A Survey of Computer-Based Information Systems Security Implemented by Large Private Manufacturing Companies in Kenya

By

OGETO VERONICA M. K.

A Management Research Project Submitted in Partial Fulfilment of the Requirements for the Degree of Masters in Business Administration, Faculty of Commerce, University of Nairobi.

DECEMBER 2004

DECLARATION

This project is my original work and has not been submitted for a degree programme in any other university.

Signed: _____ Date: 28/02/2005.

Veronica M. K. Ogeto

This research project has been submitted for examination with my approval as the University Supervisor.

Signed: _____ Date: 28th February 2005

Mr. Joel K. Lelei

Lecturer, Department of Management Science,

Faculty of Commerce

University of Nairobi

DEDICATION

I dedicate this dissertation to my father John, mother Anne, brother Pantaleo, sister Angela and my friends without whom the completion of this work would not have been possible.

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

Tables (cont..) **Page**

Figures **Page**

LIST OF ABBREVIATIONS

AV	Anti Virus
CAD	Computer Aided Design
CAM	Computer Aided Manufacturing
DoS	Denial of Service
DRP	Disaster Recovery Plan
ERP	Enterprise Resource Planning software
GDP	Gross Domestic Product
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technology
IDS	Intrusion Detection Systems
IP	Internet Protocol
IS	Information System
IT	Information Technology
LAN	Local Area Network
NIST	National Institute of Standards and Technology - America
PC	Personal Computer
PKI	Public Key Infrastructure
RMON	Remote Monitor standard / Remote network MONitoring
TCP/IP	Transmission Control Protocol/ Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

ACKNOWLEDGEMENT

I wish to express my sincere gratitude to the Faculty of Commerce, University of Nairobi, for providing me with a conducive environment within which to undertake this project in partial completion of a degree of Masters in Business Administration. Special regards go to my project supervisor, Mr. Joel K. Lelei for his guidance, encouragement and advice.

I also wish to thank Mr. Charles Onsongo and the other staff members of Research Path Associates for their friendly attitude, support and unceasing help of various kinds, which enabled me to successfully complete my project.

Special thanks go to my classmates and friends for their personal support, untiring guidance and patience during this project.

Finally, my father John, mother Anne, brother Pantaleo and sister Angela, who have been a source of inspiration, encouragement and support.

ABSTRACT

The need for computer-based information systems in manufacturing is now increasingly inevitable given that, the number of transactions is high, the customers are many and geographically widespread, and the volumes in terms of raw materials, work-in-progress and stock are very large. In such cases, the manual methods of keeping track of customers, payments, orders, stock, debtors and creditors would be very difficult, complicated and very inefficient causing manufacturing firms to be susceptible to theft amongst other vices. However, with the increased introduction of computer-based information systems, manufacturing firms are now exposed to many risks that could result in the possibility of financial loss and reputational harm. This has resulted in increased pressure on businesses to understand the need for information systems security and implement information system security measures to protect these systems; hence the need for the study on computer based information systems security within the manufacturing sector.

Past studies on information systems security in Kenya have been done with a special focus on the financial sector; these studies have shown that financial institutions in general do not have comprehensive security programmes. They tend to focus only on specific information system security aspects. These aspects include input controls only or processing controls only or hardware controls only or software controls only or output and storage controls only or procedure controls only or physical facility controls only. Few have a combination of these controls but none have all the controls.

All the above notwithstanding, it should also be noted that the information systems used by institutions in the financial sector have a different focus from those used by companies in the manufacturing sector. While the focus in financial institutions is mainly customer account management and the flow of funds, manufacturing information systems tend to focus on raw materials, work-in-progress, finished stock, order processing and invoicing. The information systems security measures are expected then to vary from industry to industry and from firm to firm. In relation to this, the importance attached to different security measures or approaches are also expected to differ, as would the challenges to implementing information system security.

Thus, what applies in one sector will not necessarily hold in another. Hence the need to research into computer based information systems security focusing specifically on manufacturing firms. With regards to the manufacturing sector, studies have been done in information systems security with a focus on manufacturing firms in the US and the UK. The results show that a majority of security professionals believe that their organisations are at risk of major cyber attack. As a result, most of the firms researched have a formal security program function in place and of those companies that have a formal security program, almost all of them have the approval of top management. However the studies also show that in comparison to the best practices of information system security, some of the firms' information system security programmes are lacking in that they do not consider all security aspects like: the importance of policies and procedures; security consideration in deploying new projects; security training and awareness for staff; monitoring, administering and evaluating security programs to determine success or failure; incident response management and contingency plans (disaster recovery plans) development and auditing.

In Kenya, most of the large private manufacturing firms have implemented different information system security measures. What these measures and their importance are, as well as the challenges faced in their implementation need to be known. It is with this in mind that this research was undertaken with the following 3 objectives: to identify information system security measures or approaches implemented in manufacturing companies in Kenya, to determine the relative importance attached to the different security measures or approaches and to identify the challenges to implementing information system security in manufacturing companies in Kenya.

To address the above objectives, data were collected from 120 large private manufacturing firms using questionnaires and analysed using various statistical tools. The sample was obtained through, first, stratified sampling on the basis of classification of manufacturing companies by industry as defined in the Directory of Industries published by the Kenya Industrial Research and Development Institute, to ensure that the final sample had representatives from each category. Then second, judgemental sampling within each stratum or category to ensure that all the sample members had computer-based information systems. Out of these 120 large private manufacturing firms, 100 responded to the questionnaires. The data collected were subjected to statistical analysis.

