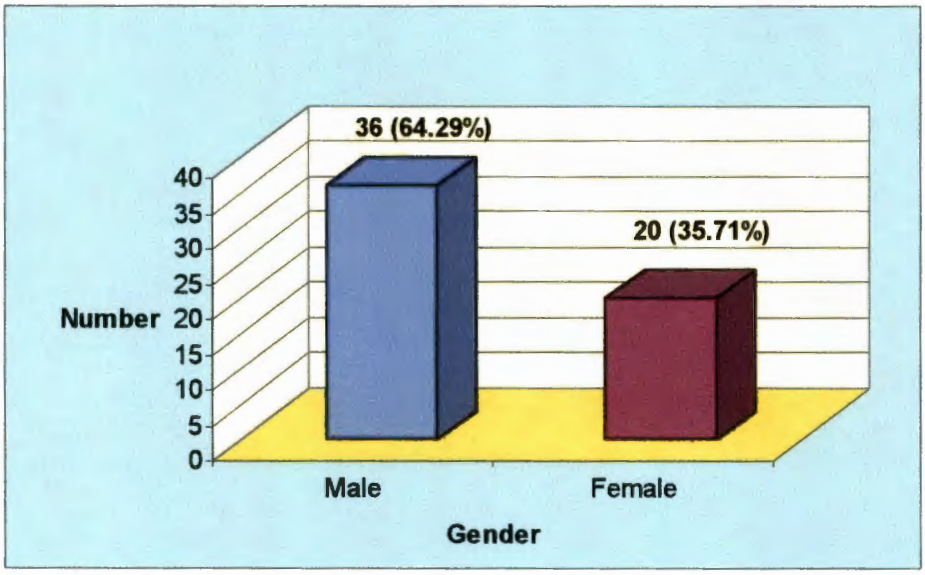
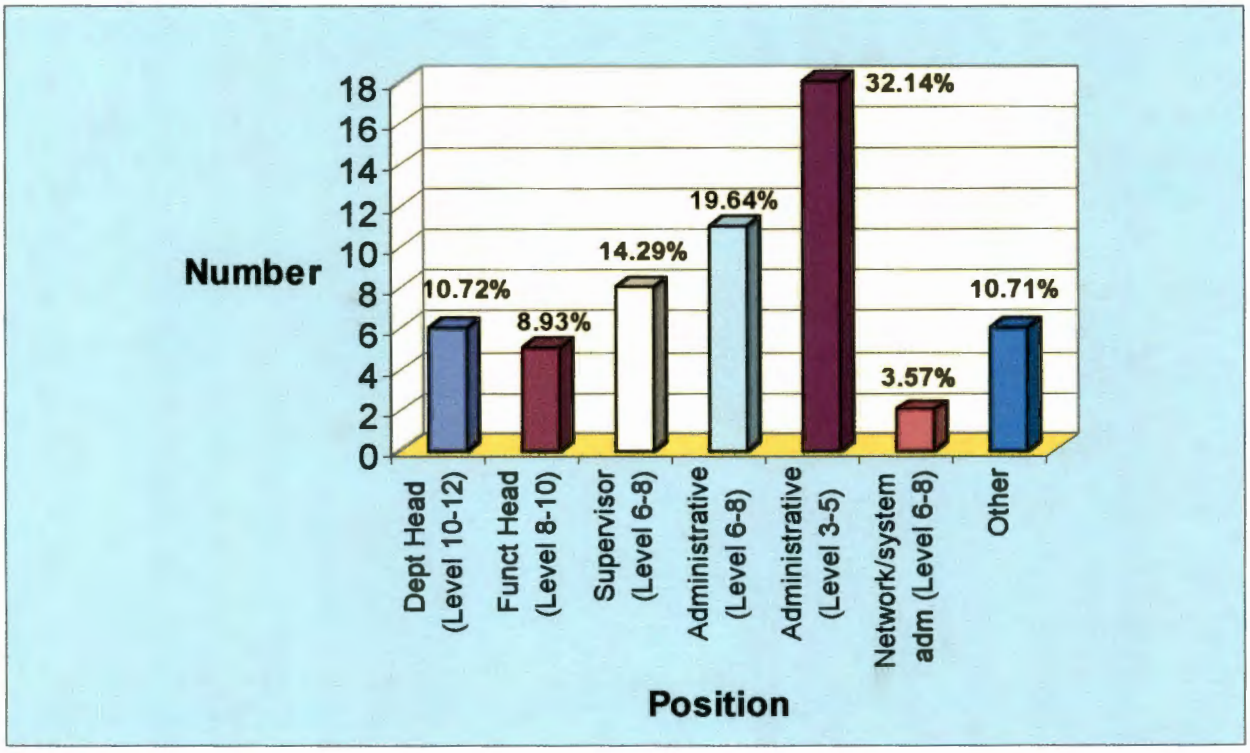


Figure 6.5 indicates that the majority of respondents (64.29%) are male.

6.6.2.1.3 Position and job level

The respondents were asked to indicate their position and job level at Kynoch Fertilizer (Pty) Ltd. The frequency distribution of respondents according to position is depicted in figure 6.6.

Figure 6.6: Distribution according to position and job level



More than half of the respondents is administrative personnel and falls into the 6-8 (19.64%) and 3-5 (32.14%) job level categories.

6.6.2.1.4 Department

Respondents had to indicate in which of the departments they are working. The distribution of respondents according to department is illustrated in figure 6.4 above. According to figure 6.4 the largest percentage of respondents is from finance (30.36%) and production (28.57%), which can be attributed to the fact that production is the largest department of Kynoch Fertilizer (Pty) Ltd and that finance has a very high usage of computers.

6.6.2.1.5 Length of service

The number of years that respondents are employed by Kynoch Fertilizer (Pty) Ltd is presented in table 6.8.

Table 6.8: Distribution of respondents according to years of service

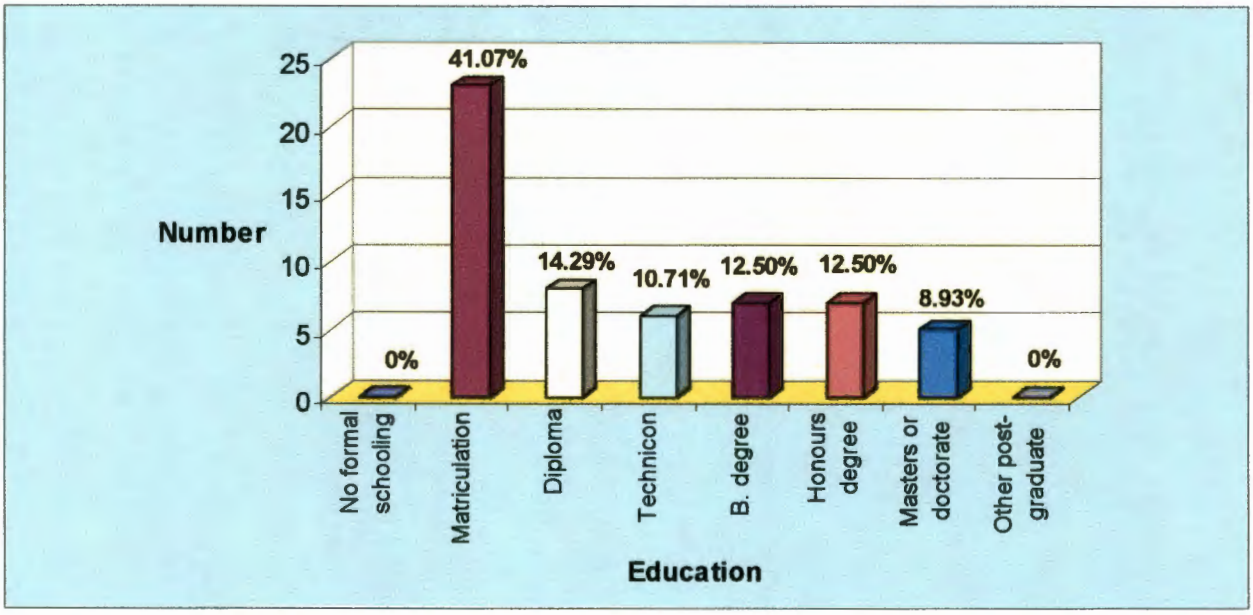
Years of service	Count	Cumulative count	% of total cases	Cumulative % of total cases
Less than 1	4	4	7.14	7.14
1 to 5	14	18	25.00	32.14
6 to 10	20	38	35.71	67.86
11 to 15	12	50	21.43	89.29
16 to 20	3	53	5.36	94.64
21 to 25	3	56	5.36	100.00
26 to 30	0	56	0.00	100.00
More than 30	0	56	0.00	100.00
Total	**56**	**56**	**100.00**	**100.00**

It can be seen from table 6.8 that the highest frequencies appear in the 6 to 10 year (35.71%) and 1 to 5 year (25%) categories. More than two thirds (67.86%) of the respondents has ten or less years of service.

6.6.2.1.6 Educational level

Respondents were asked to indicate the statement which best describes their educational level. The results are presented in figure 6.7.

Figure 6.7: Distribution of respondents according to educational level

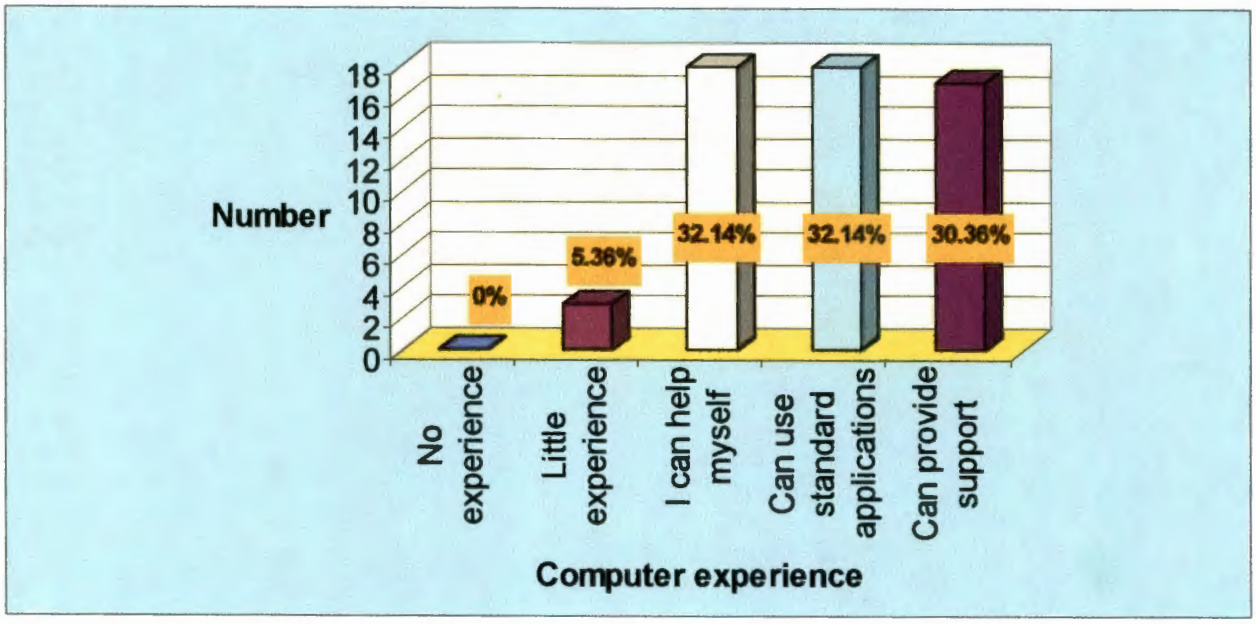


From the above table it is evident that the highest level of education of a large group of respondents (41.07%) is matriculation. However, there are quite a few respondents with postgraduate degrees, for example 12.50% with an honours degree and 8.93% with a masters or doctorate degree.

6.6.2.1.7 Level of computer experience

The different levels of computer experience of respondents are given in the next figure.

Figure 6.8: Distribution of respondents according to level of computer experience



Most computer users who responded have a fair level of computer experience. Of the respondents 62.5% can either use standard applications like Microsoft Word or Quattro Pro (32.14%), or can provide support to other computer users (30.36%). Another 32.14% can help themselves and only a relatively small number acknowledges that they have little experience in the use of computers and need help (5.36%).

6.7.2.2 Results of section B and C

The general computer users, as well as business process support personnel completed section B. The departmental and functional heads completed section C, which is exactly the same as section B, except for statements 20 to 22 which were added.

6.7.2.2.1 Information security awareness and knowledge

Section B and C started out with four statements to determine the general information security awareness and basic knowledge regarding information security amongst computer users at Kynoch Fertilizer (Pty) Ltd. The results of the statements are presented in table 6.9.

Table 6.9: Information security awareness and knowledge

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
1	Important to person	55	3.67	3.54	3.80	0.47	-0.76
8	Very good knowledge	55	2.71	2.53	2.89	0.66	-0.02
9	Adequate training	55	2.02	1.83	2.21	0.71	-0.03
10	Regular updates	55	2.15	1.95	2.34	0.70	-0.21

Although computer users regard information security as very important (3.67 out of a possible 4), they evaluate their own information security knowledge much lower (2.71). A total of 35.71% did not agree with the statement that they have got a very good knowledge about information security. It is also clear that the majority of respondents (73.21%) do not regard the information security training that they received as new employees as adequate (2.02). Neither do they receive regular information security updates or reminders (2.15; 66.07% disagreed).

6.7.2.2.2 The management of information security

Statements 2 to 7 tested the perception of respondents regarding the management of information security. The results are presented in table 6.10.

Table 6.10: The management of information security

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
2	Important to senior management	55	3.33	3.15	3.50	0.64	-0.41
3	Top management accept and understand responsibility well	53	3.02	2.85	3.19	0.60	-0.01
4	Top management strategies meet needs	54	2.87	2.68	3.06	0.70	-0.16
5	Past performance of top management excellent	53	2.64	2.44	2.84	0.74	0.69
6	High level of alignment between business and information security strategy	53	2.79	2.63	2.96	0.60	0.10
7	Effective administration	55	2.55	2.39	2.70	0.57	-0.18

From the results it is clear that 89.29% of respondents think that senior management regards information security as very important (3.33). Although somewhat less convinced (3.02),

78.57% of respondents also feel that the current top management at Kynoch Fertilizer (Pty) Ltd accept and understand their responsibility towards information security and control well. Respondents are however less positive with regard to top management's information security strategies (2.87; 69.64% agreed) and past performance (2.64; 46.43% agreed). The effectiveness of the information security administration and alignment between business and information security strategies are also evaluated lower (respectively 2.55 and 2.79; 53.58% and 66.07% agreed).

6.7.2.2.3 The overall state of security

The next eleven statements had as goal to establish the overall state of security at Kynoch Fertilizer (Pty) Ltd. The results are summarised in table 6.11.

Table 6.11: Overall state of security

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
11	Effective planned incident response	54	2.39	2.19	2.58	0.71	0.25
12	Effective formal incident response team	54	2.48	2.29	2.67	0.69	-0.64
13a	Satisfied with security of client/server system	52	2.98	2.83	3.13	0.54	-0.79
13b	Satisfied with security of NT file servers	47	2.85	2.66	3.04	0.66	-0.31
13c	Satisfied with security of communication servers	48	2.81	2.61	3.02	0.70	-1.24
13d	Satisfied with security of customer universe	44	2.61	2.40	2.82	0.69	-0.65
13e	Satisfied with security of desktop computers	44	2.48	2.28	2.68	0.66	-0.91
13f	Satisfied with security of remote computing	43	2.44	2.24	2.65	0.67	-0.79
13g	Satisfied with security of laptops	45	2.38	2.18	2.57	0.65	-0.56
14	Information is very accessible	53	3.04	2.88	3.20	0.59	0.00
19	Satisfied with security of Internet connection	45	2.89	2.71	3.07	0.61	-0.57

A total of 57.14% of respondents disagreed that Kynoch Fertilizer (Pty) Ltd has an effective planned incident response when an intruder is detected in the computer network (2.39). Only 53.57% agreed that Kynoch Fertilizer (Pty) Ltd has an effective response team (2.48). When asked to respond to the overall level of security, respondents were positive about the security of

the client/server system on which the SAP/R3 system is running (2.98; 82.14% agreed), the Internet connection (2.89; 64.29% agreed), the Windows NT file servers (2.85; 62.5% agreed), and the customer universe system (2.61; 50% agreed). The respondents were less positive about the level of security of desktop computers (2.48; 44.64% agreed), remote computing (2.44; 41.07% agreed), and laptops (2.38; 42.86% disagreed). A total of 80.36% of respondents agreed that despite all the security measures their information is still very accessible (3.04).

The distribution of the responses to statement 13c is negatively skewed (-1.24), with the result that the mean (2.81) is probably not a good indication of the central tendency. If the frequency distribution is consulted, it is evident that 35 out of 48 respondents agreed and 4 strongly agreed that they are satisfied with the overall level of security on the communication servers.

6.7.2.2.4 Information security risks

The goal of statements 15 and 16 was to determine if there was an increase in information security risks. The results are presented in the next table.

Table 6.12: Security risks

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
15	Security risks increased over the past 3 years	49	2.94	2.76	3.12	0.63	0.04
16	Security risks relative to growth in computing resources increased more	48	2.94	2.79	3.09	0.52	-0.09

A total of 67.86% of respondents felt that information security risks increased over the past three years (2.94). This increase in risks is greater than the increase in computing resources (2.94; 71.43% agreed).

When respondents were asked to elaborate on the increase in security risks over the past three years, the following aspects were mentioned.

Risks decreased because:

- Passwords were introduced (3).
- Authorisation profiles have been introduced (2).

- Online backups are made.

Risks increased because:

- Client/server technology was implemented.
- The number of personal computers increased tremendously.
- The amount of information handled increased.
- Access via personal computers increased.
- The change to SAP/R3 was very slow and thus the risk factor increased and gave opportunity for active fraud.
- Valuable information can easily be lost.

6.7.2.2.5 Information security concerns and threats

In table 6.13 the results are given of statements 17 and 18 that endeavoured to establish the information security concerns of respondents, as well as the perceived level of threat with regard to the unauthorised disclosure of information.

Table 6.13: Security concerns and threats

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
17c	Concerned about end-user computing security awareness	52	**2.87**	2.66	3.07	0.74	-0.38
17a	Concerned about network security	53	**2.79**	2.59	3.00	0.74	-0.23
17e	Concerned about distributed computing security	51	**2.71**	2.52	2.89	0.67	-0.40
17d	Concerned about monitoring user compliance with policies	51	**2.71**	2.51	2.90	0.70	-0.24
17b	Concerned about multiple log-ons and passwords	54	**2.70**	2.51	2.90	0.72	-0.13
17g	Concerned about internet access	48	**2.63**	2.40	2.85	0.76	-0.14
17f	Concerned about winning top management commitment	48	**2.54**	2.36	2.72	0.62	-0.45
17h	Concerned about external or remote access (dial-in)	48	**2.54**	2.35	2.73	0.65	-0.64
18f	Perceived level of threat of computer "terrorists"	50	**2.76**	2.54	2.98	0.77	-0.11
18c	Perceived level of threat of employees who do not need to know	49	**2.61**	2.42	2.81	0.67	-0.21
18b	Perceived level of threat of competitors	46	**2.61**	2.38	2.84	0.77	0.22

Table 6.13 (continued)

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
18a	Perceived level of threat of suppliers	50	**2.56**	2.36	2.76	0.70	0.14
18d	Perceived level of threat of customers	49	**2.47**	2.29	2.65	0.62	-0.16
18e	Perceived level of threat of public interest groups	46	**2.46**	2.24	2.67	0.72	0.53
18g	Perceived level of threat of government	47	**2.30**	2.12	2.48	0.62	0.83

The information security concerns of respondents and the perceived level of threat of unauthorised disclosure of information in table 6.13 is respectively listed in order of importance according to the arithmetic means.

6.7.2.2.6 Information or financial losses

Section C also contained three additional statements regarding the consequences of and obstacles to information security. These statements were specifically aimed at management. In table 6.14 the responses of the managers regarding information and financial losses are presented.

Table 6.14: Information or financial losses

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
20b	Rarely experienced losses due to malicious attacks from outside	12	**2.42**	2.09	2.74	0.51	0.39
20c	Rarely experienced losses due to malicious attacks from employees	12	**2.42**	2.09	2.74	0.51	0.39
20a	Rarely experienced losses due to viruses	13	**2.54**	2.22	2.85	0.52	-0.18
20d	Rarely experienced losses due to inadvertent errors by insiders and outsiders	12	**2.58**	2.26	2.91	0.51	-0.39
20g	Rarely experienced losses due to industrial espionage	12	**2.58**	2.26	2.91	0.51	-0.39
20h	Rarely experienced losses due to unknown sources	13	**2.62**	2.31	2.92	0.51	-0.54
20e	Rarely experienced losses due to lack of systems or telecommunications availability	13	**2.69**	2.40	2.98	0.48	-0.95
20f	Rarely experienced losses due to natural disasters	13	**2.85**	2.62	3.07	0.38	-2.18

Table 6.14 (continued)

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
21d	Information losses mainly ascribed to software errors	13	**2.92**	2.76	3.09	0.28	-3.61
21c	Information losses mainly ascribed to computer failures	12	**2.83**	2.59	3.08	0.39	-2.06
21f	Information losses mainly ascribed to network failures	13	**2.69**	2.40	2.98	0.48	-0.95
21a	Information losses mainly ascribed to network break-ins	12	**2.33**	2.02	2.65	0.49	0.81
21g	Information losses mainly ascribed to other reasons	9	**2.33**	1.95	2.72	0.50	0.86
21e	Information losses mainly ascribed to stolen data	12	**2.00**	1.62	2.38	0.60	0.00
21b	Information losses mainly ascribed to employee sabotage	12	**1.92**	1.59	2.24	0.51	-0.21

Managers were relatively sure that although information security problems were encountered, information and financial losses over the past three years were rarely experienced. The information security threats and resultant losses (statement 20), as ranked by the respondents, are listed according to the arithmetic means in table 6.14. Statement 20f is largely negatively skewed (-2.18), which is a sign that the mean is probably not a good indication of central tendency. The skewness is due to the fact that eleven respondents (61.11%) agreed that Kynoch Fertilizer (Pty) Ltd rarely experienced information or financial losses due to natural disasters. Only two respondents (11.11%) disagreed with the statement.

The reasons for information losses at Kynoch Fertilizer (Pty) Ltd (statement 21) is also ranked in table 6.14 according to the arithmetic mean. The arithmetic means of the last four reasons are an indication that respondents did not feel strongly that they contributed to information losses. Statements 21c and 21d are also highly negatively skewed (-2.06 and –3.61), which is mainly due to the fact that ten (out of twelve) respondents agreed about the importance of computer failures and twelve (out of thirteen) agreed about the importance of software errors as reasons for information losses.

6.7.2.2.7 Obstacles to addressing information security

Statement 22 was inserted to ascertain the major obstacles to addressing information security at Kynoch (Pty) Ltd. The results are given in table 6.15.

Table 6.15: Obstacles to information security

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
22e	Lack of budget	13	**2.85**	2.62	3.07	0.38	-2.18
22d	Security planning does not form part of total strategic and business planning	13	**2.77**	2.50	3.03	0.44	-1.45
22b	Lack of human resources	13	**2.69**	2.40	2.98	0.48	-0.95
22c	Lack of management awareness of the importance of information security	13	**2.69**	2.40	2.98	0.48	-0.95
22f	Other obstacles	6	**2.67**	2.12	3.21	0.52	-0.97
22a	Lack of tools or security solutions	13	**2.62**	2.31	2.92	0.51	-0.54

The obstacles to addressing information security are ranked in table 6.15 according to the arithmetic means. Statements 22e and 22d are negatively skewed (respectively –2.18 and -1.45), which indicates that the majority of respondents (eleven and ten out of thirteen) agreed that the major obstacles to addressing information security are lack of budget, and the fact that security planning do not form part of the total business planning. This observation is also supported by the relatively low standard deviations (0.38 and 0.44).

6.7.2.2.8 Backup procedures

The second part of section B and C concerned microcomputer or workstation security. The first two statements tested for backup procedures of computer users. The statistics of these two questions are summarised in the following table.

Table 6.16: Backup procedures

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
20/23	Regular backups	47	2.70	2.47	2.93	0.78	-0.86
35/38	Record version numbers and creation dates for backups	49	2.39	2.19	2.58	0.67	0.21

Although 60.71% of respondents make regular backups of their hard disks (2.70), only 35.71% record the version numbers and creation dates (2.39).

6.7.2.2.9 Physical security

The next six statements had as goal to evaluate a few general aspects of physical security. The results are offered in table 6.17.

Table 6.17: Physical security

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
22/25	Regularly take micro off-site	46	2.33	2.10	2.55	0.76	-0.32
23/26	Written permission required to take micro off-site	47	2.87	2.64	3.11	0.80	-0.03
24/27	Micro seldom left in unattended vehicle	46	2.89	2.62	3.17	0.92	-0.48
25/28	All floppy disks are labelled	46	2.83	2.62	3.04	0.71	-0.13
26/29	Cables do not trail across floor	49	2.92	2.68	3.16	0.84	-0.51
28/31	All wiring electrically safe	49	3.16	2.98	3.34	0.62	-0.66

It seems as if employees rarely take their microcomputers off-site (2.33; only 37.5% agreed) and that when employees want to take the microcomputer off-site, written permission from the manager is required (2.87; 55.36% agreed). If the computer is taken off-site it is seldom left in an unattended vehicle (2.89; 57.14% agreed).