The findings of the study show that the majority of the large private manufacturing firms in Kenya appreciate the need for information systems security and have implemented a great number of measures or approaches which include: passwords, software licensing agreements, backup policies and procedures, different levels of access restriction, alternative power supply, virus management, email logs or filters, account deactivation of employees who have left the firm and temperature controlled room depending on the relative importance attached to the different security measures or approaches by the firm.

The study also showed that the following information systems security measures were highly ranked in terms of importance within the large private manufacturing firms in Kenya: A central policy/document core to the IS security programme, security reporting to senior management, information systems code of conduct/ethics, mechanisms to test for software fixes and proper configurations, Remote Access policies and procedures, training of employees on IS security, implementation of Disaster Recovery Plans(DRP), back up policies and procedures, procedures for destroying unneeded sensitive files, virus management processes, environmental security measures and firewalls.

Finally the main challenges to implementing information system security in manufacturing companies in Kenya were noted to be inadequate legislation governing information systems security, lack of information systems security planning, lack of training on information systems security, lack of time to develop a comprehensive information systems security program and lack of information systems security guidelines.

The development of a comprehensive information security program is recommended which should include people and technology and should involve policies, procedures, audits, monitoring, and an investment of time and money.

The study is expected to be valuable in the formulation of policy and legislation with regards to information security and assist in the enhancement of ICT based information systems security.

Some of the limitations encountered during the undertaking of this study were, first, the nature of this study required divulging security related information; as a result, some of the members in the

sample considered it too sensitive and declined to respond to the questionnaire. Second, some of those who responded may not have given the exact security position given the sensitive nature of the information. Third, the study only incorporated responses from IT managers and their assistants. Perhaps richer responses would have been obtained if the study incorporated end-user responses. Fourth, there was lack of prior adequate information on information systems security in manufacturing which would have provided a strong foundation for the study. Finally, the time constraint made it impossible to collect more diverse data and increase the sample size.

CHAPTER 1: INTRODUCTION

1.1 Background

The fundamental driving objective of a firm is ensuring its survival and profitability. Survival and profitability in the modern business environment depends on information. There is therefore a need for computer based information systems to store and process data in order to produce information for decision-making. Regardless of the enterprise's business data resident on the enterprise's computer based information systems are both valuable and vulnerable (Caelli and Shain, 1991).

Vulnerability of information systems is very critical today. The reason is that business enterprises today have extensive electronic communication pathways extending well beyond the physical bounds of the business operation. As such, the enterprise computer based information systems are exposed to both internal and external threats that can lead to disastrous results such as the loss or modification of critical business data, disruption of services and compromise of proprietary business plans or processes. Thus, there is a pressing need for information system security measures or approaches to protect the computer based information systems.

Information system security can be defined as the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources. There are different forms or measures of information system security today, and these could be grouped into five general categories. The first is access control mechanisms which include firewalls, intrusion detection systems, malicious code detection systems and virus detection systems. The second is authentication mechanisms which include biometrics, smart cards and passwords. The third is confidentiality mechanisms which include Virtual Private Networks (VPNs), encryption and cryptography. The fourth is integrity and non-repudiation mechanisms which include logging and auditing, data mining for intrusion detection and Public Key Infrastructure (PKI). And the fifth is availability mechanisms which include Denial of Service (DoS) defence, disaster recovery and contingency planning vulnerability assessment (Dykman and Davis, 1992).

Information system security can be implemented by developing and implementing effective information security program. Such programs involve policies, procedures, security measures, audits, monitoring, staff recruitment and training, disaster recovery and an investment of time and money. In order for information security programs to be effective, they should have set objectives. The objectives of an information security program are set forth in a security policy statement, which is the cornerstone of any effective program for managing and controlling an organization's information assets be it in manufacturing, airlines, finance, or other operations. (Caelli and Shain, 1991).

Organisations that are likely to implement computer based information systems require simultaneous multiple access to data, have large volumes of data that requires complex processing, access to data from multiple sources that maybe geographically spread, speed in processing and retrieval, easy reporting, accuracy especially with complex computation and measurements, quick and easy communication and sharing of resources for example printers, such include but are not limited to organisations in the following sectors transport, communication, banking, government and manufacturing.

In the manufacturing sector the number of transactions is high, the customers are many and geographically widespread, and the volumes in terms of raw materials, work-in-progress and stock are very large. The manual methods of keeping track of customers, payments, orders, stock, debtors and creditors are proving to be very difficult, complicated and inefficient. This has resulted in an increase in demand for computerisation and indeed the implementation of computer based information systems in many manufacturing firms. Computer based information systems within manufacturing firms serve both the firm and its customers. Given this wide range of end users, computer based information systems within manufacturing firms tend to be very susceptible to security breach. Thus manufacturing firms need to implement more stringent information systems security measures.

The Kenyan manufacturing firms are no exception when it comes to a need for information system security. With the target for industrialisation by 2010, various manufacturing information systems have been implemented in manufacturing firms in Kenya (Bigsten and Kimuyu, 2002). At the same time, the manufacturing sector has grown over time both in terms of its contribution

to the country's GDP and employment. Kenya has the biggest formal manufacturing sector in East Africa (Bigsten and Kimuyu, 2002). The growth has resulted in increased complexity in terms of operations due to the volumes and geographical dispersion. This in turn has resulted in an increase of demand for computerisation and therefore the introduction of information systems and the need for information system security.

Past studies by Richu (1989) and Wasilwa (2003) on information systems security in Kenya have shown that organisations in general do not have comprehensive security programmes. Organisations tend to focus only on specific information system security aspects. Such aspects include input controls only or processing controls only or hardware controls only or software controls only or output and storage controls only or procedure controls only (which include separation of duties, standard procedure and documentation, authorisation requirements and disaster recovery) or physical facility controls only (which include physical protection controls, biometric controls, telecommunications controls and computer failure controls). Few have a combination of these controls but none have all the controls.

Richu's (1989) study was undertaken with special focus on information systems security in financial institutions in Kenya, and he found that most of the information systems security risks perceived by the management of financial institutions were of a physical nature such as floods and fire. The study showed that the emphasis in terms of severity or importance in this sector was given to the four aspects of information system security. The first is physical access controls. These controls ranked the highest with most institutions incorporating mechanisms to prevent unauthorised physical access. The second were procedure controls especially those involving separation of duties to prevent key person dependency. The third were hardware controls to prevent unauthorised configuration changes and/or monitor hardware failure and the fourth were authentication mechanisms which prevent unauthorised system access by requiring some form of identification to permit access. This ranking was mainly due to past experience and vulnerability assessment carried out by the institutions. Other information systems security risks were not given sufficient considerations.

Richu (1989), also observed that further to the control aforementioned, the management in financial institutions in Kenya have integrated a selection of various information system security

approaches which include anti-virus software, e-mail logs/filters, system administrative logs, encryption, intrusion detection systems, one-time password generators (smartcards, tokens, keys) and passwords (changed every 30 or 60 days).

Wasilwa (2003) undertook a study on computer security vulnerability in the banking industry in Kenya. In the study, it was found that the major threat facing computerised security systems was the organisation's own employees. The study indicated that a 79.7% level of computer security awareness exists in the banking sector in Kenya. The study further showed that the vulnerability levels range is moderate and that most of the banks have addressed majority of the countermeasures to computer system threats effectively. Even then, the introduction of the Internet and other technological developments has resulted in greater information system security risk through the introduction of multiple entry points for information systems security breach.

Wasilwa (2003) identified the possible threats as susceptibility to: authentication, authorisations, communication technology, inter/intra network user activity, hardware failure or configuration changes, environmental hazards and fire, key person dependency, improper handling of storage media, business continuity and unauthorised physical access. Other threats that he observed include unauthorised programmatic access loss of data or software files, unauthorised information theft or disclosure, failure and instability of electrical power sources, user operator errors, software flaws and theft of system resources. Susceptibility to loss of data or software files was ranked the lowest, while susceptibility to unauthorised physical access was ranked the highest.

All the above notwithstanding, it should also be noted that the information systems used by institutions in the financial sector have a different focus from those used by companies in the manufacturing sector. While the focus in financial institutions is mainly customer account management and the flow of funds, manufacturing information systems tend to focus on raw materials, work-in-progress, finished stock, order processing and invoicing. The information systems security measures are expected then to vary from industry to industry and from firm to firm. In relation to this, the importance attached to different security measures or approaches are also expected to differ, as would the challenges to implementing information system security.

Thus what applies in one sector will not necessarily hold in another. Hence the need to research into computer based information systems focusing specifically on manufacturing firms.

An online research done by the Information Systems Security Association (ISSA) with a focus on manufacturing firms in the US and the UK shows that 65% of security professionals believe that their organisations are at risk of major cyber attack. As a result, 77% of the organisations researched have a formal security program function in place and of those companies that have a formal security program function, 96% have a function approved by top management.

The formal programs include a documented business continuity plan covering personnel and facilities and a documented disaster recovery plan regarding critical business applications and supporting technology. ISSA's findings also showed that 75% of security professionals say that their organisations are prepared to defend against a major cyber attack. It was also observed that 76% of security professionals said that the recent threats and vulnerabilities have made their organisation's capabilities to defence against a major cyber attack more secure. Finally, the research also showed that in comparison to the best practices of information system security, some manufacturing companies' information system security programmes are lacking in that they do not consider security aspects like: the importance of policies and procedures; security consideration in deploying new projects; security training and awareness for staff; monitoring, administering and evaluating security programs to determine success or failure; incident response management and contingency plans (disaster recovery plans) development and auditing.

The reasons why the aforementioned security aspects are not considered by the firms were not identified. However Pfleeger (1989), observed that generally, some of the challenges in implementing comprehensive information system security programs include, lack of funds, lack of awareness of the threats and vulnerabilities and possible countermeasures, lack of information sharing among manufacturing firms, lack of analysis and warning capabilities. Others include lack of senior management attention to information security, inadequate accountability for job and program performance related to IT security; limited security training and the fact that some aspects of information system security thought to be more critical than others are quite demanding or challenging to implement.