Floppy disks are clearly labelled (2.83; 57.14% agreed) and all cabling (2.92; 64.29% agreed), especially electrical wiring (3.16; 80.36% agreed), is safe.

6.7.2.2.10 Access security

The next subsection tried to determine the level of access security and is presented in table 6.18.

Table 6.18: Access security

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
127/30	Do not leave micro on when unattended	49	2.61	2.34	2.88	0.93	-0.10
29/32	Always have to enter identification and password	49	3.10	2.87	3.33	0.80	-0.70
30/33	User identification is unique	52	3.29	3.15	3.43	0.50	0.46
31/34	Password is unique	51	3.39	3.25	3.53	0.49	0.46
32/35	Change password regularly	52	2.81	2.61	3.01	0.72	0.30
33/36	Log-off when leaving micro for more than 15 minutes	52	2.23	1.98	2.48	0.90	0.53

Just less than half of the computer users (27 out of 56 or 48.21%) do not leave their micros on when unattended (2.61). However, 46.43% of computer users (36 out of 56) do not log off from the network when leaving the micro for more than fifteen minutes (2.23).

The use of login identifications and passwords are mostly according to general standards (3.39, 3.29, and 3.10; 71.43%, 91.07%, and 91.07% respectively agreed). However, passwords can be changed more regularly (2.81; 58.93% agreed).

6.7.2.2.11 Information systems development and documentation security

The security aspects of information systems development and documentation were established by three questions as depicted in table 6.19.

Table 6.19: Information systems development and documentation

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
21/24	Applications are documented sufficiently	50	2.88	2.67	3.09	0.75	-0.11
34/37	Test all new applications and changes	48	2.81	2.60	3.03	0.73	-0.03
37/40	Insist that all new applications and changes be delivered with documentation	52	2.88	2.68	3.09	0.73	-0.13

New applications and changes to existing applications are tested (2.81; 57.14% agreed) and are usually sufficiently documented (2.88; 62.5% agreed). Respondents also insist that new

applications and changes to existing applications be accompanied by full documentation (2.88; 66.07% agreed).

6.7.2.2.12 Operations and maintenance security

In table 6.20 the results of statement 36 are given. This statement had as goal to determine the state of operations and maintenance security.

Table 6.20: Operations security

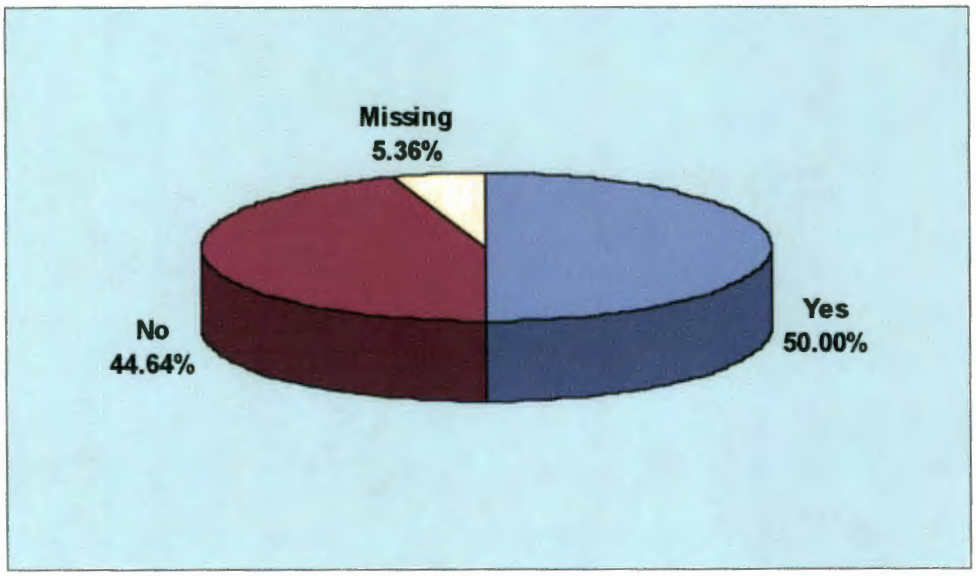
Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
36/39	Only I myself and specialists manipulate system software	52	3.15	2.97	3.34	0.67	-0.59

A total of 82.14% of respondents indicated that no other people than they themselves or the company's computer specialists are allowed to manipulate the system software (3.15).

6.7.2.2.12 Computer viruses

Questions 38 and 41 tried to determine the extent of computer virus attacks at Kynoch Fertilizer (Pty) Ltd. The results are presented in figure 6.9.

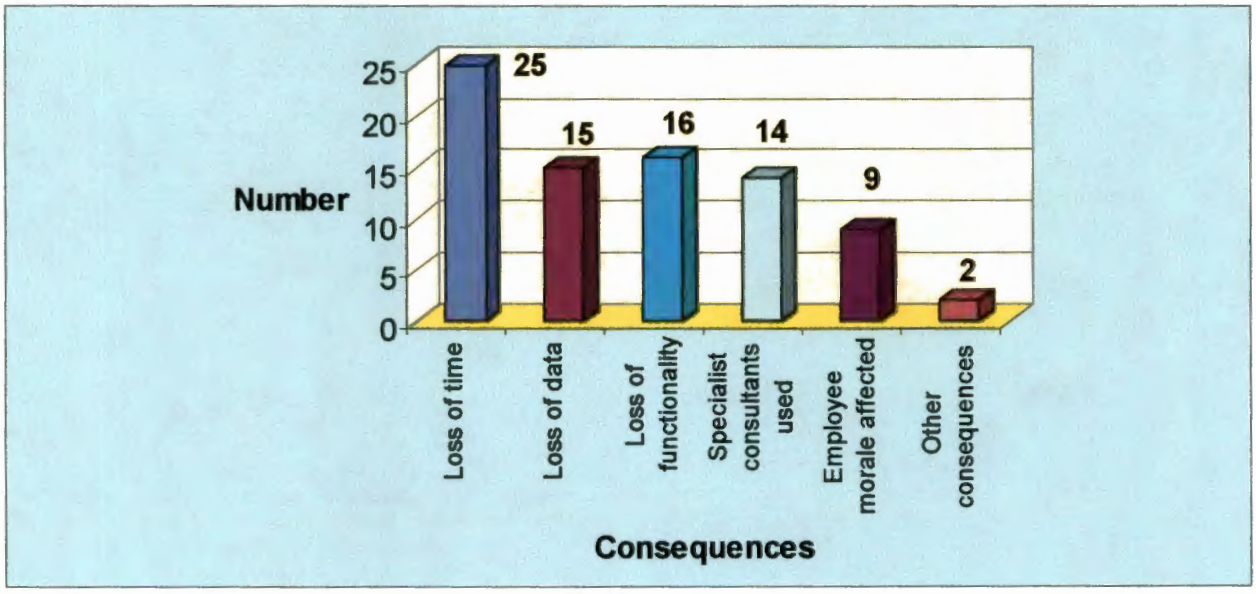
Figure 6.9: Computer virus attacks



From the pie chart it is evident that halve of the respondents (50%) experienced a computer virus attack.

In questions 39 and 42 the consequences of the virus attack were established. The results are illustrated in figure 6.10.

Figure 6.10: Consequences of the computer virus attack



From figure 6.10 it is clear that the consequences of computer virus attacks can be ranked as follows:

1. Loss of time (25; 44.64%).
2. Loss of functionality (16; 28.57%).
3. Loss of data (15; 26.79%).
4. Specialist consultants used (14; 25%).
5. Employee moral affected (9; 16.07%).
6. Other consequences (2; 3.57%).

When respondents were asked about the type of virus in questions 40 and 43, the following responses were received:

- CAP (4).

- Unknown (3).
- Stone.
- Concept.
- Various types.
- Exebug.

Respondents also furnished other details about the computer virus attack:

- Loss of valuable time (2).
- System inoperable.
- Destroyed all data.
- Not serious due to virus protection programs.
- Problems were solved rapidly by own personal computer specialists.
- File corruption experienced.

6.7.2.2.13 General information security observations

On a question if there were any general information security observations respondents mentioned the following items:

- Computer staff unqualified, incompetent, unreliable and renders a poor service (4).
- Low commitment to work amongst computer staff.
- Not enough staff.

6.7.2.2 Results of section D

Only the business process support personnel completed section D. Since the business process support department is a very small department and four out of a possible five employees with the necessary technical knowledge responded, care should be taken when interpreting the results. In many instances the distribution of responses were skewed, which is relatively normal with such a small number of respondents. For this reason the skewness will not be interpreted in this section.

6.7.2.3.1 General information security

The first seven statements tested the state of general information security. The results are summarised in table 6.21 below.

Table 6.21: General security

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
1a	High level of security in system development of client/server system	4	2.75	1.95	3.55	0.50	-2.00
1b	High level of security in system development of NT or UNIX system	4	2.75	1.95	3.55	0.50	-2.00
1c	High level of security in system development of communications system	4	2.75	1.95	3.55	0.50	-2.00
1d	High level of security in system development of desktop computing	4	2.75	1.95	3.55	0.50	-2.00
1e	High level of security in system development of remote computing	4	2.25	1.45	3.05	0.50	2.00
1f	High level of security in system development of laptop computing	4	2.25	1.45	3.05	0.50	2.00
2f	Virus detection software is regularly used	4	3.50	2.58	4.42	0.58	0.00
2g	Secure modems are regularly used	4	3.25	2.45	4.05	0.50	2.00
2i	Firewalls are regularly used	4	3.25	2.45	4.05	0.50	2.00
2d	Network access control software is regularly used	4	3.00	--	--	0.00	--
2b	Token-based or one-time passwords are regularly used	4	2.75	1.95	3.55	0.50	-2.00
2k	PC access control software is regularly used	4	2.75	1.95	3.55	0.50	-2.00
2l	PC hardware security devices are regularly used	4	2.50	1.58	3.42	0.58	0.00
2r	Terminal key locks or lock words are regularly used	4	2.50	1.58	3.42	0.58	0.00
2j	Redundant communications are regularly used	4	2.50	0.91	4.09	1.00	2.00
2n	Business continuity planning software is regularly used	4	2.25	1.45	3.05	0.50	2.00
2c	Security evaluation software is regularly used	4	2.00	0.70	3.30	0.82	0.00
2e	Single sign-on software is regularly used	4	2.00	--	--	0.00	--
2m	Signature verification is regularly used	4	2.00	--	--	0.00	--
2o	Telecommunications encryption is regularly used	4	2.00	--	--	0.00	--
2p	Biometrics to authenticate users are regularly used	4	2.00	--	--	0.00	--

Table 6.21 (continued)

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
2q	Message authentication is regularly used	4	2.00	--	--	0.00	--
2a	File encryption is regularly used	4	1.75	0.95	2.55	0.50	-2.00
2h	Public-key cryptography is regularly used	4	1.75	0.95	2.55	0.50	-2.00
3	Has an experienced team for information security	4	2.25	0.73	3.77	0.96	-0.85
4	Business continuity planning is a high priority	4	2.75	1.95	3.55	0.50	-2.00
5a	Computer/operations centre is important in continuity planning	4	2.75	1.95	3.55	0.50	-2.00
5b	LAN is important in continuity planning	4	2.75	1.95	3.55	0.50	-2.00
5c	End-user computing is important in continuity planning	4	2.75	1.95	3.55	0.50	-2.00
5d	Recovery of mission critical business processes is important in continuity planning	4	2.75	1.95	3.55	0.50	-2.00
5e	Complete restoration of systems is important in continuity planning	4	2.75	1.95	3.55	0.50	-2.00
6	The formal corporate information security policy is very important	4	2.75	1.95	3.55	0.50	-2.00
7a	Centralised security administration is very important according to security policy	4	2.75	1.95	3.55	0.50	-2.00
7b	Business continuity planning is very important according to security policy	4	2.75	1.95	3.55	0.50	-2.00
7c	Surveillance and monitoring is very important according to security policy	4	2.75	1.95	3.55	0.50	-2.00
7d	External access is very important according to security policy	4	2.75	1.95	3.55	0.50	-2.00
7e	Data classification is very important according to security policy	4	2.75	1.95	3.55	0.50	-2.00
7f	Records management is very important according to security policy	4	2.75	1.95	3.55	0.50	-2.00
7g	End user computing is very important according to security policy	4	2.75	1.95	3.55	0.50	-2.00
7h	Non disclosure agreements are very important according to security policy	4	2.00	--	--	0.00	--
7i	Electronic commerce is very important according to security policy	4	2.50	1.58	3.42	0.58	0.00
7j	Incident response is very important according to security policy	4	2.50	1.58	3.42	0.58	0.00

From the results it is clear that in most instances (1a-d: 75% agreed) there is a high level of integration of security considerations in the system development process, except remote and laptop computing (1e-f: 75% disagreed).

Security measures, which are regularly used by Kynoch Fertilizer (Pty) Ltd (statement 2), are ranked in table 6.21 according to the arithmetic means. Single sign-on software, signature verification, telecommunications encryption, biometric authentication, message authentication (2.00; 100% disagreed); and file encryption and public-key cryptography (1.75; 75% disagreed and 25% strongly disagreed) are not used.

Only 50% of respondents view the team for information security as experienced (2.25). 75% regard business continuity planning as a high priority (2.25). All five aspects of business continuity planning (5a-f) are regarded as important (2.75; 75% agreed).

A total of 75% of respondents deem the company's formal corporate information security policy as very important (2.75). Aspects 7a-g are regarded as the most important (2.75; 75% agreed), whilst 7i-j (2.50; 50% agreed) are somewhat less important. Only non-disclosure agreements by personnel are regarded as not important (2.00; 100% disagreed).

6.7.2.3.2 Network security

Statements 8 to 28 tested network security. Table 6.22 presents the results.

Table 6.22: Network security

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
8	Network security is very effective	4	2.75	1.95	3.55	0.50	-2.00
9	Network is protected from internal and external attack	4	2.25	1.45	3.05	0.50	2.00
10	LAN usage is monitored	4	2.50	1.58	3.42	0.58	0.00
11	Network connections to business partners and clients are constantly monitored	4	2.25	1.45	3.05	0.50	2.00
12	All transmitted information is encrypted	4	2.00	--	--	0.00	--
13a	Passwords are important for EDI	1	3.00	--	--	--	--
13b	Trading partner ID and profile verification are important for EDI	1	2.00	--	--	--	--
13c	Encryption is important for EDI	1	2.00	--	--	--	--
13d	Message authentication codes are important for EDI	1	2.00	--	--	--	--
13e	Control totals are important for EDI	1	2.00	--	--	--	--
13f	Functional acknowledgements are important for EDI	1	2.00	--	--	--	--

Table 6.22 (continued)

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
13g	Application acknowledgements are important for EDI	1	2.00	--	--	--	--
14	Network totally prevent contamination through viruses	4	2.75	1.23	4.27	0.96	0.85
15	All application programs are fully protected not to run if infected	4	3.00	1.70	4.30	0.82	0.00
16	Network disable and control autoexec.bat and config.sys files	4	2.50	0.91	4.09	1.00	2.00
17	Network operation is tightly coupled to login routine	4	3.00	1.70	4.30	0.82	0.00
18	Login only from specified workstations	4	2.00	--	--	0.00	--
19	The user is the only person who can change the password	4	2.50	0.91	4.09	1.00	-2.00
20	Login name and password are encrypted	4	2.50	1.58	3.42	0.58	0.00
21	Start-up script is imposed	4	2.25	1.45	3.05	0.50	2.00
22	Start-up script is only modifiable by the system director	4	2.75	1.95	3.55	0.50	-2.00
23	Each user has a totally private work area	4	2.50	0.91	4.09	1.00	-2.00
24	File space can be fully restricted	4	3.00	--	--	0.00	--
25	All users can send files but cannot read other files	4	2.75	1.95	3.55	0.50	-2.00
26	User are denied ability to run any program on network	4	1.75	0.95	2.55	0.50	-2.00
27	Each network node is protected by physical access control	4	1.50	0.58	2.42	0.58	0.00
28	Cable routing is routinely inspected	4	2.25	0.73	3.77	0.96	-0.85

Although 75% of respondents said that network security is effective (2.75), they are not confident that the network is adequately protected from attacks (2.25; 75% disagreed) or monitored (statement 10 – 2.50, 50% disagreed; statement 11 – 2.25, 75% disagreed). Transmitted information is not encrypted (2.00; 100% disagreed).

Only one respondent reacted to statements 13a-g by disagreeing. The reason why the other respondents did not answer the question is probably because Kynoch Fertilizer (Pty) Ltd is at this stage only preparing to use electronic data interchange in the future. The response can thus be ignored.

It seems as if application programs (3.00; 75% agreed) and the network (2.75; 50% agreed) are protected against viruses. However, the network does not disable or control the operation of autoexec.bat and config.sys files (2.50; 75% disagreed).

Although the network operation is tightly coupled to the login routine (3.00; 75% agreed), login of a given user is not restricted to a specified workstation (2.00; 100% disagreed). A total of 100% of the respondents disagreed that the user is the only person who can alter his or her password (2.50). Start-up scripts are not imposed (2.25; 75% disagreed), but is modifiable by the system director only (2.75; 75% agreed).

Respondents were mostly positive about statements 23 to 25 (75%, 100% and 75% agreed respectively).

6.7.2.3.3 Internet security

Because the Internet is greatly contributing to information security risks (see chapter 3), it was essential to determine the Internet security at Kynoch Fertilizer (Pty) Ltd. The results are offered in table 6.23.

Table 6.23: Internet security

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
31a	Passwords are used regularly for the Internet	4	3.00	--	--	0.00	--
31c	Firewalls are used regularly for the Internet	4	3.00	--	--	0.00	--
31d	Token-based or one-time passwords are used regularly for the Internet	4	2.75	1.95	3.55	0.50	-2.00
31b	Encryption is used regularly for the Internet	4	2.00	--	--	0.00	--
29	All internet activities are monitored constantly	4	2.75	1.95	3.55	0.50	-2.00
30	Possibility of break-in via the Internet is remote	4	2.75	1.95	3.55	0.50	-2.00

A total of 75% of respondents are positive about Internet monitoring (2.75) and the remoteness of someone breaking into the system (2.75). The control techniques used on the Internet are ranked in table 6.23 according to importance. Encryption is apparently not used as a technique (2.00; 100% disagreed).

6.7.2.3.4 Personnel controls

The usage of personnel controls at Kynoch Fertilizer (Pty) Ltd was established through statements 32 to 39. The results are displayed in the following table.

Table 6.24: Personnel controls

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
32	Responsibilities are divided	4	3.00	--	--	0.00	--
33	Departments and close associates are totally separated	4	2.75	1.95	3.55	0.50	-2.00
34	Background checks on all new employees	4	2.00	--	--	0.00	--
35	Employees who constipate a threat can be transferred or dismissed	4	2.25	1.45	3.05	0.50	2.00
36	All critical jobs are rotated	4	2.00	--	--	0.00	--
37	All personnel take security seriously	4	2.25	0.73	3.77	0.96	-0.85
38	Casual practises are common	4	2.50	0.91	4.09	1.00	-2.00
39	A "clean desk" policy is enforced	4	1.75	0.95	2.55	0.50	-2.00

It seems as if only the controls that are mentioned in statements 32 and 33 are employed (100% and 75% agreed respectively). Lacking are the controls that are mentioned in statements 34 to 39.

6.7.2.3.5 Control of sensitive programs

Sensitive programs, or programs where a programmer can by only changing program instructions misappropriate company assets and conceal the act even though adequate administrative processing controls are in place, are the topic of statements 40 to 44. Sensitive programs are the programs in the system where important internal control tests are made and have been identified as payroll, accounts payable, fixed assets, purchasing, and inventory control (see chapter 4). The reactions to the control measures regarding sensitive programs are presented in table 6.25.

Table 6.25: Sensitive programs

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
40	Separation of the maintenance responsibility is adequate	4	2.25	0.73	3.77	0.96	-0.85
41	Programs and documentation are always stored in a secure location	4	2.25	0.73	3.77	0.96	-0.85
42	Unauthorised parting and changing of sensitive programs is prevented	4	2.25	0.73	3.77	0.96	-0.85
43	Independent party reviews requests for updates	4	2.25	0.73	3.77	0.96	-0.85
44	Periodic audits of program changes are sufficient	4	2.50	1.58	3.42	0.58	0.00

Respondents were negatively inclined regarding the security of sensitive programs. In all statements, except statement 44, 25% of the respondents disagreed and 25% strongly disagreed. A total of 50% disagreed in statement 44.

6.7.2.3.6 New program and program change controls

In table 6.26 the results are given of statements testing the security of new programs and program changes.

Table 6.26: New programs and program changes

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
45	All new programs and changes are reviewed by management	4	2.75	1.95	3.55	0.50	-2.00
46	Knowledgeable person reviews new programs and changes	4	2.50	1.58	3.42	0.58	0.00
47a	All revisions are supported by written requests	4	3.00	--	--	0.00	--
47b	All requests are properly approved by management	4	3.00	--	--	0.00	--
47c	Program documentation is adequate and maintained	4	2.25	1.45	3.05	0.50	2.00
48	Procedure prevents programs from change without consent of user's department	4	2.00	--	--	0.00	--
49a	New programs are reviewed by user department management	4	2.50	1.58	3.42	0.58	0.00
49b	Data used to test programs and results are reviewed by user department management	4	2.50	1.58	3.42	0.58	0.00

Table 6.26 (continued)

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
50	A full history of changes is maintained	4	2.25	1.45	3.05	0.50	2.00
51	No new or changed program will be accepted without approvals	4	2.75	1.95	3.55	0.50	-2.00
52	Adequate controls to insure that review and approval procedures are not bypassed	4	2.50	1.58	3.42	0.58	0.00
53	All program tests and debugging are supervised	4	2.50	1.58	3.42	0.58	0.00

It seems as if the measures mentioned in statements 45, 47a-b, and 51 are employed as security measures (respectively 2.75, 3.00, and 2.75; 75%, 100% and 75% agreed). A total of 100% of respondents disagreed with statement 48 (2.00) and 75% with statements 47c and 50 (2.25). The rest of the statements are undecided (2.50; 50%).

6.7.2.3.7 Input and output controls

Input and output controls are an important part of information systems control (see chapter 4) and are checked in statements 54 to 60. The results of these statements are presented in table 6.27.

Table 6.27: Input/output controls

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
54	Adequate input controls	4	2.75	1.95	3.55	0.50	-2.00
55	Adequate output controls	4	2.75	1.95	3.55	0.50	-2.00
56	Effective controls for rejected transactions	4	3.00	--	--	0.00	--
57	Effective controls for correcting errors	4	3.00	--	--	0.00	--
58	Responsibility has been established for following up of all input errors	4	2.75	1.95	3.55	0.50	-2.00
59	Necessary action is taken on logged exceptions	4	2.75	1.95	3.55	0.50	-2.00
60	To test validation controls invalid transactions are regularly fed	4	2.75	1.95	3.55	0.50	-2.00

Respondents were quite positive about input and output controls. A total of 100% of respondents agreed with statements 56 and 57 (3.00) and 75% with 54 to 55 and 58 to 60 (2.75).

6.7.2.3.8 Tape and disk library security

As part of operational control (see chapter 4) the management of the tape and disk library was researched in statements 61 to 74. The results are depicted in table 6.28.

Table 6.28: Tape and disk library management

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
61	Tapes are stored in a special library	4	2.75	1.95	3.55	0.50	-2.00
62	Adequate alarm and sprinkler system	4	2.00	--	--	0.00	--
63	Only one person is responsible for the administration	4	2.50	1.58	3.42	0.58	0.00
64	Access restricted to authorised personnel only	4	2.75	1.95	3.55	0.50	-2.00
65	Inventory list is updated regularly	4	2.25	1.45	3.05	0.50	2.00
66	The minimum information is always included	4	2.00	--	--	0.00	--
67	There is a tape retention plan	4	2.75	1.95	3.55	0.50	-2.00
68	Confidential material is clearly identified	4	2.50	1.58	3.42	0.58	0.00
69	Strict accountability for confidential material	4	2.50	1.58	3.42	0.58	0.00
70	Old tapes and disks are always degaussed	4	2.00	--	--	0.00	--
71	Sign-out logs are strictly used	4	2.25	1.45	3.05	0.50	2.00
72a	Old master is always retained	4	2.25	1.45	3.05	0.50	2.00
72b	Tape librarian monitors old master	4	2.25	1.45	3.05	0.50	2.00
72c	Tape librarian controls entire replacement operation	4	2.75	1.95	3.55	0.50	-2.00
72d	Son-father-grandfather theory is faithfully practised	4	2.75	1.95	3.55	0.50	-2.00
73	Tape library control records are always accurate and up to date	4	2.75	1.95	3.55	0.50	-2.00
74a	Excess of maximum borrowing period is identified and resolved	4	2.25	1.45	3.05	0.50	2.00
74b	Tapes not located in periodic inventories are identified and resolved	4	2.75	1.95	3.55	0.50	-2.00
74c	Tapes authorised for release but not found are identified and resolved	4	2.00	--	--	0.00	--
74d	Tapes for which responsible person is not identified are identified and resolved.	4	2.00	--	--	0.00	--

Respondents were not very positive about the security measures implemented to control the tape and disk library. 100 percent of respondents disagreed with statements 62, 66, 70, 74c and 74d (2.00). A total of 75% of respondents disagreed with statements 65, 71, 72a-b and 74a (2.25). However, 75% were positive about the control measures mentioned in statements 61, 64, 67, 72c-d, 73 and 74b (2.75). Statements 63, 68 and 69 are undecided (2.50; 50%).