These and other challenges need to be addressed identified and tackled when looking at information security programs, so as to enhance information systems security in the future. As can be seen above, security is very significant with regards to information systems. Different manufacturing firms have implemented different information system security measures. What these measure are, why they were implemented and what challenges were faced or are still being faced in implementing them and others in large private manufacturing firms in Kenya are unknown. It is with this in mind that this research was undertaken to identify information system security measures or approaches implemented in manufacturing companies in Kenya, determine the relative importance attached to the different security measures or approaches and identify the challenges to implementing information system security in manufacturing companies in Kenya.

1.2 Statement of the Problem

There has been an increase in the number of manufacturing firms that are using computer-based information systems as an information resource or delivery channel for enhancing productivity. Increased reliance on computer based information systems has led to an increase in incidences of information system insecurity. This applies to Kenyan manufacturing firms which have had a number of information system security issues to contend with and the need for instituted security measures for defence. The measures adopted as expected would vary in terms of the technologies used, their complexity, their comprehensiveness, their cost and the point of implementation.

Computer-based information systems are context specific. They are specific in terms of the sector in which the information systems are used, their application and the possible threats to these systems. By extension computer-based information systems security is also context specific. Information systems in the manufacturing sector are different from information systems in other sectors in terms of their focus. Thus, while the focus in financial institutions is mainly customer account management and the flow of funds, that of manufacturing information systems tend to be on raw materials, work-in-progress, finished stock, order processing, invoicing, and so on. Generalisation across both sectors is not possible. Hence the information system security threats and the security measures applied in the financial sector may not fully help in understanding the same within the manufacturing sector.

Past researches done in Kenya by Richu (1989) and Wasilwa (2003) on information systems security focused on the financial sector. Richu did a detailed research on Security Considerations for Computer Based Financial Systems in Kenya; however, he left out new developments such as Internet technology. Wasilwa took into account vulnerability within the banks, however, what is critical and he left out is the different security measures. Also what was omitted was the importance given to the different measures and the challenges for effective information system security management.

Thus, a study on the computer-based information systems security for information systems used by manufacturing firms is needed. The study undertaken was designed to fill this gap, with the following questions being addressed: What are the various information system security measures or approaches implemented by manufacturing companies in Kenya? What is the relative importance attached to the different security measures or approaches? And finally, what are the challenges to implementing information system security in manufacturing companies in Kenya?

1.3 Objectives of the Study

The objectives of the study are:

1. To identify information system security measures or approaches implemented in large manufacturing firms in Kenya.
2. Determine the relative importance attached to the information system security measures or approaches in large manufacturing firms in Kenya.
3. Identify challenges to implementing information system security in large manufacturing firms in Kenya.

1.4 Importance of the Study

The findings of the study would be useful to several persons: firstly, information system managers will use the knowledge in enhancing their ICT based information systems security. Secondly, it will provide the government with knowledge, the basis of which can be used in the formulation of policy and legislation with regards to information security. Finally, it will provide a basis for further studies in information systems security for academics/scholars. The material obtained will make a useful contribution to theory with regards to Information System security planning and programme development, and management.

1.5 Scope of the Study

The study provides a broad overview of information system security and tries to identify various information system security measures or approaches implemented by the management in manufacturing companies in Kenya. Further, the study also tries to determine the relative importance attached to the different information security measures or approaches. Finally, the study tries to identify the challenges to implementing a comprehensive information system security program in manufacturing firms in Kenya. The study recognizes that the computer security field continues to evolve. To address changes and new issues, further continued research in this area is highly recommended.

The scope of this research comprised large private manufacturing companies operating in Kenya. The small companies were excluded. In addition manufacturing companies that fall in the public sector (predominantly government owned) were also excluded.

This study is structured into five chapters as follows: Chapter 1 is an introductory chapter and provides a background to the study, states the research problem, objectives, importance and scope of the study. Chapter 2 is devoted to a review of literature relevant to the study. First, consideration is given to the threats to information systems. Next, the components of a comprehensive information system security programme are elaborated upon. This is subsequently followed by a review of the different information system security measures or approaches. Finally, challenges to implementing a comprehensive information system security program are enumerated upon. Chapter 3 covers the research methodology. It discusses the research design, the population of the study, the sampling plan and sample size, the data collection method and finally, the data analysis techniques. Chapter 4 provides an analysis of the data collected and the interpretations. Chapter 5 gives a summary of the research findings, conclusions, recommendations made, limitations of the study and recommendations for future research.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

A computer based information system can be defined as a system that uses the resources of people, hardware, data and software to perform input, processing, output, storage and control activities that convert data resources into information products. Information systems are grouped into different classes and are derived from information needs which are related to the management functions, management levels, structure of decisions, and individual characteristics (O'Brien, 1999).

The different classes of information systems include: operational level systems which are used for day-to-day processing; knowledge, work and office systems which secure information at the knowledge level of the organisation; management information systems which provide managers with information from internal and external sources used in decision making; decision support systems aid management in making unique decisions through modelling, and executive support systems which serve the strategic level of the firm in decision making (Laudon and Laudon, 2002).

The different information systems mentioned above support business operations and processes, support decision-making and support strategies for competitive advantage of firms such as e-commerce, intranets and extranets. Given this, organisations in all sectors of the economy depend upon computer based information systems and communications networks, and share common requirements to protect sensitive information. It is important to establish secure information technology systems in order to protect the integrity, confidentiality, reliability, and availability of information (Maiwald, 2002).

ICT is being applied in manufacturing mainly to automate processes within organisations. The main forms include Enterprise Resource Planning (ERP) Software, Office Automation and Communication software, Computer Aided Design (CAD) and Computer Aided Manufacturing (CAM). ICT allows for the automation of office tasks for example report writing; facilitates communication for example email; resource management and control for example budgeting; allows for the use of Expert systems to be used to test designs (for example in Aero-dynamics,

Structural assignments); aids in quality management as CAD / CAM maintains quality and finally provides for the use of Robots to maintain production / quality (Ruthberg and Tipton, 1993).

ERPs are used for budgeting, sales order processing, invoice processing, logistics/stock control management, employee payroll, payment management – debtor and creditor payments and others. Office Automation software include Microsoft office, Word perfect which are used for functions like report writing. Communication software includes software like Microsoft Outlook, Lotus Notes, used for email, scheduling of meetings. CAD can be used to make Vector based – line drawings, can be made solid using 3D modelling, provides a walk through for architectural designs, drawing device independent, can be scaled without distortion and ensures a high degree of accuracy. CAM takes designs from CAD systems, utilises automated systems, allows fast turn round from design to manufacture, and provides internationally recognised codes. Robots can be used as sensors, as a method of processing, and as actuators to provide movement. Robots perform tirelessly, reduce labour costs, provide consistent quality of work, do not require heating or light and can work in hazardous areas. All the above notwithstanding, like all other information systems, the systems mentioned above are open to security incidents or threats (Ruthberg and Tipton, 1993).

2.2 Threats to Information Systems Security

The threats to information systems security are many and varied and will change as new safeguards are developed. The Internet by itself introduces a host of vulnerabilities that attackers can exploit – and do, on an ever-increasing basis. If a Web site is critical to a company's business operations, one security breach or attack on a computer-based information system can cause millions of dollars in downtime and lost profits. Never before has managing these threats and vulnerabilities been more crucial to the success of the business. In general, there are four kinds of information security threats: interruption, interception, modification and fabrication (Maiwald, 2002).

Interruptions include any delay or disruption of normal business operations. Computer down time caused by viruses and their removal is a very common problem today. Even just a few minutes for each employee can add up to many lost productive staff hours or staff days. *Interceptions* are any

unauthorized access to information, which may or may not result in the illicit use of data. Browsing through stored files and monitoring network or telephone transfers are considered access. *Modification* includes tampering with information once access has been achieved by changing software or hardware controls or the data itself. Think of the consequences if an intruder changed the amounts owed to a company by outside vendors. All of the billings will be incorrect and the cash flow totally disrupted. *Fabrication* means fraud and counterfeiting. It is modification in a way to benefit the intruder or to cause problems for the corporation. It can involve skilfully adding data or objects to the computing system such as transactions or additional files on a database.

The threats include but are not limited to first, software bugs which can be seen in the form of buffer overflow problems; unexpected combinations; unhandled input when somebody enters input that doesn't match the specification and race conditions which occur when two programs need to access the same data at the same time (Caelli and Shain, 1991).

Second, system configuration threats which include default configurations when systems are shipped to customers with default, easy-to-use configurations which are "easy-to-break-in"; lazy administrators who configure machines with an empty root/administrator password and hole creation when programs are configured to run in a non-secure mode (Caelli and Shain, 1991). Third, password cracking due to really weak passwords; dictionary attacks where intruders use a program that will try every possible word in the dictionary and brute force attacks where an intruder may try all possible combinations of characters (Caelli and Shain, 1991).

Fourth, sniffing unsecured traffic. On shared medium for example on traditional Ethernet, all one has do is put a sniffer on the wire to see all the traffic on a segment; server sniffing done on switched networks by installing a sniffing program on a server (especially one acting as a router), one can probably use that information to break into client machines and remote sniffing caused by equipment with RMON enabled and public community strings (Caelli and Shain, 1991).

Fifth, design flaws these include TCP/IP protocol flaws for example smurf attacks, ICMP Unreachable disconnects, IP spoofing and UNIX design flaws because there are number of

inherent flaws in the UNIX operating system that frequently lead to intrusions (Caelli and Shain, 1991).

Sixth, malicious code and virus detection systems. Malicious code is not limited to viruses, but several other types of malicious code are generally detected by anti-virus (AV) software. These other categories of malicious code include the following: worms, Trojan horses, malicious mobile code and spyware (Caelli and Shain, 1991).

Others are errors and omissions, fraud and theft, employee sabotage, loss of physical and infrastructure support, malicious hackers, industrial espionage and threats to personal privacy (Kephart and White, 1993).

2.3 A Comprehensive Information System Security Programme

The threats to information systems need to be contained. This containment is best done via an information system security programme. An information system security programme should support the mission of the organization. It is an integral element of sound management. It should be cost-effective. The individuals' responsibilities and accountability should be made explicit. It requires a comprehensive and integrated approach; and finally, should be periodically reassessed.

Whether manufacturing firms contract with third-party providers for computer services such as e-commerce, or maintain computer services in-house, the organisation's management is responsible for ensuring that systems and data are protected against risks associated with emerging technologies and computer networks. If a manufacturing company is relying on a third-party provider, management must generally understand the provider's information security program to effectively evaluate the security system's ability to protect the organisation's data.