6.7.2.3.9 Computer centre security

To determine the security of the computer centre or server room operations statements 75 to 84 were put to respondents. Table 6.29 contains the results.

Table 6.29: Computer centre operations

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
75	Operating procedures are sufficiently descriptive	4	2.75	1.95	3.55	0.50	-2.00
76	Operating procedures are kept up to date	4	2.50	1.58	3.42	0.58	0.00
77	An operation log is constantly maintained	4	2.25	1.45	3.05	0.50	2.00
78	The operation log is inspected daily	4	2.00	--	--	0.00	--
79	Computer centre personnel are the only individuals allowed to operate the machines	4	3.00	--	--	0.00	--
80	Adequate safeguards are exercised to ensure only authorised persons are permitted in the computer areas	4	2.75	1.95	3.55	0.50	-2.00
81	Personnel know what to do when an unauthorised person enters	4	2.75	1.95	3.55	0.50	-2.00
82	Personnel know what to do in the event of a fire or other emergency	4	2.75	1.95	3.55	0.50	-2.00
83	All visitors are escorted	4	2.00	--	--	0.00	--
84	Centre staff are thoroughly screened before hiring	4	2.75	1.95	3.55	0.50	-2.00

From table 6.29 it is evident that only computer centre personnel are allowed to operate the servers (3.00; 100% agreed). Respondents were however somewhat less positive about the security measures mentioned in statements 75, 80-82, and 84 (2.75; 75% agreed). A total of 75% of respondents indicated that an operation log is not constantly maintained to record any significant events and actions taken (2.25), whilst 100% indicated that the operation log is not

inspected daily by management (2.00). Visitors to the computer area are not escorted (2.00; 100% disagreed). Statement 76 is undecided (2.50; 50%).

6.7.2.3.10 Fire control

Fire precautions, which forms an important part of physical security controls, were extensively checked by statements 85 to 115. The results can be found in the following table.

Table 6.30: Fire precautions

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
85	Computer centre personnel know exactly what to do when fire occurs	4	2.75	1.95	3.55	0.50	-2.00
86	All personnel know exactly what to do when fire occurs	4	2.75	1.95	3.55	0.50	-2.00
87	Clear and adequate fire instructions are posted	4	3.00	--	--	0.00	--
88	Fire alarm pull boxes and emergency power switches are clearly visible	4	3.00	--	--	0.00	--
89	There are enough fire alarm pull boxes	4	2.50	1.58	3.42	0.58	0.00
90	Computer centre personnel are regularly trained in fire fighting	4	2.50	1.58	3.42	0.58	0.00
91	All computer centre personnel have been assigned individual responsibilities	4	2.50	1.58	3.42	0.58	0.00
92	Frequent fire drills are held	4	2.50	1.58	3.42	0.58	0.00
93a	Adequate sprinklers	4	2.00	0.70	3.30	0.82	0.00
93b	Adequate carbon dioxide flooding	4	2.50	0.91	4.09	1.00	-2.00
93c	Adequate halon flooding	4	2.25	0.73	3.77	0.96	-0.85
94	All extinguishers are accessible	4	3.00	--	--	0.00	--
95	Personnel safety precautions are adequate when carbon dioxide or halon will be used	4	3.00	--	--	0.00	--
96	A "dry pipe" arrangement has been employed	4	2.50	1.58	3.42	0.58	0.00
97	Sprinkling can be pre-empted	4	2.00	--	--	0.00	--
98	Water supply is adequate	4	3.00	--	--	0.00	--
99	Fire detection system is adequate	4	3.00	--	--	0.00	--
100a	Adequate smoke detectors in ceiling	4	2.75	1.95	3.55	0.50	-2.00
100b	Adequate smoke detectors in air ducts	4	2.50	1.58	3.42	0.58	0.00

Table 6.30 (continued)

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
100c	Adequate smoke detectors under raised floor	4	2.50	1.58	3.42	0.58	0.00
101	Smoke detectors are tested sufficiently	4	2.50	1.58	3.42	0.58	0.00
102	All extinguishers are checked sufficiently	4	2.75	1.95	3.55	0.50	-2.00
103	Emergency power shutdown automatically switches of air conditioning	4	2.50	1.58	3.42	0.58	0.00
104	Adequate emergency lightning	4	2.50	1.58	3.42	0.58	0.00
105	Adequate coverage of alarm stations	4	2.75	1.95	3.55	0.50	-2.00
106	Access to centre without delay	4	2.75	1.95	3.55	0.50	-2.00
107	Smoking prohibited	4	3.00	1.70	4.30	0.82	0.00
108a	Combustible curtains and rags are avoided	4	3.25	2.45	4.05	0.50	2.00
108b	Flammable cleaning fluids are avoided	4	3.25	2.45	4.05	0.50	2.00
108c	Paper and other supplies are avoided	4	2.75	1.23	4.27	0.96	0.85
109	Cleanliness is adequate	4	3.25	2.45	4.05	0.50	2.00
110	Adjoining areas are suitably protected from fire	4	2.75	1.95	3.55	0.50	-2.00
111	Computer centre is housed in a suitable building	4	2.75	1.95	3.55	0.50	-2.00
112	Walls, doors, partitions, and floors will resist the spread of fire	4	1.75	0.95	2.55	0.50	-2.00
113	Storage media are always stored away from the computer room	4	2.75	1.95	3.55	0.50	-2.00
114	Duplicate copies of all programs and records are stored away from the computer room	4	2.50	1.58	3.42	0.58	0.00
115	Fire insurance is adequate	4	2.75	1.95	3.55	0.50	-2.00

Respondents are mostly positive about fire precautions. A total of 100% of the respondents indicated that the control measures mentioned in statements 108a-b, 109 (3.25; 75% agreed; 25% strongly agreed) and 87-88, 94-95, 98-99 (3.00; 100% agreed) are in use. 75 percent of respondents agreed with statements 107 (3.00), 85-86, 100a, 102, 105-106, 110-111, 113, 115 (2.75) and 93b (2.50).

Control measures that are not employed are 112 (1.75; 100% disagreed), 97 (2.00; 100% disagreed) and 93a (2.00; 25% strongly disagreed; 50% disagreed). A large number of

statements are undecided (50% agreed/disagreed), namely 93c (2.25), 108c (2.75), 89-92, 96, 100b-c, 101, 103-104, 114 (2.50).

6.7.2.3.11 Physical disaster controls

The goal of statements 116 to 136 was to investigate the control measures implemented to limit and prevent information losses due to other physical disasters than fire. The results of these statements are presented in table 6.31.

Table 6.31: Physical disasters

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
116	Building is structurally sound	4	2.75	1.95	3.55	0.50	-2.00
117	Building will withstand high winds, floods and earthquakes	4	3.00	--	--	0.00	--
118	Building is adequately protected against bomb attacks	4	2.50	1.58	3.42	0.58	0.00
119	Building and all equipment are correctly grounded for lightning	4	2.50	1.58	3.42	0.58	0.00
120	Overhead water and steam pipes have been eliminated	4	3.00	--	--	0.00	--
121	Excluded from basement area	4	3.00	--	--	0.00	--
122	Drainage system will take water away from the computers	4	3.00	--	--	0.00	--
123	Mob action or sabotage is not probable	4	3.00	--	--	0.00	--
124	High quality self-locking doors	4	2.00	--	--	0.00	--
125	Effective access control to building by guards	4	2.00	--	--	0.00	--
126	Effective electronic access control	4	2.00	--	--	0.00	--
127	Good liaison with local police	4	3.00	--	--	0.00	--
128	All personnel can handle telephone bomb threats	4	2.50	1.58	3.42	0.58	0.00
129	Adequate protection from power failures and "brownouts"	4	2.75	1.95	3.55	0.50	-2.00
130	Voltage is constantly monitored	4	2.50	1.58	3.42	0.58	0.00
131	Adequate protection from communication line failures	4	2.75	1.95	3.55	0.50	-2.00
132	Adequate alternate means of transmission	4	2.75	1.95	3.55	0.50	-2.00
133	Failure of main telecommunications cable will not effect alternate transmission capability	4	2.75	1.95	3.55	0.50	-2.00

Table 6.31 (continued)

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
134	All lines are monitored for noise, errors, and dropouts	4	2.50	1.58	3.42	0.58	0.00
135a	Adequate insurance against fire	4	3.00	--	--	0.00	--
135b	Adequate insurance against natural disasters	4	3.00	--	--	0.00	--
135c	Adequate insurance against water damage	4	3.00	--	--	0.00	--
135d	Adequate insurance against power failures	4	2.25	1.45	3.05	0.50	2.00
135e	Adequate insurance against fraud	4	3.00	--	--	0.00	--
135f	Adequate insurance against crime	4	2.50	1.58	3.42	0.58	0.00
135g	Adequate insurance against sabotage	4	3.00	--	--	0.00	--
135h	Adequate insurance against errors	4	2.25	1.45	3.05	0.50	2.00
136	Insurance covers all losses including data and business	4	2.25	1.45	3.05	0.50	2.00

From table 6.31 it is evident that respondents felt mostly positive about the physical disaster control measures. A total of 100% of respondents denoted that they agree with statements 117, 120-123, 127, 135a-c, 135e and 135g (3.00), whilst 75% agreed with statements 116, 129, and 131-133 (2.75). Only regarding statements 124-126 did 100% of respondents disagree (2.00). 75 percent of respondents disagreed with statements 135d, 135h, and 136 (2.25). Statements 118-119, 128, 130, 134 and 135f are undecided (2.50; 50%).

6.7.2.3.12 Documentation control

Documentation management was evaluated and the results are given in table 6.32.

Table 6.32: Documentation management

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
137	Clear written documentation standards	4	2.50	1.58	3.42	0.58	0.00
138	Documentation standards are strictly enforced	4	2.00	--	--	0.00	--

It is apparent from the above table that documentation standards are not strictly enforced before new systems are implemented or existing ones are changed (2.00; 100% disagreed). Respondents were however uncertain about the standards for written documentation (2.50; 50%).

6.7.2.3.13 Contingency plan and backup

The next few statements had as goal to establish the state of the contingency plan and backup. Table 6.33 presents the results.

Table 6.33: Contingency plan and backup procedures

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
139	Effective contingency plan	4.00	2.25	1.45	3.05	0.50	2.00
140	Clear instructions	4.00	2.25	1.45	3.05	0.50	2.00
141	Address various levels of service interruption	4.00	2.25	1.45	3.05	0.50	2.00
142	All vital records have been identified and classified	4.00	2.00	--	--	0.00	--
143	Procedures and responsibility assignments are well understood	4.00	3.00	--	--	0.00	--
144	Complete checklist of personnel to contact exists	4.00	3.00	--	--	0.00	--
145	Adequate backup facilities	4.00	3.00	--	--	0.00	--
146	Thorough recovery plan	4.00	3.00	--	--	0.00	--
147	Backup files	4.00	3.00	--	--	0.00	--
148	Effective database recovery system	4.00	3.00	--	--	0.00	--
149	Various levels of backup files	4.00	3.00	--	--	0.00	--
150	Regular test of backup	4.00	2.75	1.95	3.55	0.50	-2.00
151	Adequate provision to permit rapid recovery	4.00	3.00	--	--	0.00	--

According to the responses of respondents, most aspects of the contingency plan are in order. For instance 100% of respondents agreed with statements 143-149, 151 (3.00) and 75% with statement 150 (2.75). However, respondents were of opinion that vital records have not been identified and classified (2.00; 100% disagreed), as well as that the contingency plan is not effective, does not contain clear instructions, and does not address various levels of service interruption (2.25; 75% disagreed).

6.7.2.3.14 Physical security

In table 6.34 the results of the subsection on physical security are given.

Table 6.34: Physical security

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
152	Adequate procedures to preclude unauthorised entry	4	2.75	1.95	3.55	0.50	-2.00
153	Access controls are effectively administered	4	2.25	1.45	3.05	0.50	2.00
154	Adequate access controls in server areas	4	2.00	--	--	0.00	--
155	Adequate controls over removal of materials	4	1.75	0.95	2.55	0.50	-2.00
156	Clearly defined procedures for disposal of confidential printed materials	4	2.75	1.95	3.55	0.50	-2.00
157	Computer centre is a "restricted area"	4	2.25	0.73	3.77	0.96	-0.85
158	Adequate control system to computer centre	4	2.25	0.73	3.77	0.96	-0.85

From the above it is evident that computer users at Kynoch Fertilizer (Pty) Ltd feels that unauthorised entry by disgruntled employees are controlled adequately and that clearly defined procedures exist for the disposal of confidential printed materials (2.75; 75% agreed). Respondents disagreed with statements 155 (1.75; 75% disagreed; 25% strongly disagreed), 154 (2.00; 100% disagreed), 153 (2.25; 75% disagreed). Statements 157-158 are border cases (2.25; 50% agreed; 25% disagreed; 25% strongly disagreed).

6.7.2.3.15 Logical access security

The next two statements had as goal to determine the state of logical access security. The results are depicted in the following table.

Table 6.35: Logical access

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
159	Authorisation over all accesses and levels can be granted and revoked	4	3.00	--	--	0.00	--
160	All access violations can be identified	4	2.75	1.95	3.55	0.50	-2.00

A total of 100% of the respondents agreed that authorisation over all accesses and access levels can be granted and revoked (3.00), whilst 75% agreed that all access violations and attempted access violations can be identified and documented (2.75).

6.7.2.3.16 Computer viruses

The important information security aspect of computer viruses was addressed in statements 161 to 162. The results are presented in table 6.36.

Table 6.36: Computer viruses

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
161	Considers problem of computer viruses as serious	4	3.25	2.45	4.05	0.50	2.00
162c	Security software is important	4	3.25	2.45	4.05	0.50	2.00
162d	User controls are important	4	3.25	2.45	4.05	0.50	2.00
162f	Regular backups are important	4	3.25	2.45	4.05	0.50	2.00
162k	Disaster recovery plans are important	4	3.25	2.45	4.05	0.50	2.00
162j	Security measures for PC's are important	4	2.75	1.95	3.55	0.50	-2.00
162h	Insurance against losses is important	4	2.50	1.58	3.42	0.58	0.00
162i	Physical security measures are important	4	2.50	1.58	3.42	0.58	0.00
162g	Compliance with security policy is a criterion in performance appraisals	4	2.25	1.45	3.05	0.50	2.00
162a	A documented virus security policy is important	4	2.00	--	--	0.00	--
162b	Definition of potential losses is important	4	2.00	--	--	0.00	--
162e	Documented safe user practices are important	4	2.00	--	--	0.00	--

Respondents felt relatively strong about the statement that Kynoch Fertilizer (Pty) Ltd considers the problem of computer viruses as very serious (3.25; 75% agreed; 25% strongly agreed). Their rating of the importance of the various security measures with regard to computer viruses (statement 162) is given according to arithmetic means in table 6.36. Statements 162a-b and 162e were not regarded as important at all (2.00; 100% disagreed).

When asked if Kynoch Fertilizer (Pty) Ltd ever suffered a computer virus attack (question 163), 100% of respondents replied with a yes.

Question 164 tried to determine the consequences of the computer virus attack. The various categories were not mutually exclusive. Computer viruses mainly resulted in a loss of time and data (4 respondents), as well as the use of specialist consultants (3 respondents).

The computers that were affected by the computer virus attack were mostly microcomputers (4 respondents) and to a lesser extent the servers or mini computers (1 respondent).

When asked about the type of virus in question 166 only one respondent mentioned the CAPS virus.

6.7.2.4 Results of section E

All departmental and functional heads, supervisors, as well as business process support or information technology personnel completed section E. The goal of this section is to obtain an rating of the various aspects of information security.

6.7.2.4.1 Physical and environmental security

In the first subsection respondents were asked to rate the physical and environmental security, which is summarised in table 6.37.

Table 6.37: Physical and environmental security

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
1	Central site	15	2.87	2.51	3.22	0.64	0.10
2	Fire protection	15	2.73	2.24	3.22	0.88	-0.83
3	Power protection	15	2.80	2.43	3.17	0.68	0.26
4	Other hazard protection	15	2.87	2.67	3.06	0.35	-2.40
5	Physical access	15	2.47	2.06	2.88	0.74	1.33
6	After hours access	15	2.47	2.00	2.93	0.83	0.55
7	Remote sites	13	2.08	1.62	2.54	0.76	-0.14

The first four variables were all rated by the majority of respondents as good and very good (respectively 50%, 50%, 45.46%, and 59.09%). The last three variables were rated as poor and very poor (respectively 45.46%, 40.91%, 40.91%).

Variable four is negatively skewed (-2.40), which can be attributed to the fact that thirteen respondents (out of fifteen) rated hazard protection as good and only two rated it as poor. Variable five is positively skewed (1.33) because ten respondents evaluated physical access as poor and only three as good and two as very good.

6.7.2.4.2 Computer operations security

The security rating of computer operations are given in table 6.38.

Table 6.38: Computer operations

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
1	Server performance monitoring	15	2.93	2.68	3.19	0.46	-0.35
2	Service performance standards	15	3.00	2.79	3.21	0.38	0.00
3	Documented procedures	15	2.40	2.12	2.68	0.51	0.46
4	Operational logging	15	2.93	2.60	3.26	0.59	0.00
5	Problem logging and resolution	15	2.73	2.48	2.99	0.46	-1.18
6	Regular backups	15	2.80	2.32	3.28	0.86	-0.34
7	Training of personnel	15	2.33	1.93	2.73	0.72	-0.63

From table 6.38 it is evident that most aspects of computer operations were evaluated as good. Variables 1-2 and 4-6 were rated as good and very good (59.09%, 63.64%, 54.55%, 50%, and 45.46%). The majority of respondents rated only variables 3 and 7 as poor and very poor (40.91% and 36.36%).

Variable 5 is negatively skewed (-1.18) mainly due to the fact that eleven respondents rated problem logging as good and only four as poor.

6.7.2.4.3 Administrative security

The rating of administrative security was the goal of the next 6 variables. The results are displayed in table 6.39.

Table 6.39: Administrative security

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
1	Action plans	14	2.86	2.47	3.24	0.66	0.15
2	Co-ordination of plans	14	2.43	2.13	2.73	0.51	0.32
3	Employment and termination	14	2.57	2.27	2.87	0.51	-0.32
4	Security policies	14	2.50	2.20	2.80	0.52	0.00
5	Standards	14	2.79	2.54	3.03	0.43	-1.57
6	Unified IT control	14	2.71	2.44	2.98	0.47	-1.07

Again respondents rated most aspects as good, namely variables 1, 3, 5 and 6 (45.46%, 36.36%, 50%, and 45.46%). However, co-ordination of plans was rated as poor by 36.36% of the respondents (2.43). The aspect of security policies is undecided (2.50).

Variables 5 and 6 are both negatively skewed (respectively –1.57 and –1.07). A total of eleven respondents rated variable 5 as good and only three rated it as poor. Ten respondents rated variable 6 as good and four rated it as poor.

6.7.2.4.4 Configuration security

The following seven variables that were rated concerned configuration security and are depicted in table 6.40.

Table 6.40: Configuration security

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
1	Application software	15	3.00	--	--	0.00	--
2	Change control	15	2.87	2.58	3.15	0.52	-0.28
3	Controls over local initiatives	15	2.80	2.57	3.03	0.41	-1.67
4	Formal systems development	15	2.67	2.40	2.94	0.49	-0.79
5	Inventory	15	2.87	2.67	3.06	0.35	-2.40
6	Systems software	15	2.93	2.79	3.08	0.26	-3.87
7	Systems hardware	15	2.93	2.79	3.08	0.26	-3.87

The majority of respondents rated all seven aspects of configuration security as good and very good (68.18%, 54.55%, 54.55%, 45.46%, 59.09%, and 63.64% respectively).

Variables 3, 5, 6 and 7 are all negatively skewed. When the frequency tables are consulted it is apparent that the cause is that twelve respondents rated variable 3 as good, thirteen variable 5 and fourteen variables 6 and 7.

6.7.2.4.5 Documentation security

In the next table the results are given regarding the rating of documentation security.

Table 6.41: Documentation security

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
1	Backups	15	2.87	2.51	3.22	0.64	0.10
2	Classification schemes	15	2.53	2.12	2.94	0.74	1.07
3	Disposal of sensitive documentation	15	2.47	2.18	2.75	0.52	0.15
4	Protection of sensitive documentation	15	2.13	1.94	2.33	0.35	2.40
5	Standards	15	2.47	2.18	2.75	0.52	0.15

Respondents mostly rated documentation security as poor, except backups that 40.91% respondents rated as good and 9.09% as very good (2.87). Variables 2 and 4 are positively skewed, which can be attributed to a high "poor" count in both cases (respectively 9 and 13).

6.7.2.4.6 Data security

Data security was evaluated by putting 11 variables to the respondents. The results are presented in table 6.42.

Table 6.42: Data security

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
1	Access control software	15	2.93	2.79	3.08	0.26	-3.87
2	Access to stored data	15	2.80	2.57	3.03	0.41	-1.67
3	Classification scheme	15	2.47	2.18	2.75	0.52	0.15
4	Consistency across environments	15	2.33	2.06	2.60	0.49	0.79
5	Control of data input	15	2.60	2.32	2.88	0.51	-0.46
6	Database encryption	15	2.47	2.18	2.75	0.52	0.15
7	Data protection	15	2.80	2.57	3.03	0.41	-1.67
8	Off-site backup	15	2.33	2.06	2.60	0.49	0.79
9	Review of authorisations	13	2.54	2.22	2.85	0.52	-0.18
10	Review of exceptions	13	2.46	2.15	2.78	0.52	0.18
11	Secure distribution of output	13	2.54	2.14	2.94	0.66	-1.19

The majority of respondents rated six of the eleven variables regarding data security as good, namely 1-2, 5, 7, 9, and 11 (63.64%; 54.55%; 40.91%; 54.55%, 31.82% and 36.36% respectively). The remaining five aspects were rated as poor (2.33-2.47). Variables 1, 2, 7 and 11 are all negatively skewed. This is because fourteen respondents rated variable 1, twelve variables 2 and 7, and eight variable 11 as good.

6.7.2.4.7 Telecommunications security

The next aspect of information security that respondents were asked to rate, was telecommunications security. The results can be found in the next table.

Table 6.43: Telecommunications security

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
1	Access tables kept up to date	15	2.67	2.40	2.94	0.49	-0.79
2	Authentication of users, messages	15	2.73	2.48	2.99	0.46	-1.18
3	Control of dial-up	15	2.73	2.34	3.12	0.70	0.43
4	Encryption	15	2.60	2.32	2.88	0.51	-0.46
5	Logging of access attempts	15	2.60	2.25	2.95	0.63	-1.41
6	Password management	15	2.67	2.40	2.94	0.49	-0.79
7	Sign-on procedures	15	3.13	2.94	3.33	0.35	2.40
8	Unique user ID's	15	2.93	2.60	3.26	0.59	0.00
9	Use of access control packages	15	2.80	2.37	3.23	0.77	-0.68

Respondents reacted positively to all nine variables by mostly rating the security as good and very good (2.60-3.13). Variables 2 and 5 are negatively skewed and variable 7 is positively skewed. The frequency table shows that eleven respondents rated variable 2 and ten variable 5 as good. Thirteen respondents rated sign-on procedures as good and two as very good.

6.7.2.4.8 Microcomputer security

Microcomputer security is an important part of information security and was rated according to 8 variables, which is presented in table 6.44.

Table 6.44: Microcomputer security

Variable	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skewness
1	Audit and review	15	2.40	2.12	2.68	0.51	0.46
2	Backups	15	2.07	1.68	2.46	0.70	-0.09
3	Central policy on acquisition	15	2.80	2.49	3.11	0.56	-0.11
4	Control of application development	15	2.67	2.40	2.94	0.49	-0.79
5	Control of data	15	2.47	2.18	2.75	0.52	0.15
6	Control of proprietary software	15	2.33	1.93	2.73	0.72	-0.63
7	Encryption	15	2.20	1.89	2.51	0.56	0.11
8	Microcomputer security policy	15	2.33	1.99	2.68	0.62	-0.31

From table 6.44 it can be deducted that most respondents rated microcomputer security as poor and very poor (2.07-2.47). The only two exceptions where the majority of respondents were positive, are central acquisition policy (2.80; 45.46% good; 4.55% very good) and control of application development (2.67; 45.46% good).