To ensure the security of information systems and data, manufacturing firms should have a sound information security program that identifies, measures, monitors, and manages potential risk exposure. Fundamental to an effective information security program is ongoing risk assessment of threats and vulnerabilities surrounding networked and/or Internet systems. Institutions should consider the various measures available to support and enhance information

security programs. Institutions should also consider plans for responding to an information security incident.

A manufacturing company's board of directors and senior management should be aware of information security issues and be involved in developing an appropriate information security program. A comprehensive information security policy should outline a proactive and ongoing program incorporating three components: Prevention, Detection and Response (Carroll, 1995).

Prevention measures include sound security policies, well-designed system architecture, properly configured firewalls, strong authentication programs, vulnerability assessment tools and penetration analyses. Vulnerability assessment tools generally involve running scans on a system to proactively detect known vulnerabilities such as security flaws and bugs in software and hardware. These tools can also detect holes allowing unauthorized access to a network, or insiders to misuse the system. Penetration analysis involves an independent party (internal or external) testing an institution's information system security to identify (and possibly exploit) vulnerabilities in the system and surrounding processes. Using vulnerability assessment tools and performing regular penetration analyses will assist an institution in determining what security weaknesses exist in its information systems (Fitz and Kratz, 1993).

Detection measures involve analysing available information to determine if an information system has been compromised, misused, or accessed by unauthorized individuals. Detection measures may be enhanced by the use of intrusion detection systems that act as a burglar alarm, alerting the manufacturing firm or service provider to potential external break-ins or internal misuse of the system(s) being monitored.

Another key area involves preparing a response program to handle suspected intrusions and system misuse once they are detected. Organisation should have an effective incident response program outlined in a security policy that prioritises incidents, discusses appropriate responses to incidents, and establishes reporting requirements.

Before implementing prevention, detection and response measure, a firm should perform an information security risk assessment. Depending on the risk assessment, certain risk assessment

tools and practices may be appropriate. However, use of these measures should not result in decreased emphasis on information security or the need for human expertise.

A thorough and proactive risk assessment is the first step in establishing a sound security program. This is the ongoing process of evaluating threats and vulnerabilities, and establishing an appropriate risk management program to mitigate potential monetary losses and harm to an institution's reputation. Threats have the potential to harm an institution, while vulnerabilities are weaknesses that can be exploited. The extent of the information security program should be commensurate with the degree of risk associated with the firm's systems, networks, and information assets. The extent to which a firm contracts with third-party vendors will also affect the nature of the risk assessment program (Caelli and Shain, 1991).

Performing a sound risk assessment is critical to establishing an effective information security program. The risk assessment provides a framework for establishing policy guidelines and identifying the risk assessment tools and practices that may be appropriate for a firm. Manufacturing firms among other organisations, should have a written information security policy, sound security policy guidelines, and well-designed system architecture, as well as provide for physical security, employee education, and testing, as part of an effective program.

When firms contract with third-party providers for information system services, they should have a sound oversight program (Dykman and Davis, 1992). At a minimum, the security-related clauses of a written contract should define the responsibilities of both parties with respect to data confidentiality, system security, and notification procedures in the event of data or system compromise. The firm needs to conduct a sufficient analysis of the provider's security program, including how the provider uses available risk assessment tools and practices. Institutions also should obtain copies of independent penetration tests run against the provider's system.

When assessing information security products, management should be aware that many products offer a combination of risk assessment features, and can cover single or multiple operating systems. Several organizations provide independent assessments and certifications of the adequacy of computer security products (for example firewalls). While the underlying product may be certified, firms should realize that the manner in which the products are configured and

ultimately used is an integral part of the products' effectiveness. If relying on the certification, banks should understand the certification process used by the organization certifying the security product (Dykman and Davis, 1992).

Other examples of items to consider in the risk assessment process include: Identifying mission-critical information systems, and determining the effectiveness of current information security programs. For example, vulnerability might involve critical systems that are not reasonably isolated from the Internet and external access via modem. Secondly, assessing the importance and sensitivity of information, and the likelihood of outside break-ins (for example by hackers) and insider misuse of information. The assessment should identify systems that allow the transfer of funds, other assets, or sensitive data/confidential information, and review the appropriateness of access controls and other security policy settings. Thirdly, assessing the risks posed by electronic connections with business partners. The other entity may have poor access controls that could potentially lead to an indirect compromise of the manufacturing firm's system. Another example involves vendors that may be allowed to access the firm's system without proper security safeguards, such as firewalls. This could result in open access to critical information that the vendor may have "no need to know." And finally, determining legal implications and contingent liability concerns associated with any of the above.

Serious hackers, interested computer novices, dishonest vendors or competitors, disgruntled current or former employees, organized crime, or even agents of espionage pose a potential threat to a firm's computer security (Lunt, 1991). The Internet provides a wealth of information to companies and hackers alike on known security flaws in hardware and software. Hackers also may breach security by misusing vulnerability assessment tools to probe network systems, then exploiting any identified weaknesses to gain unauthorized access to a system. Internal misuse of information systems remains an ever-present security threat.