6.7.2.4.9 Contingency planning

Contingency planning was addressed in the next eleven variables and the results can be found in table 6.45

Table 6.45: Contingency planning

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
1	Disaster recovery plan	15	2.53	2.25	2.82	0.52	-0.15
2	Testing of disaster recovery plan	15	2.20	1.97	2.43	0.41	1.67
3	Procedures to update plan	15	2.40	2.12	2.68	0.51	0.46
4	Plan stored off-site	15	2.53	2.25	2.82	0.52	-0.15
5	User involvement	15	2.20	1.97	2.43	0.41	1.67
6	Plan covers all environments	15	2.53	2.25	2.82	0.52	-0.15
7	Plan covers computer centre and network	15	2.53	2.25	2.82	0.52	-0.15
8	Alternative facilities or disaster recovery site	15	2.53	2.18	2.89	0.64	0.80
9	Full off-site backup	15	2.60	2.32	2.88	0.51	-0.46
10	Resilience	15	2.47	2.18	2.75	0.52	0.15
11	Continuation of work in case of a disaster	15	2.20	1.97	2.43	0.41	1.67

When the above table and the frequency distributions are studied, it is clear that the majority of respondents rated six aspects of contingency planning as poor (variables 2, 3, 5, 8, 10 and 11). Although respondents rated the other five aspects as good, it is only full off-site backup that was rated as good by 40.91% of the respondents (2.60). The other four aspects were only marginally rated as good (2.53).

Variables 2, 5 and 11 were positively skewed (1.67) mainly due to fact that in all three cases twelve respondents rated the variable as poor and only three as good.

6.7.2.4.10 Network operations security

The next subsection asked respondents to rate the information security of network operations. The results are presented in table 6.46.

Table 6.46: Network operations

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
1	Design and implementation standards	15	2.80	2.57	3.03	0.41	-1.67
2	Resilient design	15	2.60	2.32	2.88	0.51	-0.46
3	Sound documentation	15	2.40	2.12	2.68	0.51	0.46
4	Service-level monitoring	15	2.73	2.48	2.99	0.46	-1.18
5	Operations well organised	15	2.87	2.67	3.06	0.35	-2.40
6	Control of privileged functions	15	2.60	2.32	2.88	0.51	-0.46
7	Access control	13	2.62	2.31	2.92	0.51	-0.54

The majority of respondents rated all aspects of network security as good (2.60-2.87), except sound documentation that was rated by 40.91% as poor (2.40). Variables 1, 4 and 5 are negatively skewed mainly because of a very high number of respondents that rated the variable as good.

6.7.2.4.11 Support service security

The last part of section E concerned the security of the support services and the results are presented in the table below.

Table 6.47: Support service security

Varia-ble	Description	Valid N	Mean	Confid. -95%	Confid. +95%	Standard Deviation	Skew-ness
1	Non-disclosure agreements	15	2.33	1.99	2.68	0.62	-0.31
2	Supervision of support staff	15	2.60	2.32	2.88	0.51	-0.46
3	Supervision of visitors	15	2.07	1.74	2.40	0.59	0.00
4	Couriers	15	2.13	1.94	2.33	0.35	2.40
5	Photocopiers	15	2.00	--	--	0.00	--
6	Mail room (after hours)	15	2.27	1.88	2.66	0.70	-0.43

From table 6.47 and the frequency tables it can be deducted that the majority of respondents rated five of the six aspects of support service security as poor or very poor (2.00-2.33). It is only the supervision of support staff that was rated as good by 40.91% of the respondents (2.60). Variable 4 is very much positively skewed. This can be attributed to the fact that thirteen respondents rated courier security as poor and only two rated it as good.

6.7.2.4.12 Specific vulnerabilities

When asked to name specific vulnerabilities that Kynoch Fertilizer (Pty) Ltd experiences regarding information security, the following were mentioned by respondents:

- Information has not been classified to determine the appropriate level of information security for a specific type of information.
- Lack of policy and management commitment.
- Awareness of computer users is not up to standard.
- Sharing of drives at production leads to unauthorised access to data.

6.7.2.4.13 Impending threats

Respondents were also asked to respond to a question about impending threats that the organisation faces. They reacted as follows:

- Internal or external information sabotage.
- Information technology crash which cannot be recovered.

6.7.2.4.14 Risks associated with threats

The only risk associated with the threat of an information technology crash mentioned by respondents was the risk that production will be stopped.

6.7.2.4.15 Risks that can be reduced by applying security countermeasures

Respondents indicated that by applying appropriate security countermeasures both the above mentioned risks could be reduced. However, attention will also have to be paid to the overall moral of the people.

6.8 SUMMARY

Chapter 6 mainly contains the results of the empirical study done at Kynoch Fertilizer (Pty) Ltd. In the first part of the chapter attention was paid to the development and structure of the three questionnaires. Because an objective of the study is to determine the overall state of information security at Kynoch Fertilizer (Pty) Ltd, the population was identified as all computer users. After a thorough literature study, preliminary questionnaires were designed and tested by means of a pilot study. Afterwards the three final questionnaires were designed. The first questionnaire was aimed at general computer users and consisted of two sections. The second questionnaire was aimed at functional and departmental heads and contained three sections. The last questionnaire contained four sections and was aimed at the business process support or information technology personnel. Except for a few open questions a four point Likert scale was used.

In the second part of the chapter the process of data collection, response rate and results were discussed. Data was collected by means of questionnaires that were distributed and collected by hand. The overall response rate was 46.28%.

The results of the three questionnaires were processed statistically. Frequency tables were drawn up, arithmetic means, 95% confidence levels, standard deviations and skewness were calculated. The results were then presented in tables and graphs according to the five sections of the questionnaires. Every table and graph was shortly discussed to point out certain tendencies in the results.

The next chapter will provide certain conclusions and recommendations based on these results of the empirical study.

CHAPTER 7

CONCLUSIONS AND RECOMMENDATIONS

7.1 INTRODUCTION

In this last chapter the study as a whole is concluded and summarised. The problem being researched is shortly discussed, as well as the purpose and method of the research. The most important findings of the literature study, as well as an interpretation of the results of the empirical study are indicated. The chapter is concluded with conclusions and recommendations regarding a practical and feasible information security framework and plan.

The conclusions and recommendations, which is an important part of this chapter, will be structured as follows:

- Conclusions arrived at as a result of the analyses of the biographical and demographical data.
- Conclusions with regard to statements and questions where respondents indicated information security problems and issues.
- Recommendations for an overall information security framework and plan for Kynoch Fertilizer (Pty) Ltd.

Although an immense amount of work was done in the literature and empirical study, only the core and the most important aspects of information security will be discussed in this chapter in order to realise the objectives of the study.

7.2 PROBLEM RESEARCHED

The misuse of information technology and security risks are increasing faster than the deployment of information technology. The increased dependence on computer technology and systems therefore escalated the requirements for information security. Unfortunately there often is apathy towards information security by management, which leads to an ad hoc approach to information security and a serious lack of budget to implement the necessary countermeasures

for the safeguarding of the valuable information resource. This approach quite frequently leads to major information and financial losses (chapter 1).

7.3 PURPOSE OF THE STUDY

The main objective of the study thus was to determine the current state of information security at Kynoch Fertilizer (Pty) Ltd and to provide practical and feasible managerial recommendations for a multilevel information security plan that will withstand the current and future information security threats (chapters 1 and 2).

7.4 METHOD

7.4.1 LITERATURE STUDY

To establish a sound theoretical background a literature study was made of three major aspects of information security and control.

7.4.1.1 Information security risks, threats, vulnerabilities and problems

Chapter 3 pointed out that computer crime and fraud will become more sophisticated and popular as the use of information technology escalates over the years to come. As the number of computer applications, processing and hardware increases, the three primary risks of integrity, confidentiality and availability also increases.

The major information security threats that were discussed in chapter 3 are summarised in table 7.1.

Table 7.1: Possible information security threats

MODE	*TYPE*
External	
Visual spying	Observing of keystrokes or screens
Misrepresentation	Deceiving operators and users
Physical scavenging	Dumpster-diving for printout
Hardware misuse	
Logical scavenging	Examining discarded or stolen media
Eavesdropping and wiretapping	Intercepting electronic or other data
Interference	Jamming, electronic or otherwise
Physical attack	Damaging or modifying equipment, power
Physical removal	Removing equipment and storage media
Masquerading	
Impersonation	Using false identities external to computer systems Unauthorised use of access codes and passwords
Piggybacking attacks	Usurping communication lines, workstations
Spoofing attacks	Using playback, creating bogus nodes and systems
Network weaving	Masking physical whereabouts or routing
Pest programs (setting up opportunities for further misuse)	
Trojan horse attacks	Implanting malicious code Sending letter bombs
Logic bombs	Setting time or event bombs (a form of Trojan horse)
Malevolent worms	Acquiring distributed resources
Virus attacks	Sections of code attaching to programs and replicating
Bypasses (avoiding authentication and authority)	
Trapdoor attacks	Utilising existing flaws
Authorisation attacks	Password cracking Hacking tokens
Superzapping	Using a systems program that can bypass regular systems controls to perform unauthorised acts

Table 7.1 (continued)

MODE	*TYPE*
Active misuse (writing, using, with apparent authorisation)	
Basic active misuse (data diddling)	Creating, modifying, using, denying service Entering false or misleading data
Incremental attacks	Using salami attacks
Denials of service	Perpetrating saturation attacks
Passive misuse (reading, with apparent authorisation)	
Browsing	Making random or selective searches
Inference, aggregation	Exploiting database inferences and traffic analysis
Covert channels	Exploiting covert channels or other data leakage
Inactive misuse	
Personnel incooperation	Wilfully failing to perform expected duties, or committing errors of omission
Indirect misuse	
Fraud, hacking	Preparing for subsequent misuses, as in offline preencryptive matching, factoring large numbers to obtain private keys, autodialer scanning

It is of the utmost importance that the vulnerabilities in the information security system, the threats and the resultant risks of an organisation be identified and protected against.

7.4.1.2 Solutions and countermeasures to prevent and limit the impact of these threats and vulnerabilities

Although it is not possible to build a completely secure information system and to eliminate all threats and problems discussed in chapter 3, it is possible to minimise the impact and business disruption by implementing various control measures. The major control measures discussed in chapter four are summarised in table 7.2 below.

Table 7.2: Summary of information security controls and roles

INFORMATION SECURITY CONTROLS	
TYPE OF CONTROL	**PRINCIPAL ROLES**
Administrative	◆ Published formal control policies, procedures, and guidelines ◆ Personnel controls ◆ Screening and supervision of personnel ◆ Monitoring of employees in key positions ◆ Promotion of information security awareness amongst all relevant personnel ◆ Training programs ◆ Separation of duties and functions in job design ◆ Security inducive environment
Physical	◆ Physical security • Concentric boundaries • Physical access control ◆ Environmental control ◆ Hardware controls ◆ Software controls • Operating systems controls • Program security controls ◆ Networking security ◆ Communications security ◆ Protection against natural disasters ◆ Emergency power supply ◆ Radiation shielding
Procedural	◆ Logical access control • User identification • User authentication • User authorisation - on the level where the minimum benefit can be obtained ◆ Data control – critical record and field identification and classification program

Table 7.2 (continued)

TYPE OF CONTROL	PRINCIPAL ROLES
Operational	◆ Control over operations personnel ◆ Control over equipment maintenance ◆ Control over the use of utility programs ◆ Control over archival storage ◆ Amendment control ◆ Maintenance of computer backup tapes and software libraries ◆ Recovery procedures
Information systems	◆ Origin of data ◆ Input and capturing • Accuracy of data • Completeness of input • Validation of input • Input authorisation • Efficient handling of data rejections and recapturing methods by application systems • Control over application system interfaces ◆ Data conversion ◆ Edit checks ◆ Processing • Hardware - error detection circuitry; protection measures implemented as hardware mechanisms; fault-tolerant computer systems • Software - operating systems and DBMS security measures • Run control totals • Computer matching ◆ Output ◆ Storage and extraction • Database security • Backup and recovery • File handling • Access authorisation ◆ Communications - encryption

Table 7.2 (continued)

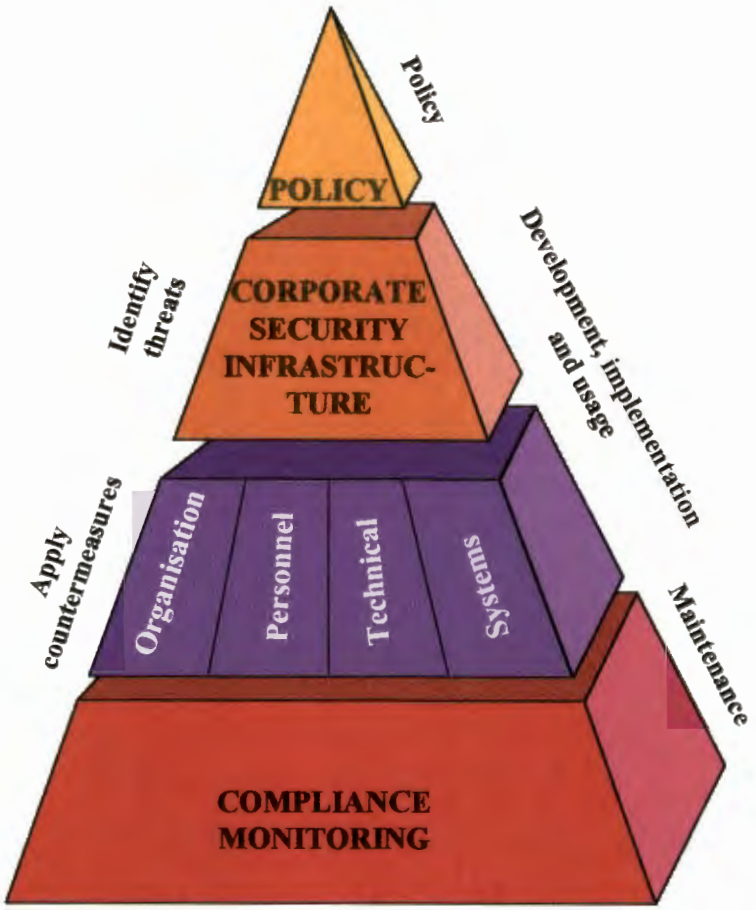
TYPE OF CONTROL	PRINCIPAL ROLES
Implementation Systems development	❖ Auditing of the systems development process to ensure systems controls and auditability ❖ Post-implementation audit ❖ Ensuring that only authorised maintenance is performed ❖ Documentation audits ❖ Centralising of change control (documentation and programs) ❖ Evaluation of user contentment
Controls of last resort	❖ Disaster recovery plan • Emergency plan • Backup plan • Recovery plan • Test plan ❖ Insurance

7.4.1.3 The management of information security and control

To be successful it is necessary that the information security controls discussed in chapter 4 be managed properly. Chapter 5 therefore concentrated on the management aspects of responsibility; security policy, objectives, standards and guidelines; security requirements; a control strategy; an information security control framework; an information security management model; and the optimum level of security with regard to cost, vulnerability, and accessibility.

The management of information security is summarised in figure 7.1:

Figure 7.1: Information security management



Adapted from Von Solms (1993:52)

The responsibility for information security rests with senior management, who may appoint an information security manager to manage the security function. The management process begins with the formulation of a corporate information security policy and a thorough audit of the corporate information security infrastructure. The audit includes an analysis of the confidentiality and criticality of computer resources, an assessment of all the various information security threats, risks and vulnerabilities, as well as an investigation of the available countermeasures, safeguards and controls.

Once the audit is completed, a budget for information security and an information security plan is submitted for approval by management. After management approval the necessary organisational, personnel, technical, systems and other countermeasures and safeguards are implemented. To determine the effectiveness of the control measures and to enforce the

implemented safeguards the security manager and his personnel do continuous monitoring, and if necessary maintenance work to ensure the required level of information security.

7.4.2 EMPIRICAL STUDY

The empirical field investigation was done at the central region of Kynoch Fertilizer (Pty) Ltd, a large fertiliser manufacturer in Potchefstroom. The central region of Kynoch Fertilizer (Pty) Ltd currently has a market share of approximately 37% and had a turnover of R761 267 million and a trading profit of R48 045 million in 1997. The company makes extensive use of computerised information, local and wide area networks, which increases the threats and risks to information security (chapter 2).

The empirical research was done by means of a field study of which three structured questionnaires on information security were an important component. The objective of the field study was to determine the state of information security at the central region of Kynoch Fertilizer (Pty) Ltd.

The theoretical knowledge gained from the literature study (chapter 3 to 5) was used to develop three preliminary questionnaires, which were tested by means of a pilot study. Afterwards the three final questionnaires aimed at general computer users, functional and departmental heads, and the business process support or information technology personnel, were designed.

The questionnaires were distributed and collected by hand with an overall response rate of 46.28%. The results of the three questionnaires were processed statistically. Frequency tables were drawn up, arithmetic means, 95% confidence levels, standard deviations, skewness and correlations were calculated and presented in tables and graphs in chapter 6.

7.5 RESULTS AND CONCLUSIONS

Based on the theory concerning the ideal information security and control situation (chapters 3 to 5) and the empirical results (chapter 6), it is now possible to determine the gap, problem areas and issues of information security and control at Kynoch Fertilizer (Pty) Ltd. This gap can be used to provide the company with a conceptual framework and recommendations for information security and control in a manufacturing organisation.

7.5.1 BIOGRAPHICAL AND DEMOGRAPHICAL INFORMATION: SECTION A

The biographical data of the total number of respondents was analysed by means of correlation analysis. From the correlation analysis of the biographical data it became evident that the following positive and negative correlations with a 95% level of confidence exist.

Positive correlations:

- As expected there is a positive correlation between the age of employees and the years of service (.43). Older employees have been longer in the service of Kynoch Fertilizers (Pty) Ltd.
- Gender and position in the company (.43). Male employees occupy the more senior positions. All eighteen respondents, who indicated that they are a functional or departmental head, or supervisor, were male.
- Educational level and level of computer experience (.38). The higher the educational level of employees, the higher is the level of computer experience.

Negative correlations:

- Level of computer experience and length of service (-.33). As can be expected, the older employees have less computer experience.
- Educational level and gender (-.39). The educational level of female employees is lower than that of their male counterparts.
- Educational level and age of employees (-.27). Younger employees are academically better qualified than the older employees.

7.5.2 SECURITY PROBLEMS AT KYNOCH: SECTIONS B, C, D AND E

From the results in chapter 6 quite a few problem areas and issues of information security at Kynoch Fertilizer (Pty) Ltd came to light. The problem areas and issues will be presented according to the various aspects of information security as were discussed in chapters 3 to 5.

The results of section D were treated with the utmost care because it consisted of only four (out of a possible five) responses. Therefore final conclusions were only made where 100% (all four) of the respondents agreed.

7.5.2.1 Management of information security

Although it seems that information management is important to senior management and that they accept their responsibility, it became evident that top management does not view the vulnerability of this strategic asset as a critical performance area. The result is that neither enough attention is paid to this problem, nor enough funds allocated to do the job (6.7.2.2.2). Quite a few management aspects therefore need attention.

7.5.2.1.1 Provision of funds for information security

A major obstacle to information security being addressed at Kynoch Fertilizer (Pty) Ltd is the lack of budget (6.7.2.2.2). The budget is the formalisation of the monetary implications of the business plans. The budget of Kynoch (Pty) Ltd therefore reflects the relative lack of concern for information security. Despite the high physical asset value of the computer systems, the budget has no specific item referring to information security (Jacobs, 1998).

7.5.2.1.2 Security planning

Another major obstacle to information security at Kynoch Fertilizer (Pty) Ltd is the fact that security planning do not form part of the total strategic and business planning. In fact there is a lack of a total information security plan on strategic level (6.7.2.2.7).

Information security strategies also need to be more effective and aligned with business strategies. The effectiveness of the security administration need to be addressed (6.7.2.2.2).

7.5.2.1.3 Assignment of specific responsibility

At present the business process support manager is responsible for information security, but because of an overload of work cannot pay justice to this very important task. The top management has not yet deemed it necessary to have a specialist information security manager to meet its needs in the information field. Although the business process support manager has

created a personnel structure under him, no specific person has been assigned the task of information security (Smith, 1998).

7.5.2.1.4 Assessment of organisational vulnerabilities, threats and risks

Neither the management nor the business process manager has any formal assessment of vulnerabilities, threats and associated risks to which the information resource is exposed. Until now little thought has been given to vulnerabilities such as fraud, theft, sabotage, espionage and other information security problems (Jacobs, 1998).

7.5.2.1.5 Investigation of information security countermeasures

No active investigation of available and new countermeasures takes place at Kynoch Fertilizer (Pty) Ltd. A formal record of information security countermeasures could not be found (Jacobs, 1998).

7.5.2.1.6 Risk management strategy

As a result of not having a formal assessment of vulnerabilities, threats and countermeasures, a formal risk management strategy to reduce the information security problem, does not exist. Risk management is often done on an ad hoc basis or as a result of some incident (Jacobs, 1998).

7.5.1.2.7 Implementation of countermeasures

Because of the lack of a well-defined risk management strategy and plan, there are no specific plans laid down to implement information security countermeasures. Countermeasures are often implemented when a person or incident requires some defensive attention to be given to a specific problem area (Jacobs, 1998).

7.5.2.1.8 Monitoring and reviewing information security effectiveness

The security management function does no specific monitoring of its own accord in the area of information security. No regular audits of information security exist (Jacobs, 1998). The disaster recovery plan is never tested (6.7.2.4.9).

7.5.2.2 Administrative security

7.5.2.2.1 Information security awareness

Security standards are not communicated enough. Regular updates and reminders on information are necessary to keep employees informed. Training of new employees in information security is almost non existent and should be addressed urgently (6.7.2.2.1).

7.5.2.2.2 Information security policy

No formal information security document could be located. Documentation on security matters does not really exist and are mostly left to the initiative and competence of employees. Formulated information security objectives or action plans could also not be traced (6.7.2.4.3).

7.5.2.2.3 Personnel controls

The dividing of responsibilities is implemented as a control measure. Attention should be paid to background checks on all new employees, rotation of critical jobs, and the enforcement of a clean desk policy (6.7.2.3.4).

7.5.2.2.4 Security conscious environment

The general perception at Kynoch is that stringent security measures operate. This perception does not, however, hold true for information security. The overall environment is all but information security conscious (Smith, 1998).

7.5.2.3 Physical security

Although the general perception is that physical security is of a high standard (6.7.2.2.9), this is however not exactly true as is evident from the following shortcomings.

7.5.2.3.1 Server room security

The operations log that records any significant events and actions is not inspected daily by management. A dangerous practise is that visitors to the computer area are not escorted (6.7.2.3.9). The level of physical access security, after hour access control and control of the removal of materials from the server area are not adequate and need attention (6.7.2.3.14 and

6.7.2.4.1). Access control, however, begins with access control to the building by the security guards and electronic access control, which both needs improvement (6.7.2.3.11).

7.5.2.3.2 Software security

Computer viruses remain an imminent threat and were widely experienced by employees and mostly affected microcomputers and to a lesser extent also the servers. Although several control measures are being used, a documented virus security policy, a definition of potential losses and documented safe user practices do not exist. The major consequences of the computer virus attacks were a loss of time, functionality and data. Macro viruses were the type mostly encountered. Virus protection, especially on microcomputers, will have to be improved dramatically (6.7.2.2.12 and 6.7.2.3.16).

7.5.2.3.3 Remote site security

The level of security of remote sites is not adequate and need attention (6.7.2.4.1).

7.5.2.4 Procedural security

7.5.2.4.1 Logical access security

Although authorisation controls are effective (6.7.2.3.15), many computers are left on when unattended and employees do not log off from the network when leaving the micro for more than fifteen minutes. This minimises the value of access control (6.7.2.2.10).

Although passwords are unique it should be changed more regularly (6.7.2.2.10).

7.5.2.4.2 Data security

There is no specific person who reviews new or existing data in terms of classifying it for storage and filing purposes or for the dissemination to potential users. Most of the information is available to all persons. There are a number of informal procedures, which do operate to limit personnel's access to certain confidential information (Smith, 1998). The classification of data, consistency across environments, database encryption, off-site backup, and the review of exceptions thus need urgent attention (6.7.2.4.6).

7.5.2.5 Operational security

Although most computer users viewed operations and maintenance security as of a high standard (6.7.2.2.12), quite a few aspects need to be corrected.

7.5.2.5.1 Maintenance security

Although mostly in order, procedures are not documented adequately, neither is enough being done about the training of personnel regarding emergencies (6.7.2.4.2).

7.5.2.5.2 Tape and disk library security

The management of the tape and disk library is not up to standards. The alarm and sprinkler system should be thoroughly revised. Degaussing of old tapes and disks should be implemented. Tapes authorised for release but not found, and tapes for which the responsible person is not identified, should be identified and resolved (6.7.2.3.8).

7.5.2.5.3 Support service security

The security of support services is an aspect of information security that was assessed very low. Non-disclosure agreements are not used. Maintenance visitors are not supervised. The security regarding couriers, photocopiers and the mailroom (especially after hours) are of a very low standard (6.7.2.4.11).

7.5.2.6 Information system security

7.5.2.6.1 Security of sensitive programs

Although negatively evaluated, nothing can be concluded with certainty regarding the security of sensitive programs like the payroll, accounts payable, fixed assets, purchasing, and inventory control. These aspects probably need attention (6.7.2.3.5).

7.5.2.6.2 Input/output security

Effective controls for point of origin review of the rejected sensitive transactions and the correcting of errors in input/output at the point of origin have been established, but will need regular auditing (6.7.2.3.7).

7.5.2.6.3 Storage security

There is no formal review of existing systems on a regular basis to determine whether redundant information is being kept (Smith, 1998).

7.5.2.6.4 Telecommunications security

Telecommunications security is adequate, except that encryption is not always used (6.7.2.4.7).

7.5.2.7 Implementation or systems development security

Information systems development and documentation security is basically on an acceptable standard (6.7.2.2.11 and 6.7.2.4.4), but a few aspects will have to be addressed by management.

7.5.2.7.1 Security of new programs and program changes

Although all revisions are supported by written requests that need to be approved by management, procedures that prevent programs from being changed without consent of the user's department do not exist and should be implemented (6.7.2.3.6).

7.5.2.7.2 Documentation

Documentation security is poor (6.7.2.4.5). Documentation standards are not strictly enforced before new systems are implemented or existing ones are changed (6.7.2.3.12). Classification schemes, disposal of sensitive documentation, protection of sensitive documentation and general standards need to be addressed (6.7.2.4.5).

7.5.2.8 Contingency planning and disaster recovery

7.5.2.8.1 Contingency plan and backup

Another aspect that was rated very negatively is contingency planning. Although some aspects of the contingency plan are in order, vital records have not been identified and classified, which makes the orderly removal of important records impossible. Another alarming aspect is that the disaster recovery plan is not regularly tested, neither are there procedures to regularly update the plan. Overall user involvement, without which the successful implementation of a disaster recovery plan is almost impossible, is lacking. Alternative facilities or a disaster recovery site do

not exist, with the result that resilience is very low and continuation of work in case of a disaster will be very unlikely (6.7.2.3.13 and 6.7.2.4.9).

7.5.2.8.2 Natural disaster security

Several precautions have been taken. Aspects that still need to be addressed are the fact that the walls, doors, partitions and floors of the server room will probably not withstand the spread of a fire, and that the sprinkling system cannot be pre-empted while personnel extinguish the fire manually to prevent machine damage (6.7.2.3.10).

High quality self-locking doors with "panic bars" on the inside at the server room are lacking. Access control to the building by the guards and electronic access control to the building need improvement because of the possibility of mob attacks (6.7.2.3.11).

7.5.2.9 Microcomputer security

Microcomputer security is one aspect that seriously needs attention. No regular audit and review or a microcomputer security policy exists. Neither are backups, control of data, control of proprietary software, or encryption on an adequate level (6.7.2.4.8). When backups on microcomputers are made, version numbers and creation dates are not recorded (6.7.2.2.8).

7.5.2.10 Network security

Although network security is perceived to be effective, serious shortcomings are that transmitted information is not encrypted, logins are not restricted to a specified workstation, and the change of passwords is not restricted to the user only (6.7.2.3.2). Another aspect that should be addressed is sound documentation, which at the moment is lacking (6.7.2.4.10).

7.5.2.11 Internet security

Internet security seems to be adequate. Passwords and firewalls are used as control techniques. Encryption is not used and should be considered (6.7.2.3.3).

7.5.2.12 Overall state of information security

Overall security of the computer systems are quite good, except that of desktop or microcomputers, remote computing and laptops, which certainly should receive urgent attention (6.7.2.2.3).

7.5.2.12.1 Planned incident response and response team

Kynoch Fertilizer (Pty) Ltd does not have an effective planned incident response or response team when an intruder is detected in the computer network (6.7.2.2.3). Consideration should be given to the establishing of a detailed incident response plan and a small response team.

7.5.2.12.2 Information security risks

The increase in information security risks over the past three years was much greater than the increase in computing resources, mainly due to the implementation of client/server technology, increase in personal computers, and an increase in the amount of information handled (6.7.2.2.4). Therefore information security deserves more attention in the future.

7.5.2.12.3 Information security concerns and threats

Information security concerns that will have to be addressed are end-user computing awareness, network security, distributed computing security, and multiple logons and passwords. The major threats of unauthorised disclosure of information are coming from computer "terrorists" and employees who do not need to know (6.7.2.2.5).

7.5.2.12.4 General information security measures

General information security measures, which are regularly used, are virus detection software, secure modems and firewalls, and network access control software. Attention will have to be paid to token-based passwords, personal computer access controls, personal computer hardware security devices, terminal key locks, lock words, redundant communication, business continuity planning software and security evaluation software.

It also became apparent that single sign-on software, signature verification, telecommunications, biometrics, message authentication are never used and should be investigated as a means of

protection. Although non-disclosure agreements by personnel are not regarded as important, it deserves attention (6.7.2.3.1).

7.5.2.12.5 Information or financial losses

Information and financial losses were rarely experienced. The major threats are however coming from malicious acts from outside and from employees, viruses, inadvertent errors by insiders and outsiders, and industrial espionage. The major reasons for information losses experienced by Kynoch Fertilizer (Pty) Ltd are software errors and computer failures (6.7.2.2.6). Although information and financial losses were rarely experienced, top management will have to urgently address these threats, as well as the reasons for information and financial losses, to prevent future losses.

7.5.3 SUMMARY

A lack of security was thus found in all three basic aspects of security, and will shortly be listed below.

7.5.3.1 Confidentiality and integrity concerns

- Passwords are not changed regularly.
- Sensitive information is not treated any differently from routine information.
- Communications are not adequately protected from intrusion.
- Dial-in security is not controlled effectively.
- Change control, version control, and problem management is not disciplined adequately.
- Program development is usually insufficiently tested and does not include rigorous data verification and validation techniques.

7.5.3.2 Availability concerns

- Information is not backed up regularly and effectively.

- Physical support services including electricity, environmental monitoring, fire and water detection and protection, physical access, air conditioning, maintenance, and the like are often missing or not up to standards.
- Virus control standards are undisciplined, especially on microcomputers.
- Asset control is almost non-existent, resulting in very poor knowledge concerning the performance of equipment, the maintenance record, and sometimes just who has responsibility for the safety of the equipment.

7.6 RECOMMENDATIONS

To remain competitive in the fertiliser market Kynoch Fertilizer (Pty) Ltd will have to implement an information security framework and plan. Eventually this plan will have to be translated into detailed action plans with appointed responsible persons at all strategic business units. Detailed action plans, however, falls without the scope of this study.

The framework and plan is based on the literature study of chapters 3 to 5 and has as goal to fill the gap between the ideal information security situation and the present information security situation at Kynoch Fertilizer (Pty) Ltd as determined by the empirical study (chapter 6).

7.6.1 AN INFORMATION SECURITY FRAMEWORK

The development of a managerial framework for information security focuses on two broad areas, namely top management functions and a multilevel information security plan.

7.6.1.1 Top management functions

An information security program must have top management involvement to be successful. It must form part the strategic objectives and business plan of Kynoch Fertilizer (Pty) Ltd. It is their task to install into their organisation a defensive threshold, which is high enough to make the investment in time and effort unprofitable to any potential adversary. Top management effects their involvement by defining policy objectives and by making resources available for the continual upkeep of information security and control.

Top management should therefore attend to and control the following aspects of information security:

7.6.1.1.1 Security policy

The initial step to effect a policy at Kynoch Fertilizer (Pty) Ltd is to have it defined, recorded and communicated throughout the organisation. The requirements for information security and control should be clearly defined. Policies should also spell out the consequences of violating security procedures. The objectives and sub-objectives should commensurate with the carefully evaluated threat exposure and risk analysis and should be quantified wherever possible. Standards and procedures should be clearly stated.

The formulation of policy is not a once-off exercise and should be reviewed constantly in order to ensure that it is still appropriate to the ever-changing security environment.

Policies that need to be considered are:

- A security policy that includes aspects of strategic nature, as well as the long term impact and implications.
- An insurance policy that involves the management of asset and resource risk in order to ensure the survival and effective functioning of the organisation.
- A policy regarding the organisation structure, which comprises personnel practise, as well as the structure within which the computer environment is organised.
- A contingency and disaster recovery policy.
- A systems development policy that describes the methodology to successfully develop application systems.
- A maintenance policy.

7.6.1.1.2 The allocation of specific responsibilities

To accomplish policy objectives usually requires that an individual be formally appointed by Kynoch Fertilizer (Pty) Ltd to be functionally responsible to top management. If the functional responsibility is for the total organisation's information security, it is imperative that the person will form part of the top management team, and that an organisation structure will be developed below him to carry out specialised tasks. Because information security management is highly

dynamic and specific, it would seem natural that a specialist manager or subordinate should be employed for information security management.

This appointed person should oversee the following aspects of information security:

- Information security assurance – informing senior management of Kynoch Fertilizer (Pty) Ltd about the quality, robustness and reliability of existing information security capabilities.
- Security condition – making sure the functions that influence information security perform as an integrated process.
- Incident evaluation – evaluating and accounting for every case in which information security is compromised or suspected of being compromised.

7.6.1.1.3 Funding of information security

To implement a risk management strategy and effective information security controls, it is necessary that top management will have to budget for adequate funding to implement its security strategy and objectives. It has been stated in chapter one that although information is a valuable asset, very few organisations have taken commitment to information security in the respect of budgeting. Few organisations have a specific budget category for information security. An indicator of top management's commitment to information security is to determine the proportion of the total budget that has been allocated to this strategic asset. It is absolutely imperative that top management at Kynoch Fertilizer (Pty) Ltd should bear in mind the value of their information asset and what can be lost if adequate information security is not employed. In the establishment of a defensive threshold to deter potential adversaries, cost and benefits will have to be traded off against one another.

7.6.1.1.4 Monitoring and reviewing information security effectiveness

It is the responsibility of top management at Kynoch Fertilizer (Pty) Ltd to ensure that the delegated task of information security management meets the policy objectives. Top management should therefore closely monitor and audit the security program of the organisation by means of the information technology manager or an independent committee.

7.6.1.2 Security management function

Once top management has created a broad framework within which information security management can take place, the delegated functionally responsible manager must implement the actual security management functions. It must, however, be borne in mind that the ultimate responsibility for security and privacy management remains with the top management of Kynoch Fertilizer (Pty) Ltd. Within the conducive environment created by the top management, the security management function should act to initiate and control the following aspects:

7.6.1.2.1 Structuring for information security

The functionally responsible manager should determine an appropriate organisation structure which will permit him to function effectively, including areas to be controlled, specialist staff to be employed, and qualifications required to effectively enforce the information security program of the organisation.

Associated with the above is the requirement to establish individual accountability. It is important for the functional manager to ensure that tasks, which are delegated, are communicated in such a way that they are clearly understood and accepted.

7.6.1.2.2 Systems review

Computer systems and information security at Kynoch Fertilizer (Pty) Ltd should be continually reviewed in the light of the continuous advancement of computer technology and the misuse of computer technology. The mission, strategy and profile of the computer environment (data and information, management information systems, computer technology and application software, as well as personnel) should also be investigated.

A valuable tool to review and test the security of present computer systems is a virtual reality simulator that simulates security breaks. The virtual simulation highlights the effect of an attack on a site, as well as possible routes into buildings and installations. It thus identifies weaknesses and indicates ways in which countermeasures might reduce the damage and increase the chances of detecting and catching a criminal.

7.6.1.2.3 Data evaluation and classification

The more data and information is handled by a computer system, the greater is the vulnerability to physical en personal security threats. It is therefore essential for the security function in an organisation to control the storage, processing and dissemination of corporate information. Probably someone from the business process support department can be appointed to evaluate existing and new data requirements and then to classify the data as personal, strategically critical or for general use. He or she will also sanction its collection and authorise its use.

7.6.1.2.4 Assessment of organisational vulnerabilities, threats and risks

It is important for Kynoch Fertilizer (Pty) Ltd to periodically evaluate its vulnerability to internal and external information security threats. The vulnerabilities and threats that potentially face an organisation were discussed in chapter 3. Attention should be paid to environmental threats, hardware, software and liveware problems and failures, fraud and theft, sabotage and industrial espionage.

Good use can be made of available programs to scan the network for security problems, flaws and vulnerabilities.

7.6.1.2.5 Monitoring of information security countermeasures

The rate of change in computer technology, as well as continuous transformation in the security countermeasure field, requires that these aspects should be monitored on a regular basis in order to keep the organisation up to date with the most modern and suitable options available to them. Countermeasures should also be evaluated on a regular basis for their effectiveness. Countermeasures have been discussed in chapter 4.

7.6.1.2.6 Risk management strategy

On the basis of the threat assessment and the most recent countermeasures, a risk strategy for Kynoch Fertilizer (Pty) Ltd needs to be formulated that takes the security and cost relationship, the security and vulnerability relationship, the security and accessibility relationship (see 5.11.3 in chapter 5), as well as effectiveness, into account to arrive at the optimum level of security (see 5.11.4 in chapter 5). Usually the end result will lead to a gap analysis, which identifies the differences between present and future objectives.

Risk management is an orderly process that analyses and manages the security risks in a computer system. The basic steps usually are:

- Identify and evaluate assets and potential areas of concern, namely hardware, software, data, people, documentation, privacy, policies, backup facilities, record retention, access control, audit trails, segregation of duties, reliability, and supplies.
- Determine the vulnerabilities of the assets by specifically considering the effects of natural disasters, outsiders, malicious insiders and unintentional errors on secrecy, integrity and availability.
- Estimate the likelihood of exploitation by using observed data of the general population or observed data for a specific system.
- Calculate the expected annual loss.
- Examine applicable controls and their costs, for example cryptographic controls; secure protocols; program development controls; program execution environment controls; operating system protection features; identification; authentication; secure operating system design and implementation; database access controls; database reliability controls; database inference controls; multilevel security controls for data, data bases, and operating systems; personal computer controls (procedural, physical, hardware, and software); network access controls; network integrity controls; controls on telecommunications media; physical controls; and physical security devices.
- Project annual savings from the implementing of new controls.

7.6.1.2.7 Implementation of countermeasures

After the establishment of strategies, it is necessary for successful implementation of the countermeasures. The best way of doing this is by assigning the task to specific individuals, who will determine priorities, assess impacts on the existing set-up, determine resources required and manage the various projects.

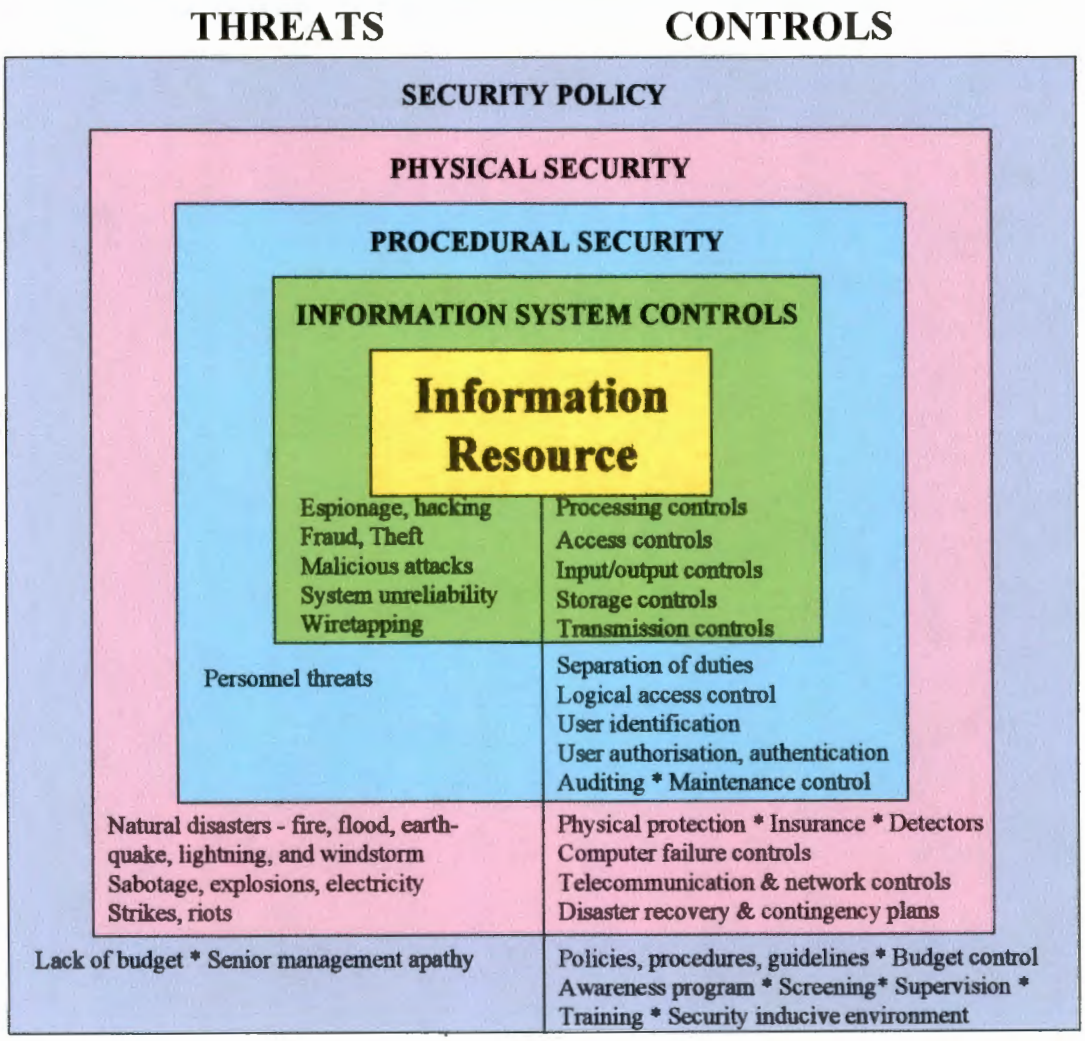
A possibility is to follow an architectural approach. An architectural approach implies a proactive understanding of how information is used throughout the organisation and its corresponding security requirements. Thus the following two aspects must be secured:

- Continuity of computing services (the availability aspect of security) by the establishment of strict maintenance service standards, the provision of redundant support services, strict change control standards, strict back up procedures, and training of employees.

- Control of access to information (the confidentiality and integrity aspects) through logical access control and user accountability. Authentication can be obtained through passwords or third party authentication software.

The implementation of countermeasures is graphically illustrated in figure 7.2.

Figure 7.2: Information security countermeasures



Adapted from O'Brien (1996:581)

From this figure it is evident that the various control measures are placed within the framework of an organisation's security policy, procedures and guidelines. The next layer in the multi-

layered information security control plan is physical security, which entails basic physical protection of all information assets. The following layer comprises procedural security and focuses on personnel and logical access control. The inner layer is that of information system controls that are mostly concerned with input, output, processing and storage controls.

7.6.1.2.8 Monitoring of information security

Regular security audits at Kynoch Fertilizer (Pty) Ltd is necessary to optimise the operations of the security program. The person or team performing the audit should report to the functionally responsible security manager and should operate independently from the monitoring of information security by top management.

Resource elements which can be used by management for the application and monitoring of information security, may include:

- A security committee and team to co-ordinate and implement all aspects regarding information security.
- Internal and external audits to ensure that information security meets the policy, procedures and rules stipulated by management.
- Quality assurance to ensure that standards and prerequisites will be met.
- Security administration that administrates and regulates information security.

7.6.1.2.9 Information security conscious environment

Many of the security problems and threats can be eliminated if the ordinary employee takes it in himself or herself to be part of the solution to information security. Security management should therefore create an environment at Kynoch Fertilizer (Pty) Ltd, which would facilitate total information security. This can only be done by:

- Starting with a comprehensive awareness program.
- Training and education programs, which emphasise the information security threats and vulnerabilities, faced by the organisation. All new employees should go through an introductory computer security course, with a refresher course every six months or at least every year.

- Thorough planning of all aspects of information security.
- Clear information security policy statements, standards and guidelines.
- Well documented procedures for information security.
- Implementation of information security.
- Top management commitment to the strict enforcing of discipline with regard to information security.

7.6.2 AN INFORMATION SECURITY PLAN

A very important part of the management framework is the information security action plan. To be effective the information security plan of Kynoch Fertilizer (Pty) Ltd should be an integrated plan, which implements multiple levels of security.

A security plan identifies and organises the security activities for a computer system and is both a description of the present situation and a plan for orderly change. A carefully written security plan, supported by senior management, notifies employees that security is important to management and therefore to the organisation as a whole. The plan should address six issues:

- **Policy:** A statement indicating the organisation's commitment to security, the goals of the organisation regarding security, where the responsibility for security lies, information security standards and guidelines.
- **Current security status:** A portrayal of the present status of information security by means of a risk analysis. The status includes a listing of all assets, the security threats, and the controls in place to protect those assets against the threats.
- **Recommendations:** Steps that will eventually lead to meeting the security goals identified previously. Controls should be listed in order of desirability.
- **Accountability:** A complete list describing the responsible persons for the implementation of each security activity. Responsible groups are personal computer users, business process support personnel, database administrators, network administrators, and personnel staff members. Responsibilities of management should also be indicated.
- **Timetable:** A precise record of times and milestones when different security functions are to be performed.

- **Monitoring:** A statement specifying a structure for constant monitoring of the effectiveness of the information security plan, as well as periodic reviews and revisions.

7.7 CRITICAL EVALUATION OF THE STUDY

The success of the study can be measured in terms of the objectives formulated in chapter 1.

7.7.1 PRIMARY OBJECTIVE

The primary objective of this study is to provide practical and feasible managerial recommendations and guidelines for the implementation of a cost effective information security framework and multilevel information security plan that will withstand the current and future information security threats to one of the most valuable assets of Kynoch Fertilizer (Pty) Ltd, namely information.

The primary objective was reached through the formulation of a practical and feasible information security framework and plan in chapter 7. It is believed that if the information security framework and multilevel plan will be implemented by Kynoch Fertilizer (Pty) Ltd, it will tremendously reduce the present information security vulnerabilities and risks, as well as limit the impact of current and future security threats.

7.7.2 SECONDARY OBJECTIVES

To realise the above mentioned primary objective the following secondary objectives were formulated:

- To establish the main factors, key issues and problems that influence information security and control.
- To delineate current trends and solutions in information security and control.
- To assess the strategic management of information security and control.
- To determine the overall state of information security at the central region of Kynoch Fertilizer (Pty) Ltd, for example strategy, policy, security plan, structures, implementations and controls, and to measure it against the ideal information security situation.

- To make recommendations regarding the improvement of information security and control at Kynoch Fertilizer (Pty) Ltd in order to fill the gap between the ideal level of information security and the current level.

The first three objectives were respectively realised through the literature study in chapters 3 to 5. Chapter 3 studied the various information security threats, as well as problems experienced with information security. Chapter 4 looked at current solutions to information security with special attention to various control measures that can be implemented to reduce information security risks. The management of information security and control was addressed in chapter 5.

The fourth objective regarding the overall state of information security at Kynoch Fertilizer (Pty) Ltd was accomplished through the empirical study in chapter 6. The last objective, namely to make recommendations regarding the improvement of information security and control at Kynoch Fertilizer (Pty) Ltd was realised in chapter 7. If the issues and problems identified by the respondents are addressed as recommended, information security at Kynoch Fertilizer (Pty) Ltd will certainly improve.

7.8 RECOMMENDATIONS FOR FURTHER STUDY

The legislative shortcomings concerning the prosecution of hackers in South Africa will have to receive urgent attention. Under current legislation, information does not enjoy the same protection that physical goods do. The complex issues relating to the definition of information will have to be resolved, existing laws will have to be re-written, and new laws will have to be created, otherwise South Africa will remain a safe haven for hackers who cannot be prosecuted for obtaining information illegally via computers. Crime will urgently have to be redefined in the cyberspace age.

7.9 CONCLUSION

We live in an age of information insecurity. Therefore organisations will have to accept that security is a cost of doing business. But ensuring information security on an enterprise wide network is often practically an elusive goal and may even be unattainable because in today's distributed networked environment, open access to information takes precedence over the protection of information integrity, and confidentiality. Various measures and controls that can

be implemented to improve information security have been discussed. The successful protection of information does, however, not hinge entirely on technological developments, but is also a matter of security awareness by senior management and all employees.

Perhaps security is a journey without end. Menaugh (1997) said that having the right mind-set for information security is not "a question of whether or not you're paranoid, it is rather whether you're paranoid enough". In this new age of cybercrime, probably the only totally secure computer system is the one that has been switched off. However, if information security is implemented properly so that it does not overkill, ignore or produce a false sense of security, it will limit the risks to which the organisation is exposed.

7.10 SUMMARY

In this last chapter some final conclusions and recommendations were made. The growing misuse of information technology and the increased dependence on computer technology and systems escalated the requirements for information security. Unfortunately there often is apathy towards information security by management, which leads to an ad hoc approach to information security, as well as major information and financial losses.

As the number of computer applications, processing and hardware increases, the three primary risks of integrity, confidentiality, and availability also increases. The major information security threats currently experienced are external threats, hardware misuse, masquerading, pest programs, bypasses, active misuse, passive misuse, inactive misuse, and indirect misuse.

Although it is not possible to build a completely secure information system and to eliminate all threats and problems, it is possible to minimise the impact and business disruption by implementing administrative, physical, procedural, operational, information systems, systems development and last resort control measures.

Based on the results of the empirical study certain final conclusions regarding the biographical data and information security problems were made. To eventually make recommendations, these conclusions were compared to the ideal information security situation as illustrated in the literature study. The research showed that various areas for improvement exist.