Many break-ins or insider misuses of information occur due to poor security programs. Hackers often exploit well-known weaknesses and security defects in operating systems that have not been appropriately addressed by the firm (Lunt, 1991). Inadequate maintenance and improper system design may also allow hackers to exploit a security system. New security risks arise from evolving attack methods or newly detected holes and bugs in existing software and hardware.

Also, new risks may be introduced as systems are altered or upgraded, or through the improper set-up of available security-related tools. A firm needs to stay abreast of new security threats and vulnerabilities. It is equally important to keep up to date on the latest security patches and version upgrades that are available to fix security flaws and bugs. Information security and relevant vendor Web sites contain much of this information.

Systems can be vulnerable to a variety of threats, including the misuse or theft of passwords. Hackers may use password-cracking programs to figure out poorly selected passwords. The passwords may then be used to access other parts of the system. By monitoring network traffic, unauthorized users can easily steal unencrypted passwords (Caelli and Shain, 1991). The theft of passwords is more difficult if they are encrypted. Employees or hackers may also attempt to compromise system administrator access (root access), tamper with critical files, read confidential e-mail, or initiate unauthorized e-mails or transactions.

A hacker may claim to be someone authorized to access the system such as an employee or a certain vendor or contractor. The hacker may then attempt to get a real employee to reveal user names or passwords, or even set up new computer accounts. Another threat involves the practice in which hackers use a program that automatically dials telephone numbers and searches for modem lines that bypass network firewalls and other security measures.

A few other common forms of system attack include: Firstly, Denial of Service (system failure), which is any action preventing a system from operating as intended. It may be the unauthorized destruction, modification, or delay of service. Secondly, Internet Protocol (IP) spoofing, which allows an intruder via the Internet to effectively impersonate a local system's IP address in an attempt to gain access to that system. Thirdly, Trojan horses, which are programs that contain additional (hidden) functions that usually allow malicious or unintended activities that may include replacing programs, or collecting, falsifying, or destroying data. And finally, viruses, which are computer programs that may be embedded in other code and can self-replicate resulting in either non-destructive or destructive outcomes in the host computer programs (Caelli and Shain, 1991).

2.4 Information System Security Measures or Approaches

There are different information system security mechanisms available to counter the aforementioned threats. These measures though they have been instituted by organisations worldwide, have some strengths and weaknesses which need to be considered when selecting what to implement in a particular organisational set-up. Some of these approaches to information system security are now discussed.

First, Access Control mechanisms. These include firewalls, Intrusion Detection Systems (IDSs), Malicious Code and Virus Detection Systems. Firewalls which most people think of as their first line of defence have the following benefits: they present a single IP address to the outside world, thus hiding the real structure of a network from intruders; they provide full auditing and reporting facilities; they include Virtual Private Network (VPN) technology; they are easy to configure for basic or minimal requirements; the appliances tend to be very difficult to hack, with little or no ability to store alien code, without physical access to the device. However, while firewalls protect external access, they leave the network unprotected from internal intrusions. Other limitations include: possible performance bottlenecks; security is concentrated to one location; possible leakage; insider attack vulnerabilities; configuration difficulties and cost. It has been estimated that 80% of losses due to "hackers" have been internal attacks (Dykman and Davis, 1992).

Intrusion Detection Systems (IDSs), automate the monitoring of events occurring in a computer system or network, and dynamically analyse them for signs of security problems. IDS strengths include wide product choices available, dynamic analysis and the provision of quality support for monitoring system activities. On the other hand IDS issues include scalability, manageability, interoperability is rarely possible, significant error rates, downtime and degraded network performance from IDS logging activities (Dykman and Davis, 1992).

Malicious Code and Virus Detection Systems help contain damage, but systems are vulnerable to new viruses until the signature files have been updated. Much of the new research and development in the area of virus detection is directed toward the newer behaviour-based systems, and it appears that organisations may shift to these newer systems in the next few years. Mobile

Code defence involves various approaches of examining inbound code and deciding what that code may do or access.

The strength of mobile code defence are they are complementary (both reactive signature-based Anti-Virus (AV) scanners and proactive behaviour-based AV products complement each other for a combined approach to virus protection); they offer runtime monitoring and reduced costs at the enterprise level through the use of centralized enterprise-wide AV administration to distribute updates. Current weaknesses are time gaps for virus signatures (lag time between virus generation and virus protection); increasing cost of maintaining current AV solutions; the rise of web-based services has opened an e-mail virus path around the enterprise mail AV protection and finally, the explosive growth of wireless devices is a growing concern as it has all the potential security issues and risks of the wired Internet as well as the additional risks caused by mobility and the broadcast nature of wireless transmissions (Dykman and Davis, 1992).

Second, Authentication mechanisms which include Biometrics and Smart Cards. Biometrics use physiological or behavioural characteristics to distinguish one person from another. Its current strengths include availability, since these characteristics are tightly bound to the person, they cannot be lost, stolen, forgotten, or loaned; improved accountability in audit trails and reduced cost in related areas like password management and related overhead costs. Its weaknesses include system cost in some technologies still high; privacy and personal concerns, especially of consumers, result in opposition to biometrics; errors caused by time and environmental conditions; accuracy not guaranteed; and compromised traits means that the original owner/user can no longer use that trait on that system, or any similar system, for life (Ruthberg and Tipton, 1993).