To bridge the present information security gap that exists at Kynoch Fertilizer (Pty) Ltd a practical and feasible information security framework and plan was recommended. Although a completely secure information system at Kynoch may not be attainable, the valuable information asset can to a large extent be protected.

If evaluated on the basis of the objectives formulated in chapter one, it can thus be concluded that the research was a success because all objectives were realised. However, the legal aspect regarding information security deserves further study.

Although information security is a journey without end, it can provide a cost-effective solution to information security threats if implemented properly.

We shall not cease from exploration
And the end of all our exploring
Will be to arrive where we started
And know the place for the first time.

T.S. Elliot
Little Gidding, 5

BIBLIOGRAPHY

ALEXANDER, M. 1995. The real security threat: the enemy within. *Datamation*, 41(13):30-33, July.

ALTER, S. 1996. Information systems: a management perspective. 2nd ed. Menlo Park : Benjamin Cummings. 728 p.

ALTON, K. 1995. Document management: how to choose a technical document and workflow management system: part III: basic features of document organisation and access. *Computer graphics*, 6(8):56-58, November.

ANDERSON, J. 1983. Computer abuse and legal remedies. Johannesburg : University of the Witwatersrand. (Dissertation - M.B.A.) 234 p.

ANGEL, D. & HESLOP, B. 1995. The Internet business companion: growing your business in the electronic age. Reading : Addison Wesley. 242 p.

ANON. 1989. Maximum security – minimal irritation. *Municipal engineer*, 20(3):3-4, March.

ANON. 1990. Taking a stand against computer viruses. *People*, 24:4-6, March.

ANON. 1995a. George Kynoch. *Die Kynoch bulletin*, 4(15):1.

ANON. 1995b. Kynoch kunsmis – die maatskappy vandag. *Die Kynoch bulletin*, 4(15):1.

ANON. 1995c. Sentrale streek - besigheidsplan 1995-2000. Potchefstroom : Kynoch. 14 p.

ANON. 1996a. The South African fertilizer industry. *Nitrogen*, 223:17-20, September/October.

ANON. 1996b. South Africa's nitrogen fertilizer producers. *Nitrogen*, 223:22-23, September/October.

ANON. 1996c. Sentrale streek - besigheidsplan 1996-2001. Potchefstroom : Kynoch. 19 p.

ANON. 1996d. McAfee network security and management: anti-virus solutions. Johannesburg : Syscon. 10 p.

ANON. 1997. Sentrale streek - besigheidsplan 1997-2002. Potchefstroom : Kynoch. 25 p.

ANON. 1998. RFC 11 35. Available on the Internet: http://info.internet.isi.edu/in-notes/rfc/files/rfcll35.txt [Date of use: 25 June 1998].

APPLEGATE, L.M., McFARLAN, F.W. & McKENNEY, J.L. 1996. Corporate information systems management: text and cases. 4th ed. Chicago : Irwin. 796 p.

ASLAM, T., KRSUL, I. & SPAFFORD, E.H. 1997. Use of a taxonomy of security faults. Available on the Internet: FTP: Taxonomy_of_Security_Faults.ps at coast.cs.purdue.edu [Date of use: 10 May 1997].

AVOLIO, F.M. & RANUM, M.J. 1997. A network perimeter with secure external access. Available on the Internet: FTP: Avolio_Ranum_isoc.94-paper.ps.Z at coast.cs.purdue.edu [Date of use: 10 May 1997].

BADENHORST, K.P. 1989. 'n Metodologie vir die implementering van rekenaarsekerheid in 'n groot organisasie. Johannesburg : Randse Afrikaanse Universiteit. (Verhandeling – M.Sc.) 232 p.

BERENSON, M.L. & LEVINE, D.M. 1996. Basic business statistics: concepts and applications. 6th ed. Englewood Cliffs : Prentice-Hall International. 943 p.

BETH, T., BORCHERDING, M. & KLEIN, B. 1994. Valuation of trust in open networks. (*In* Gollmann, D.G., *ed.* Computer security - ESORICS 94: third European symposium on research in computer security, Brighton, United Kingdom, November 7-9, 1994: proceedings. Berlin : Springer-Verlag. p. 3-18.)

BEZUIDENHOUT, R.J. 1988. 'n Strategiese bestuursbenadering tot sekuriteit en beheer binne 'n komplekse gerekenariseerde inligtingstelselomgewing. Potchefstroom : PU vir CHO. (Skripsie - M.B.A.) 141 p.

BISKUP, J., MORGENSTEIN, M. & LANDWEHR, C.E., *eds.* 1994. Database security, VIII: status and prospects – proceedings of the IFIP WG 11.3 working conference on database security, Bad Salzdetfurth, Germany, 23-26 August, 1994. Amsterdam : North Holland. 403 p.

BOWEN, A. 1994. (Back) up the river without a copy. *S.A. computer buyer*, 2(6):36-38, July.

BOWEN, A. 1995. Disknet. *S.A. computer buyer*, 3(1):98, January.

BOYLE, P. 1996. A great server room. *PC magazine: Southern Africa*, 4(3):1-8, April.

BROTHERS, M.H. 1990. Computer virus protection procedures. (*In* Denning, P.J., *ed.* Computers under attack: intruders, worms, and viruses. New York : ACM Press. p. 356-380.)

CAMPLING, R. 1997. Computer crime is a profitable business. *Computer week*, 20(38):1, September.

CARDEN, E. 1976. The design of an order processing and inventory control information system for a pharmaceutical company. Pretoria : Unisa. (Dissertation - M.B.L.) 167 p.

CHAPMAN, D.B. 1997. Network (in)security through IP packet filtering. Available on the Internet: FTP: Brent_Chapman_packet_filtering.ps.Z at coast.cs.purdue.edu [Date of use: 10 May 1997].

CHEN, L. 1994. Oblivious signatures. (*In* Gollmann, D.G., *ed.* Computer security - ESORICS 94: third European symposium on research in computer security, Brighton, United Kingdom, November 7-9, 1994: proceedings. Berlin : Springer-Verlag. p. 161-172.)

CHRISTOFFERSON, P., EKHALL, S., FÅK, V., HERDA, S., MATGTILA, P., PRICE, W. & WIDMAN, K. 1988. Crypto users' handbook: a guide for implimentors of cryptographic protection in computer systems. Amsterdam : Elsevier Science Publishers. 93 p.

CLAASSEN, G.J. 1994. Security model, protocols and architecture for open distributed systems. Pretoria : University of Pretoria. (Thesis - Ph.D.) 293 p.

CLARKE, L.G. 1976. Die beplanning en beheer van 'n bestuursinligtingstelsel wat geskep word met die klem op strategiese beplanning en die uitwerking wat dit het op die huishouding van die onderneming. Pretoria : Universiteit van Pretoria. (Skripsie - M.B.A.) 63 p.

CLEMENT, J.H. 1992. Evaluation and control of information technology investments. Johannesburg : University of the Witwatersrand. (Dissertation - M.B.A.) 134 p.

CLOETE, J. 1995. Biometrics : special identification methods for Nedcor's low income group. Potcefstroom : Potchefstroom University for Christian Higher Education. (Dissertation – M.B.A.) 107 p.

CONRADIE, H. 1996. Computer crimes and computer criminals. *Elektron*, 13(1):71, January.

CORBRIDGE, B., HENIG, R. & SLATER, C. 1997. Packet filtering in an IP router. Available on the Internet: FTP: filtering_ip_router.ps.Z at coast.cs.purdue.edu [Date of use: 10 May 1997].

CROSBIE, M., DOLE, B., ELLIS, T., KRSUL, I. & SPAFFORD, E. 1997. IDIOT - Users guide. Available on the Internet: FTP: IDIOT_User_Guide.ps at coast.cs.purdue.edu [Date of use: 10 May 1997].

CROSBIE, M. & SPAFFORD, E. 1997. Applying genetic programming to intrusion detection. Available on the Internet: FTP: mcrosbie-spaf-AAAI-paper.ps.Z at coast.cs.purdue.edu [Date of use: 10 May].

CUNNINGHAM, P.M. 1989. The business security handbook. Mellville : Hans Strydom Publishers. 189 p.

CURRIE, W. 1995. Management strategy for I.T.: an international perspective. London : Pitman. 310 p.

DAELLENBACH, H.G. 1994. Systems and decision making: a management science approach. Chichester : Wiley. 545 p.

DAVIS, B.D. & OLSON, M.H. 1987. Management information systems: conceptual foundations, structure and development. 3rd ed. New York : McGraw-Hill. 693 p.

DENNING, P.J., *ed.* 1990. Computers under attack: intruders, worms, and viruses. New York : ACM Press. 554 p.

DE RU, W.G. 1992. Die toepassing van ekspertstelseltegnologie binne inligtingsekerheid. Johannesburg : Randse Afrikaanse Universiteit. (Verhandeling - M.Sc.) 278 p.

DE SOETE, M. 1993. Public key cryptography. (*In* Preneel, B., Govaerts, R. & Vandewalle, J., *eds.* Computer security and industrial cryptography: state of the art and evolution: ESAT course, Leuven, Belgium, May 21-23, 1991. Berlin : Springer-Verlag. p. 33-49.)

DE VRIES, M. 1997. Verbal communication to the author. Potchefstroom.

DOUGALL, E.G., *ed.* 1993. Computer security: proceedings of the IFIP TC11 ninth international conference on information security, IFIP/Sec'93, Toronto, Canada, 12-14 May, 1993. Amsterdam : North-Holland. 417 p.

DRUMMOND, R. 1997. Safe and secure electronic commerce. *Computer week*, 20(18):26-27, May.

DU TOIT, L.M. 1992. 'n Model vir inligtingsekerheidsdokumentasie. Johannesburg: Randse Afrikaanse Universiteit. (Verhandeling - M.Sc.) 186 p.

EDWARDS, N.G. 1988. Die ontwikkeling en implementering van 'n formele model vir logiese toegangsbeheer in rekenaarstelsels. Johannesburg : Randse Afrikaanse Universiteit. (Verhandeling - M.E.B.) 181 p.

ELLIOT, G. & STARKINGS, S. 1998. Business information technology systems, theory and practice. London : Longman. 343 p.

ELOFF, J.H.P. 1980. Rekenaarsekuriteit met besondere verwysing na die programmatuuraspek. Johannesburg : Randse Afrikaanse Universiteit. (Verhandeling - M.Sc.) 201 p.

ELOFF, J. 1995. Information security: state-of-the-art overview. *Information technology review*, 2(11):39-40, November.

ERNST & YOUNG. 1996. Second annual information security survey: trends, concerns, and practices. Johannesburg. 15 p.

ERNST & YOUNG. 1997. Third annual information security survey: analysis of trends, issues & practices. Johannesburg. 14 p.

ERNST & YOUNG INTERNATIONAL. 1997. First annual global information security survey. 16 p.

ERNST & YOUNG INTERNATIONAL. 1998. Second annual global information security survey. 29 p.

ERWIN, G.J. & BLEWETT, C.N. 1996. Business computing: an African perspective. Kenwyn : Juta. 697 p.

ETHERIDGE, D. & SIMON, E. 1992. Information networks: planning and design. New York : Prentice Hall. 290 p.

FISHER, J. 1998a. Java and JavaScript vulnerabilities, CIAC notes 96-01, March 18 1996. Available on the Internet: http://www.ciac.org/ciac/notes/notes96-01.shtml [Date of use: 6 May 1998].

FISHER, J. 1998b. Security and web search engines, CIAC notes 96-01, March 18 1996. Available on the Internet: http://www.ciac.org/ciac/notes/notes96-01.shtml [Date of use: 6 May 1998].

FITZGERALD, J. 1984. Designing controls into computerized systems. Redwood City : Fitzgerald. 157 p.

FITZGERALD, K.J. 1994. Establishing security in a multi-platform, multi-vendor, enterprise-wide IT environment. *Information management & computer security*, 2(4):9-15.

FORCHT, K.A. 1994. Computer security management. Danvers : Boyd & Fraser. 486 p.

FORREST, S. & PERELSON, A. 1997. Self-nonself discrimination in a computer. Available on the Internet: FTP: self-nonself.ps.gz at coast.cs.purdue.edu [Date of use: 10 May 1997].

FRANK, F. 1997. Artificial intelligence and intrusion detection: current and future directions. Available on the Internet: FTP: ai-intrusion-detection.ps.Z at coast.cs.purdue.edu [Date of use: 10 May 1997].

GERICKE, S. 1987. Security and control of electronic funds transfer specific to a corporate dial-up environment. Johannesburg : Rand Afrikaans University. (Dissertation - M.Com.) 50 p.

GOLLMANN, D.G., *ed.* 1994. Computer security - ESORICS 94: third European symposium on research in computer security, Brighton, United Kingdom, November 7-9, 1994: proceedings. Berlin : Springer-Verlag. 468 p.

GONZALEZ, S. 1996. Satan and Courtney: a devil of a team. *PC magazine: Southern Africa*, 4(1):113-114, February.

HAAG, S., CUMMINGS, M. & DAWKINS, J. 1998. Management information systems for the information age. Boston : Irwin/McGraw-Hill. 528 p.

HABRA, N., LE CHARLIER, B., MOUNJI, A. & MATHIEU, I. 1997a. ASAX: software architecture and rule-base language for universal audit trail analysis. Available on the Internet: FTP: HabraCharlierEtAl92.ps at coast.cs.purdue.edu [Date of use: 10 May 1997].

HABRA, N., LE CHARLIER, B., MOUNJI, A. & MATHIEU, I. 1997b. Preliminary report on advanced security audit trail analysis on UNIX. Available on the Internet: FTP: HabraCharlierEtAl94.ps at coast.cs.purdue.edu [Date of use: 10 May 1997].

HARDJONO, T. & SEBERRY, J. 1994. Authentication via multi-service tickets in the *Kuperee* server. (*In* Gollmann, D.G., *ed.* Computer security - ESORICS 94: third European symposium on research in computer security, Brighton, United Kingdom, November 7-9, 1994: proceedings. Berlin : Springer-Verlag. p. 143-160.)

HEYDENRYCH, F. 1996. When will the Internet grow up? *Information technology review*, 3(2):12-13,15-16,19, March.

HIGHLAND, H.J. 1993. A view of information security tomorrow. (*In* Dougall, E.G., *ed.* Computer security: proceedings of the IFIP TC11 ninth international conference on information security, IFIP/Sec'93, Toronto, Canada, 12-14 May, 1993. Amsterdam : North-Holland. p. 1-11.)

HOFFMAN, L.J. 1973. Security and privacy in computer systems. Los Angeles : Melville Publishing Company. 422 p.

HOLTON, G. 1996. Computer viruses are out there but you may still surf the Internet with confidence. (*In* Networld & Landaba 96.) [CD-ROM.]

HRUSKA, J. 1992. Computer viruses and anti-virus warfare. 2nd ed. New York : Ellis Horwood. 224 p.

HUSAIN, K. & PARKER, T. 1996. Linux unleashed. Indeanapolis : Sams Publishing. 1176 p.

HUSSAIN, D.S. & HUSSAIN, K.M. 1992. Information management: Organization, management and control of computer processing. New York : Prentice Hall. 373 p.

HUYSAMEN, G.K. 1994. Methodology for the social and behavioural sciences. Halfway House : Southern. 237 p.

JACOBS, A. 1996a. Sentrale streek besigheidsproses ondersteuning besigheidsplan 1996-2001. Potchefstroom : Kynoch. 14 p.

JACOBS, A. 1996b. Sentrale streek besigheidsproses ondersteuning memorandum. Potchefstroom : Kynoch. 16 p.

JACOBS, A. 1997a. Sentrale streek besigheidsproses ondersteuning besigheidsplan 1997-2002. Potchefstroom : Kynoch. 16 p.

JACOBS, A. 1997b. Verbal communication to the author. Potchefstroom.

JACOBS, A. 1998. Verbal communication to the author. Potchefstroom.

JIWA, A., SEBERRY, J., & ZHENG, Y. 1994. Beacon based authentication. (*In* Gollmann, D.G., *ed.* Computer security - ESORICS 94: third European symposium on research in computer security, Brighton, United Kingdom, November 7-9, 1994: proceedings. Berlin : Springer-Verlag. p. 125-141.)

KALAKOTA, R. & WHINSTON, A.B. 1997. Electronic commerce. Reading : Addison-Wesley. 431 p.

KEPHART, J.O. 1997. A biologically inspired immune system for computers. Available on the Internet: FTP: immune.ps.Z at coast.cs.purdue.edu [Date of use: 10 May 1997].

KIM, G.H. & SPAFFORD, E.H. 1997a. Experiences with Tripwire: using integrity checkers for intrusion detection. Available on the Internet: FTP: Tripwire-SANS.ps.Z at coast.cs.purdue.edu [Date of use: 10 May 1997].

KIM, G.H. & SPAFFORD, E.H. 1997b. The design and implementation of Tripwire: a file system integrity checker. Available on the Internet: FTP: tripwire.ps.Z at coast.cs.purdue.edu [Date of use: 10 May 1997].

KIM, G.H. & SPAFFORD, E.H. 1997c. Tripwire v1.2. Available on the Internet: FTP: Tripwire-1.2.tar.Z at coast.cs.purdue.edu [Date of use: 10 May 1997].

KNIGHT, J. 1995. Personal computing for business. London : Pitman. 308 p.

KROENKE, D. & HATCH, R. 1997. Business information systems: an introduction. 5th ed. New York : Mitchell McGraw-Hill. 516 p.

KO, C., FRINCKE, D.A., GOAN, T. (JR.), HEBERLEIN, L.T., LEVITT, K., MUKHERJEE, B. & WEE, C. 1997. Analysis of an algorithm for distributed recognition and accountability. Available on the Internet: FTP: net-accountability.ps.gz at coast.cs.purdue.edu [Date of use: 10 May 1997].

KUMAR, S. 1997. Classification and detection of computer intrusions. Available on the Internet: FTP: Kumar-intdet-phddis.ps.Z at coast.cs.purdue.edu [Date of use: 10 May 1997].

KUMAR, S. & SPAFFORD, E.H. 1997. A software architecture to support misuse intrusion detection. Available on the Internet: FTP: kumar_spaf-sof-arch.ps.Z at coast.cs.purdue.edu [Date of use: 10 May 1997].

LAY, P.M.Q., ECCLES, M.G., JULYAN, F.W. & BOOT, G. 1994. Die beginsels van handelsdataverwerking. 4de uitg. Kenwyn : Juta. 598 p.

LAUDON, K.C. & LAUDON, J.P. 1995. Information systems: a problem-solving approach. 3rd ed. Fort Worth : Dryden Press. 653 p.

LAUDON, K.C. & LAUDON, J.P. 1997. Essentials of management information systems: organisation and technology. 2nd ed. Upper Saddle River : Prentice Hall. 563 p.

LAUDON, K.C. & LAUDON, J.P. 1998. Management information systems: new approaches to organisation and technology. 5th ed. Upper Saddle River : Prentice Hall International. 693 p.

LENIHAN, W. 1995. Essentials of tight computer security. *Bottom line business*, 24(11):11-12, June.

LE ROUX, A.H. 1989. Die definisie, motivering en implementering van 'n effektiewe kontrolebasis vir beheer oor inligtingstelselprojekte. Potchefstroom : PU vir CHO. (Skripsie - M.B.A.) 107 p.

LIND, D.A. & MASON, R.D. 1994. Business statistics for business and economics. Burr Ridge : Irwin. 504 p.

LODIN, S.W., SCHUBA, C. & KUMAR, S. 1997. Report on CMAD III: 3rd annual workshop on computer misuse and anomaly detection, Sonoma Mission Inn, Sonoma, California, January 10-12, 1995. Available on the Internet: http://www.cs.purdue.edu/coast/cmad_rep.htm [Date of use: 15 May 1997].

LONG, L. 1994. Introduction to computers and information systems. 4th ed. Englewood Cliffs : Prentice Hall. 462 p.

LOUW, E. 1990. Computer viruses: a management concern. Johannesburg : University of the Witwatersrand. (Dissertation - M.B.A.) 232 p.

LOWE, S.J. 1994. Enterprisewide network security: effective implementation and international standards. Charleston : Computer Technology Research Corp. 153 p.

LUBBE, S. & ARMSTRONG, G. 1995. Computer crime and the measures of detection and prevention of such crime. *Vital*, 10(1):19-31, December.

LUCAS, H.C. 1997. Information technology for management. 6th ed. New York : McGraw-Hill. 714 p.

MANDELL, M. 1990. The West German hacker incident and other intrusions. (*In* Denning, P.J., *ed.* Computers under attack: intruders, worms, and viruses. New York : ACM Press. p. 150-185.)

MARTIN, J. 1973. Security, accuracy, and privacy in computer systems. Englewood Cliffs : Prentice-Hall. 626 p.

MARTIN, E.W., DEHAYES, D.W., HOFFER, J.A. & PERKINS, W.C. 1994. Managing information technology: what mangers need to know. 2nd ed. New York : Macmillan. 755 p.

MAURER, U.M. & SCHMID, P.E. 1994. A calculus for secure channel establishment in open networks. (*In* Gollmann, D.G., *ed.* Computer security - ESORICS 94: third European symposium on research in computer security, Brighton, United Kingdom, November 7-9, 1994: proceedings. Berlin : Springer-Verlag. p. 175-204.)

McAFFEE, J. & HAYNES, C. 1989. Computer viruses, worms, data diddlers, killer programs and other threats to your system. New York : St Martin's Press. 235 p.

McLEOD, R. 1998. Management information systems. 7th ed. Upper Saddle River : Prentice Hall. 655 p.

MENAUGH, M. 1997. First line of defense, 10 February 1997. Available on the Internet: http://www.computerworld.com/search/AT-html/9702/970210Slcar0210a.html [Date of use: 20 March 1997].

MENCHING, J.R & ADAMS, D.A. 1991. Managing an information system. Englewood Cliffs : Prentice Hall. 448 p.

MENZIES, R. 1993. Information systems security. (*In* Peppard, J., *ed.* IT strategy for business. London : Pitman. p. 160-175.)

MOUNJI, A. 1997. Advanced security audit trail analysis on Unix. Available on the Internet: FTP: asax-brochure.ps.gz at coast.cs.purdue.edu [Date of use: 15 May 1997].

MURRAY, W. 1995. Security should pay, not cost. *Information technology review*, 2(6):21-24, June.

Misstofvereniging van Suid-Afrika. 1994. Bemestingshandleiding. 3de uitgawe. Lynwoodrif. 116 p.

NORTON, B.R. 1984. A methodology for evaluating the effectiveness of information services. Johannesburg : University of the Witwatersrand. (Dissertation - M.B.A.) 111 p.

O'BRIEN, J.A. 1996. Management information systems: managing information technology in the networked enterprise. 3rd ed. Chicago : Irwin. 623 p.

O'BRIEN, J.A. 1997. Introduction to information systems. 8th ed. Chicago : Irwin. 514 p.

O'BRIEN, J.A. 1998. Introduction to information systems: an internetworked enterprise perspective. 2nd alternate ed. Boston : Irwin/McGraw-Hill. 591 p.

OLIVIER, M.S. 1991. Secure object-oriented databases. Johannesburg : Rand Afrikaans University. (Thesis - Ph.D.) 183 p.

ORVIS, B. 1998a. Microsoft Word macro viruses, CIAC notes 95-12, September 25 1995. Available on the Internet: http://www.ciac.org/ciac/notes/notes12.shtml [Date of use: 6 May 1998].

ORVIS, B. 1998b. Microsoft Word macro virus update, CIAC notes 96-01, March 18 1996. Available on the Internet: http://www.ciac.org/ciac/notes/notes96-01.shtml [Date of use: 6 May 1998].

PARKER, D.B. 1990. The Trojan horse virus and other crimoids. (*In* Denning, P.J., *ed.* Computers under attack: intruders, worms, and viruses. New York : ACM Press. p. 544-554.)

PARKER, D.B. 1996. Computer security. (*In* Microsoft Encarta 97 Encyclopedia.) [CD-ROM.]

PERLMAN, L. 1994. The victim's guide to viruses. *S.A. computer buyer*, 2(1):54-58, February.

PFLEEGER, C.P. 1989. Security in computing. Englewood Cliffs : Prentice Hall. 538 p.

POST, G.V. & ANDERSON, D.L. 1997. Management information systems: solving business problems with information technology. Boston : Irwin/McGraw-Hill. 700 p.

POTTAS, D. 1990. 'n Gerekenariseerde bestuurshulpmiddel vir 'n hoofraamtoegangsbeheerstelsel. Johannesburg : Randse Afrikaanse Universiteit. (Verhandeling - M.Sc.) 145 p.

POTTAS, D. 1995. The automatic generation of information security profiles. Johannesburg : Rand Afrikaans University. (Thesis - Ph.D.) 172 p.

PRENEEL, B., GOVAERTS, R. & VANDEWALLE, J., *eds.* 1993. Computer security and industrial cryptography: state of the art and evolution: ESAT course, Leuven, Belgium, May 21-23, 1991. Berlin : Springer-Verlag. 274 p.

PRITCHARD, J.A.T. 1979. Security in on-line systems. Manchester : NCC Publications. 187 p.

PROSISE, J. 1996. The Netscape security breach. *PC magazine: Southern Africa*, 4(5):119-121, June.

RANUM, M.J. 1995. Internet firewalls: frequently asked questions. Available on the Internet: http://www.v-one.com/faq.htm [Date of use: 10 May 1997].

RANUM, M.J. 1997. A network firewall. Available on the Internet: FTP: Marcus_Ranum_Network_Firewall.ps.Z at coast.cs.purdue.edu [Date of use: 10 May 1997].

RANUM, M.J. & AVOLIO, F.M. 1997. A toolkit and methods for Internet firewalls. Available on the Internet: FTP: Avolio_Ranum_usenix-paper.ps.Z at coast.cs.purdue.edu [Date of use: 10 May 1997].

RAYNER, A.A. 1969. A first course in biometry for agricultural students. Pietermaritzburg : University of Natal Press. 626 p.

REICHARD, K. 1995. Will your business be safe? *PC magazine: Southern Africa*, 3(5):84, June.

RILLEY, C.D. 1981. A managerial framework for the evaluation of information security and privacy in a large chemical organisation. Pretoria : UNISA. (Dissertation - M.B.L.) 129 p.

ROBINSON, A.T. 1997. Internet firewalls - an introduction. Available on the Internet: FTP: Robinson_Firewalls.ps at coast.cs.purdue.edu [Date of use: 10 May 1997].

ROBSON, W. 1997. Strategic management and information systems: an integrated approach. 2nd ed. London : Pitman. 575 p.

ROOS, J.H. & MASHILE, C. 1997. Fertilizer promotion and extension in South Africa. (Address delivered at the IFDC/FSSA international training programme on fertilizer marketing. Pretoria. 11 p.

RORBYE, T.W. 1993. The impact on information systems controls within an organisation when making use of an EDI VAN. Johannesburg : Rand Afrikaans University. (Dissertation - M.Com.) 95 p.

RUSSELL, D. & GANGEMI, G.T. 1992. Computer security basics. Sebastopol : O'Reilly & Associates. 448 p.

SCHAUER, H. & WOLFHUGEL, C. 1997. An Internet gatekeeper. Available on the Internet: FTP: internet_gatekeeper.ps at coast.cs.purdue.edu [Date of use: 10 May 1997].

SCHULTHEIS, R & SUMNER, M. 1998. Management information systems: the manager's view. 4th ed. Burrough Ridge : Irwin/McGraw-Hill. 743 p.

SCOTT, R.F. 1996. Secure data transmission between computers. Durban : University of Natal. (Dissertation - M.Sc. Eng.) 140 p.

SHOCH, J.F & HUPP, J.A. 1990. The "worm" programs - early experience with a distributed computation. (*In* Denning, P.J., *ed.* Computers under attack: intruders, worms, and viruses. New York : ACM Press. p. 264-281.)

SHARRATT, J.R. 1974. Data control guidelines. Manchester : NCC Publications. 136 p.

SMITH, C. 1998. Verbal communication to the author. Potchefstroom.

SMITH, J. 1996. The security impact of remote and Internet access on corporate networks. (*In* Networld & Landaba 96.) [CD-ROM.]

SMRČKA, K. 1996. Virtual reality is firmly anchored in technology and the commercial world, *Martin Creamer's engineering news*, 16(16):57, April.

SOLOMON, A. & KAY, T. 1994. Dr Solomon's PC anti-virus book. Oxford : Newtech. 294 p.

SPAFFORD, E.H., HEAPHY, K.A. & FERBRACHE, D.J. 1990. A computer virus primer. (*In* Denning, P.J., *ed.* Computers under attack: intruders, worms, and viruses. New York : ACM Press. p. 316-355.)

STAIR, R.M. 1992. Principles of information systems: a managerial approach. Boston : Boyd & Fraser. 701 p.

STANG, D.J. 1992. Dealing with network security threats: securing your LAN. Washington : International computer security association. 227 p.

STANIFORD-CHEN, S., CHEUNG, S., CRAWFORD, R., DILGER, M., FRANK, J., HOAGLAND, J., LEVITT, K., WEE, C., YIP, R. & ZERKLE, D. 1997. GrIDS - a graph based intrusion detection system for large networks. Available on the Internet: FTP: grids-nissc96.ps at coast.cs.purdue.edu [Date of use: 10 May 1997].

SOKKOL, P.K. 1995. From EDI to electronic commerce: a business initiative. New York : McGraw-Hill. 305 p.

STEYN, A.G.W., SMIT, C.F., DU TOIT, S.H.C. & STRASHEIM, C. 1994. Moderne statistiek vir die praktyk. Pretoria : J.L. van Schaik. 736 p.

STINSON, D.R., *ed.* 1994. Advances in cryptology - CRYPTO '93: 13th annual international cryptology conference, Santa Barbara, California, USA, August 1993: proceedings. Berlin : Springer-Verlag. 491 p.

STRASSMAN, P. 1997. What's the best IS defense? Being prepared, 10 May 1997. Available on the Internet: http://www.computerworld.com/search/AT-html/9702/970210SL021ps.html [Date of use: 2 April 1998].

STROSS, C. 1996. The web architect's handbook. Harlow : Addison Wesley. 289 p.

SUNDARAM, A. 1998. An introduction to intrusion detection. Paper published by ACM crossroads and technology manager. Available on the Internet: http://www.cs.purdue.edu/homes/sundaram/papers/intrus.html [Date of use: 15 May 1998].

SWANEPOEL, R. 1997. SAP administrator's reference guide: HP-UX 10.01 – SAP 2.2F – ORACLE 7.1.6: v1.1. Johannesburg : HiPerformance Systems. 62 p.

TABIBIAN, O.R. 1995. Commerce builder, communications builder. *PC magazine: Southern Africa*, 3(10):75,77-78, November.

TACKETT, J., GUNTER, D. & BROWN, L. 1995. Using Linux. Indianapolis : Que. 861 p.

THIBODEAU, P. 1997. Technology forum international conference held to address Internet security, New York, January 1997. Available on the Internet: http://www.computerworld.com /search/AT-html/9701/970122conferencesecurity.html [Date of use: 20 March 1997].

THOMPSON, K. 1990. Reflections on trusting trust. (*In* Denning, P.J., *ed.* Computers under attack: intruders, worms, and viruses. New York : ACM Press. p. 97-104.)

THOMPSON, A.A. & STRICKLAND, A.J. 1996. Strategic management: concepts and cases. 9th ed. Chicago : Irwin. 1035 p.

THURAISINGHAM, B.M. & LANDWEHR, C.E., *eds.* 1993. Database security, VI: status and prospects - results of the IFIP WG 11.3 workshop on database security, Vancouver, Canada, 19-21 August, 1992. Amsterdam : North Holland. 397 p.

TRICKETT, D.B. 1972. Management control information systems within a large organisation. Pretoria : University of South Africa. (Dissertation - M.B.L.) 168 p.

VAN DER MERWE, S.P. 1992. Die ontwikkeling van 'n landboubestuursinligtingstelsel deur middel van 'n inligtingsentrum in die hoëveldstreek. Potchefstroom: PU vir CHO. (Skripsie - M.B.A.) 156 p.

VAN DER SPUY, P.M. 1971. Die inligtingstelsels vir beplanning en beheer in 'n langtermyn-versekeringsmaatskappy met spesifieke verwysing na die bestuursrekeningkundige stelsel. Pretoria : Unisa. (Skripsie - M.B.L.) 156 p.

VAN DYK, P. 1990. Rekenaarsekerheid in mikrorekenaarstelsels. Johannesburg : Randse Afrikaanse Universiteit. (Verhandeling - M.Sc.) 323 p.

VAN ROOYEN, A. 1997. Verbal communication to the author. Potchefstroom.

VAN ROOYEN, A., VAN TONDER, M.D., COETZEE, M., PRETORIUS, F.A., JACOBS, A., & CRAVEN, J. 1997. "Brainstorm". Potchefstroom. 10 p.

VILJOEN, P.J.D. 1997. Opening address at IFDC/FSSA international training programme on fertilizer marketing: challenges and opportunities. Pretoria. 5 p.

VON SOLMS, R. 1993. Information security management: processes and metrics. Johannesburg : Rand Afrikaans University. (Thesis - D.Sc.) 143 p.

VON SOLMS, S.H. 1996. S-HTTP ensures security. *Computer week*, 19(42):18, October.

VON SOLMS, S.H. & ELOFF, J.H.P. 1997. Information security. Johannesburg : Department of Computer Science, Rand Afrikaans University. 88 p.

VAN TILBURG, J. 1993. Secret-key exchange with authentication. (*In* Preneel, B., Govaerts, R. & Vandewalle, J., *eds.* Computer security and industrial cryptography: state of the art and evolution: ESAT course, Leuven, Belgium, May 21-23, 1991. Berlin : Springer-Verlag. p. 71-86.)

VAN WYK, M. 1997. Verbal communication to the author. Potchefstroom.

VAN ZYL, P.W.J. 1990. 'n Stelsel vir logiese toegangsbeheer in 'n mikrorekenaarstelsel. Johannesburg : Randse Afrikaanse Universiteit. (Verhandeling - M.Sc.) 120 p.

WAGNER, T. 1997. The business process reengineering of the capital purchasing function of Sentech (Pty) Ltd. Potchefstroom : Potchefstroomse Universiteit vir Christelike Hoër Onderwys. (Dissertation – M.B.A.) 112 p.

WALKER, B.J. & BLAKE, I.F. 1977. Computer security and protection structures. Stroudsburg : Dowden, Hutchinson & Ross. 142 p.

WARD, M. 1997. Web sites are a hacker's heaven. *New scientist*, 1:4, Jan.

WILKINSON, B.J.S. 1987. Managerial control of information systems and computer cost chargeout. Cape Town : University of Cape Town. (Dissertation - M.B.A.) 174 p.

WITTEN, I.H. 1990. Computer (in)security: infiltrating open systems. (*In* Denning, P.J., *ed.* Computers under attack: intruders, worms, and viruses. New York : ACM Press. p. 105-142.)

WONG, K. & WATT, S. 1990. Managing information security: a non-technical management guide. Oxford : Elsevier Science Publishers. 327 p.

WOOD, C.C. 1995. Writing infosec policies. *Computers & security*, 14(8):667-674.

ZWASS, V. 1992. Management information systems. Dubuque : Brown. 896 p.

ANNEXURES

ANNEXURE A

Potchefstroomse Universiteit
vir Christelike Hoër Onderwys

Potchefstroom University
for Christian Higher Education

Private bag X6001 Potchefstroom 2520
Tel (018) 299 1111 Fax (018) 299 2799

GRADUATE SCHOOL OF MANAGEMENT
Tel (018) 2991338
Fax (018) 2991416
E-Mail badlchf@puknet.puk.ac.za

Dear Kynoch employee

Information is such a valuable corporate asset, but can so easily be abused or misused. Therefore information security and control has over the years become more important in all industries. The problem, however, is that many organisations do not implement an active information security plan, or when implemented it is often done half-heartedly. There is also a growing concern regarding the ability of current tools, methods, solutions, and human resources to meet the information security challenges and issues.

To determine the information security situation at Kynoch Fertilizer (Pty) Ltd I am currently conducting an information security survey. The survey addresses information security policies and procedures, satisfaction with currently available security solutions, and security concerns. The survey is being given to a select number of employees, like yourself. As the response of every person in the population is important, we would greatly appreciate it if you would complete the enclosed survey questionnaire and return it to **Mr Andries Jacob's office** by no later than **30 April 1998**.

The questionnaire is specifically designed to obtain information about the information security at Kynoch. Almost all questions can be answered by making a cross in the appropriate column. You are to choose the column that best matches the description of how you feel about the item.

As the survey will mainly be used as the basis for a research project, your answers will be treated as confidential.

I thank you in advance for your participation.

Yours sincerely

Dr Louis Fourie
Senior Lecturer: Graduate School of Management

ANNEXURE B

INFORMATION SECURITY QUESTIONNAIRE

SECTION A

DEMOGRAPHIC AND PERSONAL INFORMATION

All participating employees must please complete this section.

Please mark the appropriate box with an X.

1. Which age category do you fall into?

Under 20	21-29	30-39	40-49	50-59	Above 60

2. Which sex category do you fall into?

Male	Female

3. What is your position?

NAME	LEVEL	
Departmental head	10-12	
Functional head	8-10	
Supervisor	6-8	
Administrative	6-8	
Administrative	3-5	
Network or system administrator	6-8	
Other	-	

4. What department are you working in?

Finance	
Marketing	
Production	
Logistics	
Human Resources	
Business process support	

5. Length of service at Kynoch (in years)?

Less than 1	1-5	6-10	11-15	16-20	21-25	26-30	More than 30

6. Which statement best describes your education level?

No formal schooling	
Matriculation	
Diploma	
Technikon qualification	
B. Degree	
Honours degree	
Masters or doctorate	
Other post-graduate qualification	

7. What is your present level of computer experience?

No computer experience	
Very little computer experience – need help	
I can help myself	
Able to use standard applications (for example MS Word, Quattro Pro)	
Can provide support	

SECTION B

COMPUTER SECURITY

All participating employees must please complete this section.
Please evaluate all questions on a four-point scale, and mark the appropriate box with an X.

	Strongly disagree	Disagree	Agree	Strongly agree
GENERAL				
1. Information and data security is important to you personally.				
2. The senior management of Kynoch regards information and data security as very important.				
3. The current top management accept and understand their responsibility towards information security and control well.				
4. The organisation's needs for information security and control are being met by the current top management strategies.				
5. Top management's past performance with regard to information security and control is excellent.				
6. There is a high the level of alignment between business and information security strategy.				
7. The effectiveness of the security administration at Kynoch is of high standing.				
8. My knowledge about information and data security is very good.				
9. I received adequate information security training as a new employee.				
10. I receive regular information security updates or reminders.				
11. My organisation has an effective planned incident response when an intruder is detected in the network or computer systems.				
12. My organisation has an effective formal incident response team				
13. I am very satisfied with the overall level of security on the following systems:				
a) Client/server system (SAP R/3 system)				
b) NT file servers (local and business units)				
c) Communication servers (Internet, Exchange, Customer One)				

	Strongly disagree	Disagree	Agree	Strongly agree
d) Customer Universe				
e) Desktop computers systems				
f) Remote computing				
g) Laptops/notebooks				
14. My information is very accessible to myself despite all the security measures.				
15. Over the past three years, Kynoch's information and data security RISKS have increased.				
Please elaborate:				
16. In retrospection, I would say that Kynoch's information and data security RISKS, relative to the growth in computing resources, have increased more.				
17. I am presently very much concerned about information and data security with regard to the following aspects:				
a) Network security				
b) Multiple log-ons and passwords				
c) End-user computing security awareness				
d) Monitoring user compliance with policies				
e) Distributed computing security				
f) Winning top management commitment				
g) Internet access				
h) External/remote access (dial-in)				
18. The *perceived level of threat* of unauthorised information being disclosed due to the following is very serious:				
a) Suppliers				
b) Competitors				
c) Employees who do not need to know				
d) Customers				
e) Public interest groups				

Section B

	Strongly disagree	Disagree	Agree	Strongly agree
f) Computer "terrorists"				
g) Government				
19. I am satisfied with the overall level of security of my connection to the Internet.				
MICROCOMPUTERS				
20. I regularly backup the hard disk.				
21. My applications are documented sufficiently for another user to operate them in my absence.				
22. I regularly take the micro off-site.				
23. Written permission is required from my manager should I wish to take the micro off-site.				
24. The micro is seldom left in an unattended vehicle.				
25. All floppy disks have a label saying clearly what is on the disk.				
26. Cables attached to the micro do not trail across the floor.				
27. I do not leave the micro switched on when unattended.				
28. All the wiring connected to my micro is electrically safe.				
29. I always have to enter a login identification and password before I can use the micro.				
30. My user identification is unique.				
31. My password is unique.				
32. I change my password regularly.				
33. I log-off from the micro when leaving it for more than fifteen minutes.				
34. I test all new applications and changes to existing applications.				
35. I record version numbers and creation dates for all backups of applications and data.				
36. I do not allow people other than myself and the company's computer specialists to manipulate the system software.				
37. I insist that all new applications and changes to existing applications be delivered with full documentation.				

	Yes	No
38. Did you ever encounter a computer-virus attack?		
39. What, if any, were the consequences of the attack? (Please mark all appropriate items)		
a) Loss of time		
b) Loss of data		
c) Loss of functionality		
d) Specialist consultants used		
e) Employee morale affected		
f) Other consequences		

40. What type of virus was it (if known)?
41. Other details of the attack
42. Any other general observations regarding information security

THANK YOU FOR YOUR VALUABLE TIME

ANNEXURE C

INFORMATION SECURITY QUESTIONNAIRE

SECTION A

DEMOGRAPHIC AND PERSONAL INFORMATION

All participating employees must please complete this section.

Please mark the appropriate box with an X.

1. Which age category do you fall into?

Under 20	21-29	30-39	40-49	50-59	Above 60

2. Which sex category do you fall into?

Male	Female

3. What is your position?

NAME	LEVEL	
Departmental head	10-12	
Functional head	8-10	
Supervisor	6-8	
Administrative	6-8	
Administrative	3-5	
Network or system administrator	6-8	
Other	-	

4. What department are you working in?

Finance	
Marketing	
Production	
Logistics	
Human Resources	
Business process support	

5. Length of service at Kynoch (in years)?

Less than 1	1-5	6-10	11-15	16-20	21-25	26-30	More than 30

6. Which statement best describes your education level?

No formal schooling	
Matriculation	
Diploma	
Technikon qualification	
B. Degree	
Honours degree	
Masters or doctorate	
Other post-graduate qualification	

7. What is your present level of computer experience?

No computer experience	
Very little computer experience – need help	
I can help myself	
Able to use standard applications (for example MS Word, Quattro Pro)	
Can provide support	

SECTION C

COMPUTER SECURITY

All participating departmental heads, functional heads and supervisors must please complete this section.

Please evaluate all questions on a four-point scale, and mark the appropriate box with an X.

	Strongly disagree	Disagree	Agree	Strongly agree
GENERAL				
1. Information and data security is important to you personally.				
2. The senior management of Kynoch regards information and data security as very important.				
3. The current top management accept and understand their responsibility towards information security and control well.				
4. The organisation's needs for information security and control are being met by the current top management strategies.				
5. Top management's past performance with regard to information security and control is excellent.				
6. There is a high the level of alignment between business and information security strategy.				
7. The effectiveness of the security administration at Kynoch is of high standing.				
8. My knowledge about information and data security is very good.				
9. I received adequate information security training as a new employee.				
10. I receive regular information security updates or reminders.				
11. My organisation has an effective planned incident response when an intruder is detected in the network or computer systems.				
12. My organisation has an effective formal incident response team				
13. I am very satisfied with the overall level of security on the following systems:				
a) Client/server system (SAP R/3 system)				
b) NT file servers (local and business units)				
c) Communication servers (Internet, Exchange, Customer One)				

	Strongly disagree	Disagree	Agree	Strongly agree
d) Customer Universe				
e) Desktop computers systems				
f) Remote computing				
g) Laptops/notebooks				
14. My information is very accessible to myself despite all the security measures.				
15. Over the past three years, Kynoch's information and data security RISKS have increased.				
Please elaborate:				
16. In retrospection, I would say that Kynoch's information and data security RISKS, relative to the growth in computing resources, have increased more.				
17. I am presently very much concerned about information and data security with regard to the following aspects:				
a) Network security				
b) Multiple log-ons and passwords				
c) End-user computing security awareness				
d) Monitoring user compliance with policies				
e) Distributed computing security				
f) Winning top management commitment				
g) Internet access				
h) External/remote access (dial-in)				
18. The *perceived level of threat* of unauthorised information being disclosed due to the following is very serious:				
a) Suppliers				
b) Competitors				
c) Employees who do not need to know				
d) Customers				
e) Public interest groups				

	Strongly disagree	Disagree	Agree	Strongly agree
f) Computer "terrorists"				
g) Government				
19. I am satisfied with the overall level of security of my connection to the Internet.				
20. The organisation has rarely experienced information or financial losses over the past three years due to:				
a) Viruses				
b) Malicious acts (outside)				
c) Malicious acts (employees)				
d) Inadvertent errors (insiders or outsiders)				
e) Lack of systems or telecommunications availability (non-natural disaster)				
f) Natural disasters				
g) Industrial espionage				
h) Unknown sources				
21. Information losses in our organisation can mainly be ascribed to:				
a) Network break-ins				
b) Sabotage (employee)				
c) Computer failures				
d) Software errors				
e) Stolen data				
f) Network failures (LAN, WAN)				
g) Other				
22. The major obstacles to addressing information security at Kynoch are:				
a) Lack of tools/security solutions				
b) Lack of human resources				
c) Lack of management awareness of the importance of security				
d) Security planning not part of total strategic and business planning				
e) Lack of budget				
f) Other				
MICROCOMPUTERS				
23. I regularly backup the hard disk.				

	Strongly disagree	Disagree	Agree	Strongly agree
24. My applications are documented sufficiently for another user to operate them in my absence.				
25. I regularly take the micro off-site.				
26. Written permission is required from my manager should I wish to take the micro off-site.				
27. The micro is seldom left in an unattended vehicle.				
28. All floppy disks have a label saying clearly what is on the disk.				
29. Cables attached to the micro do not trail across the floor.				
30. I do not leave the micro switched on when unattended.				
31. All the wiring connected to my micro is electrically safe.				
32. I always have to enter a login identification and password before I can use the micro.				
33. My user identification is unique.				
34. My password is unique.				
35. I change my password regularly.				
36. I log-off from the micro when leaving it for more than fifteen minutes.				
37. I test all new applications and changes to existing applications.				
38. I record version numbers and creation dates for all backups of applications and data.				
39. I do not allow people other than myself and the company's computer specialists to manipulate the system software.				
40. I insist that all new applications and changes to existing applications be delivered with full documentation.				

	Yes	No
41. Did you ever encounter a computer-virus attack?		
42. What, if any, were the consequences of the attack? (Please mark all appropriate items)		
a) Loss of time		
b) Loss of data		

c) Loss of functionality		
d) Specialist consultants used		
e) Employee morale affected		
f) Other consequences		

43. What type of virus was it (if known)?
44. Other details of the attack
45. Any other general observations regarding information security

THANK YOU FOR YOUR VALUABLE TIME

SECTION E

SUMMARISED INFORMATION SECURITY RATING

This section must please be completed by all participating IT personnel, departmental heads, functional heads and supervisors.

Please evaluate all questions on a four-point scale, and mark the appropriate box with an X.

PLEASE RATE THE LEVEL OF YOUR SECURITY IN CONNECTION WITH THE FOLLOWING:	Very poor	Poor	Good	Very good
PHYSICAL AND ENVIRONMENTAL SECURITY				
1. Central site				
2. Fire protection				
3. Power protection				
4. Other hazard protection				
5. Physical access				
6. After hours access				
7. Remote sites				
COMPUTER OPERATIONS				
8. Server performance monitoring				
9. Server performance standards				
10. Documented procedures				
11. Operational logging				
12. Problem logging and resolution				
13. Regular backups				
14. Training of personnel regarding emergencies				
ADMINISTRATIVE SECURITY				
15. Action plans				
16. Co-ordination of plans				
17. Employment and termination				
18. Security policies				
19. Standards				
20. Unified IT control				

	Very poor	Poor	Good	Very good
CONFIGURATION SECURITY				
21. Application software				
22. Change control				
23. Controls over local initiatives				
24. Formal systems development method				
25. Inventory				
26. Systems software				
27. Systems hardware				
DOCUMENTATION SECURITY				
28. Backups				
29. Classification schemes				
30. Disposal of sensitive documentation				
31. Protection of sensitive documentation				
32. Standards				
DATA SECURITY				
33. Access control software				
34. Access to stored data				
35. Classification scheme				
36. Consistency across environments				
37. Control of data input				
38. Database encryption				
39. Data protection				
40. Off-site backup				
41. Review of authorisations				
42. Review of exceptions				
43. Secure distribution of output				
TELECOMMUNICATIONS SECURITY				
44. Access tables kept up to date				
45. Authentication of users, messages				
46. Control of dial-up				
47. Encryption				
48. Logging of access attempts				

	Very poor	Poor	Good	Very good
49. Password management				
50. Sign-on procedures				
51. Unique user identification				
52. Use of access control packages				
MICROCOMPUTER SECURITY				
53. Audit and review				
54. Backups				
55. Central policy on acquisition				
56. Control of application development				
57. Control of data				
58. Control of proprietary software				
59. Encryption				
60. Microcomputer security policy				
CONTINGENCY PLANNING				
61. Disaster recovery plan				
62. Testing of disaster recovery plan				
63. Procedures to update plan				
64. Plan stored off-site				
65. User involvement				
66. Plan covers all environments				
67. Plan covers computer centre and network				
68. Alternative facilities/disaster recovery site				
69. Full off-site backup				
70. Resilience				
71. Continuation of work in case of a disaster				
NETWORK OPERATIONS				
72. Design and implementation standards				
73. Resilient design				
74. Sound documentation				
75. Service-level monitoring				
76. Operations well organised				
77. Control of privileged functions				
78. Access control				

SUPPORT SERVICES SECURITY	Very poor	Poor	Good	Very good
79. Non-disclosure agreements				
80. Supervision of support staff				
81. Supervision of visitors				
82. Couriers				
83. Photocopiers				
84. Mail room (after hours)				

What specific vulnerabilities does the organisation have regarding information security?

What impending threats does the organisation face?

What risks are associated with the threats?

What risks could be reduced if increased security countermeasures are applied?

How are these trade-offs made?

THANK YOU FOR YOUR VALUABLE TIME

ANNEXURE D

INFORMATION SECURITY QUESTIONNAIRE

SECTION A

DEMOGRAPHIC AND PERSONAL INFORMATION

All participating employees must please complete this section.

Please mark the appropriate box with an X.

1. Which age category do you fall into?

Under 20	21-29	30-39	40-49	50-59	Above 60

2. Which sex category do you fall into?

Male	Female

3. What is your position?

NAME	LEVEL	
Departmental head	10-12	
Functional head	8-10	
Supervisor	6-8	
Administrative	6-8	
Administrative	3-5	
Network or system administrator	6-8	
Other	-	

4. What department are you working in?

Finance	
Marketing	
Production	
Logistics	
Human Resources	
Business process support	

5. Length of service at Kynoch (in years)?

Less than 1	1-5	6-10	11-15	16-20	21-25	26-30	More than 30

6. Which statement best describes your education level?

No formal schooling	
Matriculation	
Diploma	
Technikon qualification	
B. Degree	
Honours degree	
Masters or doctorate	
Other post-graduate qualification	

7. What is your present level of computer experience?

No computer experience	
Very little computer experience – need help	
I can help myself	
Able to use standard applications (for example MS Word, Quattro Pro)	
Can provide support	

SECTION B

COMPUTER SECURITY

All participating employees must please complete this section.
Please evaluate all questions on a four-point scale, and mark the appropriate box with an X.

	Strongly disagree	Disagree	Agree	Strongly agree
GENERAL				
1. Information and data security is important to you personally.				
2. The senior management of Kynoch regards information and data security as very important.				
3. The current top management accept and understand their responsibility towards information security and control well.				
4. The organisation's needs for information security and control are being met by the current top management strategies.				
5. Top management's past performance with regard to information security and control is excellent.				
6. There is a high the level of alignment between business and information security strategy.				
7. The effectiveness of the security administration at Kynoch is of high standing.				
8. My knowledge about information and data security is very good.				
9. I received adequate information security training as a new employee.				
10. I receive regular information security updates or reminders.				
11. My organisation has an effective planned incident response when an intruder is detected in the network or computer systems.				
12. My organisation has an effective formal incident response team				
13. I am very satisfied with the overall level of security on the following systems:				
a) Client/server system (SAP R/3 system)				
b) NT file servers (local and business units)				
c) Communication servers (Internet, Exchange, Customer One)				

	Strongly disagree	Disagree	Agree	Strongly agree
d) Customer Universe				
e) Desktop computers systems				
f) Remote computing				
g) Laptops/notebooks				
14. My information is very accessible to myself despite all the security measures.				
15. Over the past three years, Kynoch's information and data security RISKS have increased.				
Please elaborate:				
16. In retrospection, I would say that Kynoch's information and data security RISKS, relative to the growth in computing resources, have increased more.				
17. I am presently very much concerned about information and data security with regard to the following aspects:				
a) Network security				
b) Multiple log-ons and passwords				
c) End-user computing security awareness				
d) Monitoring user compliance with policies				
e) Distributed computing security				
f) Winning top management commitment				
g) Internet access				
h) External/remote access (dial-in)				
18. The *perceived level of threat* of unauthorised information being disclosed due to the following is very serious:				
a) Suppliers				
b) Competitors				
c) Employees who do not need to know				
d) Customers				
e) Public interest groups				

	Strongly disagree	Disagree	Agree	Strongly agree
f) Computer "terrorists"				
g) Government				
19. I am satisfied with the overall level of security of my connection to the Internet.				
MICROCOMPUTERS				
20. I regularly backup the hard disk.				
21. My applications are documented sufficiently for another user to operate them in my absence.				
22. I regularly take the micro off-site.				
23. Written permission is required from my manager should I wish to take the micro off-site.				
24. The micro is seldom left in an unattended vehicle.				
25. All floppy disks have a label saying clearly what is on the disk.				
26. Cables attached to the micro do not trail across the floor.				
27. I do not leave the micro switched on when unattended.				
28. All the wiring connected to my micro is electrically safe.				
29. I always have to enter a login identification and password before I can use the micro.				
30. My user identification is unique.				
31. My password is unique.				
32. I change my password regularly.				
33. I log-off from the micro when leaving it for more than fifteen minutes.				
34. I test all new applications and changes to existing applications.				
35. I record version numbers and creation dates for all backups of applications and data.				
36. I do not allow people other than myself and the company's computer specialists to manipulate the system software.				
37. I insist that all new applications and changes to existing applications be delivered with full documentation.				

	Yes	No
38. Did you ever encounter a computer-virus attack?		
39. What, if any, were the consequences of the attack? (Please mark all appropriate items)		
a) Loss of time		
b) Loss of data		
c) Loss of functionality		
d) Specialist consultants used		
e) Employee morale affected		
f) Other consequences		

40. What type of virus was it (if known)?
41. Other details of the attack
42. Any other general observations regarding information security

THANK YOU FOR YOUR VALUABLE TIME

SECTION D

QUESTIONNAIRE FOR IT PERSONNEL

COMPUTER SECURITY

All participating IT personnel must please complete this section.

Please evaluate all questions on a four-point scale, and mark the appropriate box with an X.

	Strongly disagree	Disagree	Agree	Strongly agree
1. GENERAL SECURITY				
1. There is a high level of integration of security considerations in our system development processes of the following:				
a) Client/server system (SAP R/3 system)				
b) NT or UNIX system				
c) Communication system (Internet., Exchange, Customer One)				
d) Desktop computing				
e) Remote computing				
f) Laptop/notebook computing				
2. The following security measures are used regularly:				
a) File encryption				
b) One-time (token-based) passwords				
c) Security evaluation software				
d) Network access control software				
e) Single sign-on software				
f) Virus detection software				
g) Dial back or secure modems				
h) Public-key cryptography				
i) Firewalls to protect from external access				
j) Redundant communications or power				

	Strongly disagree	Disagree	Agree	Strongly agree
k) PC access control software				
l) PC hardware security devices				
m) Signature verification				
n) Business continuity planning software				
o) Telecommunications encryption				
p) Biometrics to authenticate users				
q) Message authentication codes				
r) Terminal key locks or lock words				
3. Our organisation has an experienced team solely for information security and business continuity planning.				
4. Business continuity planning is being considered a high priority.				
5. The following aspects are always important aspects of business continuity planning:				
a) Computer/operations centre				
b) LAN				
c) End-user computing				
d) Recovery of mission critical business processes				
e) Complete restoration of systems				
6. The company's formal corporate information security policy is regarded as very important.				
7. The following aspects are considered to be very important according to the security policy:				
a) Centralised security administration				
b) Business continuity planning				
c) Surveillance and monitoring				
d) External access				
e) Data classification				
f) Records management				
g) End user computing				
h) Non disclosure agreements by personnel				

		Strongly disagree	Disagree	Agree	Strongly agree
	i) Electronic commerce				
	j) Incident response and reporting				
2. NETWORK SECURITY					
8.	**The network security at Kynoch is very effective.**				
9.	**I am confident that the network at Kynoch is protected from internal and external attacks.**				
10.	**LAN usage is actively being monitored.**				
11.	**Network connections to trusted business partners and clients are constantly being monitored.**				
12.	**All transmitted information is encrypted prior to transmission outside the building.**				
13.	**The following control techniques are important to us when using EDI for business transactions:**				
	a) Passwords				
	b) Trading partner ID and profile verification				
	c) Encryption				
	d) Message authentication codes				
	e) Control totals				
	f) Functional acknowledgements				
	g) Application acknowledgements				
14.	**The network totally prevent contamination through viruses contained in DOS, shell, and device drivers used at workstations.**				
15.	**All application programs are fully protected so that, should a virus make any modification in them, they will not run in the network.**				
16.	**The network always disable and control the operation of the "AUTOEXEC.BAT" and "CONFIG.SYS" files to prevent the introduction of unauthorised programs or viruses from that source.**				
17.	**The network operation is tightly coupled to the login routine, permitting no breach during or after login.**				
18.	**The network prevents login of a given user except from specified workstations.**				
19.	**The user is the only person who can make a permanent change in his/her password.**				

		Strongly disagree	Disagree	Agree	Strongly agree
20.	**The user's login name and password are in all instances encrypted by the system, so that no other user can learn what it is.**				
21.	**A start-up script is imposed on all users to regulate the nature and extent of security that all users will experience.**				
22.	**The start-up script is modifiable by the system director only.**				
23.	**Each user is provided with a totally private, personal work area that is inaccessible to any other user, including the system director.**				
24.	**File space on the network can be fully restricted so that only selected, authorised users can access it.**				
25.	**The network permits all users to send files to a given user's "in-basket," but prevent them from reading the other files or over-writing them.**				
26.	**Users are denied the ability to run any program on the network, unless they do it through a menu system that has been designed by the system administrator.**				
27.	**Each network node is protected by physical access control.**				
28.	**The cable routing is routinely inspected to ensure that there are no taps in it.**				
	3. INTERNET SECURITY				
29.	**All internet activities are monitored constantly.**				
30.	**The possibility of someone breaking into our system via the Internet is very remote.**				
31.	**The following control techniques related to the Internet are used regularly:**				
	a) Passwords				
	b) Encryption				
	c) Firewalls (application-based, workstation-based, and/or router-based)				
	d) One-time (token-based) passwords				
	4. CONTROLS ON PERSONNEL				
32.	**Responsibilities are always divided so that fraud cannot be carried out without collusion.**				
33.	**Departments and close associates are totally separated so as to minimise the likelihood of collusion.**				

		Strongly disagree	Disagree	Agree	Strongly agree
34.	**Background checks are performed on all new employees.**				
35.	**Employees who constipate a threat can be transferred or dismissed immediately.**				
36.	**All critical jobs are rotated periodically.**				
37.	**All personnel take security seriously.**				
38.	**Casual practices - such as leaving classified documents unlocked – are common.**				
39.	**A "clean desk" policy is strictly enforced.**				
	5. SENSITIVE PROGRAMS				
	Definition of a "sensitive" program: *A sensitive program is one in which a programmer can, by changing program instructions only, misappropriate company assets and conceal the act even though adequate administrative processing controls are in place. They are the programs in the system where important internal control tests are made. The more sensitive areas have been identified as payroll, accounts payable, fixed assets, purchasing, and inventory control.*				
40.	**Separation of maintenance responsibility for sensitive programs between programmers is adequate.**				
41.	**Programs and documentation are always stored in a secure location to prevent unauthorised access.**				
42.	**Unauthorised parting and changing of sensitive programs is prevented so that no programmer or operator can bypass the safeguards.**				
43.	**An independent party always reviews all requests for updates to sensitive programs, and advises management of questionable changes.**				
44.	**Frequent unannounced periodic audits of program changes for authorisation and documentation are sufficient?**				
	6. NEW PROGRAMS AND PROGRAM CHANGES				
45.	**All new programs and changes to existing programs are reviewed and approved by management.**				
46.	**A knowledgeable person within the controller's function also regularly reviews these new programs, program changes, and program documentation on an unannounced basis.**				
47.	**If a representative sample of permanent and one-time computer jobs are evaluated:**				
	a) All jobs or revisions will be supported by written requests				

		Strongly disagree	Disagree	Agree	Strongly agree
	b) All requests will be properly approved by the department management, as well as the appropriate business process support manager				
	c) Program documentation will be adequate and maintained				
48.	**There is a thorough procedure established that prevents programs from being changed without the knowledge and consent of the user's department.**				
49.	**"User department" management formally review and approve:**				
	a) New programs and program changes during the design phase				
	b) Data used to test programs and the results of these tests				
50.	**A full history of changes to these programs is maintained.**				
51.	**The computer centre will never accept a new or changed program without the necessary approvals being evident.**				
52.	**Adequate controls have been established to insure that review and approval procedures cannot be bypassed.**				
53.	**All program tests and debugging are supervised and documented.**				
	7. INPUT/OUTPUT CONTROLS				
54.	**Adequate controls exist for input of sensitive data from point of origin.**				
55.	**Adequate controls exist for the distribution of output to designated areas.**				
56.	**Effective controls have been established for point of origin review of rejected sensitive transactions.**				
57.	**Effective controls have been established for correcting errors in input/output at the point of origin.**				
58.	**Responsibility has been established for following up all input errors to ensure that they are properly corrected and returned for processing.**				
59.	**When management receives logged exceptions (or significant events), the necessary action will always be taken.**				
60.	**To test the system's validation controls, the auditor regularly fed in invalid transactions to see what the system does with them.**				
	8. TAPE AND DISK LIBRARY				
61.	**Magnetic tapes and disk packs are stored in a special library area**				

		Strongly disagree	Disagree	Agree	Strongly agree
	(usually closed, dust free, fire resistant and lockable).				
62.	**The library has an adequate alarm and sprinkler system.**				
63.	**Only one person is responsible for the administration of the library (for example a librarian or scheduling clerk).**				
64.	**Access to the library is restricted to authorised personnel only.**				
65.	**The inventory list of tapes and disk packs is updated regularly.**				
66.	**The minimum information is always included (for example library location, serial number, job or project number, description of data, date created, and expiration of retention period)**				
67.	**There is a tape retention plan (security) which permits the reconstruction of the tape file in the event that the file is inadvertently destroyed?**				
68.	**Confidential material is clearly identified and stored in locked cabinets within the library.**				
69.	**Strict accountability for copies of confidential material exists.**				
70.	**Old tapes and disks are always degaussed or blanked out before they are destroyed.**				
71.	**Sign-out logs are strictly used for material borrowed.**				
72.	**The following master tape operations are strictly adhered to:**				
	a) The old master is always retained pending run verification				
	b) The tape librarian monitors the old master to prevent misuse or premature scratching				
	c) The entire replacement operation is performed and controlled by the tape librarian				
	d) The son-father-grandfather theory is practised faithfully				
73.	**The tape library control records are always accurate and up to date.**				
74.	**The following exceptions are always identified and resolved on a timely basis:**				
	a) Tapes on loan in excess of maximum borrowing period				
	b) Tapes not located in periodic inventories				
	c) Tapes authorised for release by systems and programming but not found				
	d) Tapes for which the responsible person is not identified				

		Strongly disagree	Disagree	Agree	Strongly agree
9. COMPUTER CENTRE OPERATIONS					
75.	Computer centre operating procedures are sufficiently descriptive in detail to guide the organisation and operation.				
76.	Computer centre operating procedures are kept up-to-date				
77.	An operation log is constantly maintained to record any significant events and actions taken.				
78.	The operation log is inspected daily by management.				
79.	Computer centre personnel are the only individuals allowed to operate the machines.				
80.	Adequate and effective safeguards are exercised to ensure that only authorised persons are permitted in computer or server areas.				
81.	Computer centre personnel clearly know what to do when an unauthorised person does come into the computer centre.				
82.	Computer centre personnel know exactly what to do in the event of fire or any other emergency.				
83.	All visitors to the computer centre are escorted.				
84.	Computer centre staff are thoroughly screened before hiring.				
10. FIRE PRECAUTIONS					
85.	The computer centre personnel know exactly what to do when different types of fire emergencies occur.				
86.	All personnel at Kynoch know exactly what to do when fire emergencies occur.				
87.	Clear and adequate fire instructions are posted in all locations.				
88.	Fire alarm pull boxes and emergency power switches are clearly visible and unobstructed.				
89.	According to my opinion there are enough fire alarm pull boxes in the computer area.				
90.	Computer centre personnel are trained in fire fighting on a regular basis.				
91.	All computer centre personnel have been assigned individual responsibilities in case of fire.				
92.	Frequent fire drills are held.				
93.	The computer room has *adequate* automatic extinguishers of the				

		Strongly disagree	Disagree	Agree	Strongly agree
	following types:				
	a) Sprinklers				
	b) Carbon dioxide flooding				
	c) Halon flooding				
94.	**All extinguishers are immediately accessible and vividly marked.**				
95.	**Personnel safety precautions are adequate for when carbon dioxide or halon flooding will be used.**				
96.	**A "dry pipe" arrangement has been employed and is coupled to an appropriate fire detection system in the case of sprinklers.**				
97.	**The sprinkling can be pre-empted while personnel extinguish the fire manually (to prevent machine damage).**				
98.	**The water supply is adequate.**				
99.	**The fire detection system is adequate.**				
100.	**There are adequate smoke detectors:**				
	a) In the ceiling				
	b) In the air ducts				
	c) Under the raised floor				
101.	**The smoke detectors are tested frequently.**				
102.	**All extinguishers are checked frequently.**				
103.	**The emergency power shutdown automatically switches off the air conditioning.**				
104.	**There is adequate emergency (battery operated) lighting in the computer centre.**				
105.	**Adequate coverage of alarm stations exists on a 24-hour basis.**				
106.	**Emergency crews can gain access to the centre without delay.**				
107.	**Smoking is totally prohibited in the computer area.**				
108.	**The following combustible materials are strictly avoided in the computer area:**				
	a) Combustible curtains and rags				
	b) Flammable cleaning fluids				
	c) Paper and other supplies				

	Strongly disagree	Disagree	Agree	Strongly agree
109. The cleanliness of the computer area is adequate.				
110. Areas adjoining the computer area are suitably protected from fire.				
111. The computer centre is housed in a suitable building.				
112. The walls, doors, partitions, and floors in the computer area will resist the spread of fire.				
113. Tapes and other data storage media are always stored away from the computer room.				
114. Duplicate copies of all programs and important records are stored away from the computer area.				
115. The fire insurance is adequate.				
11. OTHER PHYSICAL DISASTERS				
116. The building is structurally sound.				
117. The building will certainly withstand high winds, floods, and earthquakes.				
118. The building is adequately protected against bomb attacks.				
119. The building and all equipment are correctly grounded for protection from damage by lightning.				
120. All overhead water and steam pipes have been eliminated (except for sprinklers).				
121. Computers are always excluded from basement areas, which might flood.				
122. The drainage system will certainly take water away from the computers.				
123. Mob action or sabotage is not probable.				
124. The computer centre has high quality self-locking doors with "panic bars" on the inside.				
125. The access control to the building by the guards is effective.				
126. The electronic access control to the building is effective.				
127. Our organisation has a good liaison with the local police.				
128. All personnel know how to handle telephone bomb threats and other disturbances.				
129. The protection from power failures and "brownouts" are adequate.				

	Strongly disagree	Disagree	Agree	Strongly agree
130. The voltage is constantly monitored with a recording voltmeter.				
131. Protection from communication line failures is adequate.				
132. Alternate means of transmission in the case of communication line failures are adequate.				
133. If the main telecommunication cable to the building fails, this will not at all effect the alternate transmission capability.				
134. All communication lines are monitored for noise, errors, and dropouts.				
135. Insurance against the following is adequate:				
a) Fire				
b) Natural disaster				
c) Water damage				
d) Power failure				
e) Fraud				
f) Crime				
g) Sabotage				
h) Errors				
136. The insurance covers all losses including loss of data and loss of business.				
12. DOCUMENTATION				
137. Clear written documentation standards have been set.				
138. The documentation standards are strictly enforced before new systems are implemented or existing ones are changed.				
13. CONTINGENCY PLANS AND BACKUP				
139. The contingency plan is effective				
140. The contingency plan has clear instructions in case of a disaster.				
141. The contingency plan does address various levels of service interruption.				
142. All vital records have been identified and classified.				
143. Procedures and responsibility assignments for action during emergencies such as fires or civil disorders are well understood by				

		Strongly disagree	Disagree	Agree	Strongly agree
	involved personnel.				
144.	A complete checklist of personnel to contact in the event of an emergency exists.				
145.	Adequate backup facilities for the provision of services are in place.				
146.	A thorough recovery plan has been developed to bring systems back into production.				
147.	Backup files are always established at proper time intervals.				
148.	An effective data base recovery system exists.				
149.	There are various levels of backup files.				
150.	Regular tests of backup are a part of normal procedures.				
151.	Adequate provision has been made for backup of data processing and support equipment, documentation, and files to permit rapid recovery of service after an emergency.				
	14. PHYSICAL SECURITY				
152.	Adequate procedures are in effect to preclude unauthorised entry by disgruntled employees or militant groups.				
153.	Access controls in the building are effectively administered.				
154.	Adequate access controls exist in the server areas.				
155.	Adequate controls over the removal of materials from the computer area exist.				
156.	Clearly defined procedures exist for disposal of confidential printed materials.				
157.	The computer area is designated as a "restricted area" where access is limited to authorised personnel.				
158.	There is an adequate control system at the entrance to the computer centre to monitor access to it.				
	15. LOGICAL ACCESS				
159.	Authorisation over all accesses and access levels can be granted and revoked.				
160.	All access violations and attempted access violations can be identified and documented.				

	Strongly disagree	Disagree	Agree	Strongly agree
16. COMPUTER VIRUSES				
161. Our organisation considers the problem of computer viruses as very serious.				
162. The following computer security measures are considered as important by our company to deal with computer viruses:				
a) A documented virus security policy				
b) Definition of potential losses				
c) Security software				
d) User controls				
e) Documented safe user practices				
f) Regular backups				
g) Compliance with security policy is a criterion in performance appraisals				
h) Insurance against losses				
i) Physical security measures				
j) Security measures for personal computers				
k) Disaster recovery plans				

	Yes	No
163. Did your company ever suffer a computer-virus attack?		
164. What, if any, were the consequences of the attack? (Please mark all appropriate items)		
a) Loss of time		
b) Loss of data		
c) Loss of functionality		
d) Specialist consultants used		
e) Employee morale affected		
f) Other consequences		

165. Which computers were affected?	
Mainframe	

	Mini	
	Micro (PC)	

166. What type of virus was it (if known)?
167. Other details of the attack
168. Any other general observations regarding information security

SECTION E

SUMMARISED INFORMATION SECURITY RATING

This section must please be completed by all participating IT personnel, departmental heads, functional heads and supervisors.

Please evaluate all questions on a four-point scale, and mark the appropriate box with an X.

PLEASE RATE THE LEVEL OF YOUR SECURITY IN CONNECTION WITH THE FOLLOWING:	Very poor	Poor	Good	Very good
PHYSICAL AND ENVIRONMENTAL SECURITY				
1. Central site				
2. Fire protection				
3. Power protection				
4. Other hazard protection				
5. Physical access				
6. After hours access				
7. Remote sites				
COMPUTER OPERATIONS				
8. Server performance monitoring				
9. Server performance standards				
10. Documented procedures				
11. Operational logging				
12. Problem logging and resolution				
13. Regular backups				
14. Training of personnel regarding emergencies				
ADMINISTRATIVE SECURITY				
15. Action plans				
16. Co-ordination of plans				
17. Employment and termination				
18. Security policies				
19. Standards				

	Very poor	Poor	Good	Very good
20. Unified IT control				
CONFIGURATION SECURITY				
21. Application software				
22. Change control				
23. Controls over local initiatives				
24. Formal systems development method				
25. Inventory				
26. Systems software				
27. Systems hardware				
DOCUMENTATION SECURITY				
28. Backups				
29. Classification schemes				
30. Disposal of sensitive documentation				
31. Protection of sensitive documentation				
32. Standards				
DATA SECURITY				
33. Access control software				
34. Access to stored data				
35. Classification scheme				
36. Consistency across environments				
37. Control of data input				
38. Database encryption				
39. Data protection				
40. Off-site backup				
41. Review of authorisations				
42. Review of exceptions				
43. Secure distribution of output				
TELECOMMUNICATIONS SECURITY				
44. Access tables kept up to date				
45. Authentication of users, messages				

	Very poor	Poor	Good	Very good
46. Control of dial-up				
47. Encryption				
48. Logging of access attempts				
49. Password management				
50. Sign-on procedures				
51. Unique user identification				
52. Use of access control packages				
MICROCOMPUTER SECURITY				
53. Audit and review				
54. Backups				
55. Central policy on acquisition				
56. Control of application development				
57. Control of data				
58. Control of proprietary software				
59. Encryption				
60. Microcomputer security policy				
CONTINGENCY PLANNING				
61. Disaster recovery plan				
62. Testing of disaster recovery plan				
63. Procedures to update plan				
64. Plan stored off-site				
65. User involvement				
66. Plan covers all environments				
67. Plan covers computer centre and network				
68. Alternative facilities/disaster recovery site				
69. Full off-site backup				
70. Resilience				
71. Continuation of work in case of a disaster				
NETWORK OPERATIONS				
72. Design and implementation standards				

	Very poor	Poor	Good	Very good
73. Resilient design				
74. Sound documentation				
75. Service-level monitoring				
76. Operations well organised				
77. Control of privileged functions				
78. Access control				
SUPPORT SERVICES SECURITY				
79. Non-disclosure agreements				
80. Supervision of support staff				
81. Supervision of visitors				
82. Couriers				
83. Photocopiers				
84. Mail room (after hours)				

What specific vulnerabilities does the organisation have regarding information security?

What impending threats does the organisation face?

What risks are associated with the threats?

What risks could be reduced if increased security countermeasures are applied?

How are these trade-offs made?

THANK YOU FOR YOUR VALUABLE TIME