Smart Cards strengths include Access Control, they enable the verification of a cardholder's identity to permit access to physical sites, networks, individual computers and accounts; can store data used for relationship management for example differentiated servicing, targeted marketing, and loyalty point programs; can keep record of transactions on card convenience; renewability since their cryptographic keys and/or algorithms can be changed as required and fraud reduction. Their weaknesses include additional costs for installing card readers and software on all client machines; environmental vulnerabilities like static electricity, magnetic

fields, temperature, and ultraviolet light; privacy issue like tracking the movements of users, storing their private information, and sharing data among data owners (across organizations) and operational reliability since smart cards are tamper resistant, but not tamper proof. Passwords which though easy to implement can be cracked or shared (Ruthberg and Tipton, 1993).

Third, Confidentiality mechanisms which include Virtual Private Networks, encryption and cryptography. Virtual Private Networks (VPNs), provide improved connectivity, efficient access, very flexible and cost-effective means for secure, private communications without leasing or managing dedicated lines. However, there are issues of scalability with many nodes, managing keys and certificates, interoperability, not suitable for links that have high rates of flap (on-off communication) or sporadic delay (for example microwave/satellite), has a potential for excessive control traffic clogging WAN links and performance degradation (Ruthberg et al, 2000).

Encryption and cryptography are becoming increasingly popular. Their strengths include algorithms are fairly well understood and associated protocols are also fairly well understood, cryptographic techniques are extremely powerful and useful in enabling security technologies. However, these techniques are difficult to grasp and incorrect decisions may create large risks. Other issues include the strength of the algorithms varies, details are very critical, key distribution and management is tedious, standards and the compatibility between algorithms and implementations from different vendors, product quality varies, patent and trademark issues (Ruthberg et al, 2000).

Fourth, Integrity and Non-Repudiation mechanism, which include logging and auditing, data mining for intrusion detection and Public Key Infrastructure. Logging and auditing can sometimes serve as a deterrent. While still reactive and after-the-fact, today's logging and auditing tools have greatly increased capabilities of data collection and reporting. The usefulness of logging and auditing also extends to network management application processes running on intermediate systems such as routers and switches as well as network management workstations. The massive amounts of data that are, and can be, collected create issues of storage space and difficulty of analysis, log files are vulnerable to modification or destruction and auditing is a reactive rather than a proactive tool (NIST's CSL Bulletin series, 2002).

Data mining evaluates data without previously formulated hypotheses in order to discover or gain new insights that might not be apparent from traditional examination or analysis. Data mining has strong data reduction and discovery capabilities, and can be used to evaluate intrusion detection systems and logging and auditing data. The potential may be there for data mining to move from being a post-event reactive tool to one with predictive capability. However, data selection, preparation, storage, quality and accuracy, along with computing time, costs, Speed or availability of results are issues that must be overcome to reach that potential (NIST's CSL Bulletin series, 2002).

Public Key Infrastructure (PKI) provides security services for enterprise resources. The use of public keys has potential for enabling e-commerce on a large scale and creates flexibility because secure communications can take place without prior arrangement. Key management is a considerable effort, and the development and management of the necessary infrastructure for PKI is still a significant challenge (NIST's CSL Bulletin series, 2002).

Fifth, Availability mechanisms which include Denial of Service (DoS) defence, disaster recovery, contingency planning and vulnerability assessment. Denial of Service (DoS) defence strengths include: best practices and the software is widely available. However, the issues include interdependency because the security of any network on the internet depends on the security of every other network; variety of attacks: hardware, software, and the network can all be attacked, which requires multiple defences to be in place; speed of attacks can be fast; mutations are easily and quickly created and multiple defences are needed (NIST's CSL Bulletin series, 2002).

Disaster Recovery and Contingency Planning is essential for mitigating the impact of a disaster or to prevent it from happening in the first place. There are many resources available for obtaining guidance and direct support, and a peripheral benefit is a better understanding of the organization. This effort does require continual evaluation, revision, and testing to meet its intended goals (NIST's CSL Bulletin series, 2002).

Vulnerability assessment is a discovery process to try to identify weaknesses in a system's security scheme in order to reduce or better manage any associated risk. Vulnerability

assessment provide system administrators with the ability to assess the risk level of all systems that have agents loaded; provides a good way to determine the state of the network; is easy to install and try out and it can be run on a wide variety of attacks on a network and determine the network resilience to each attack. Its issues are: it is a host-based product and requires agent installation on a large majority of systems; it takes a snapshot of a network and does not provide a real time solution and finally a 100%-availability hot site can nearly double an organization's computing budget (NIST's *CSL Bulletin* series, 2002).

2.5 Challenges to Implementing a Comprehensive IS Security Program

Manufacturing firms are aware of the importance of securing their critical infrastructures. Although the actions taken to date are major steps to more effectively protect their organisation's critical infrastructures, there are a number of challenges already identified and recommendations made.

For each of these challenges, improvements have been made and continuing efforts are in progress. However, even greater efforts are needed to address them. According to the GAO report number GAO-03-564, the challenges faced by organisations in general include the following: firstly, developing a comprehensive information system security program. More complete programs are needed that will address specific roles, responsibilities, and relationships for all entities; clearly defining interim objectives and milestones; setting time frames for achieving objectives; and establishing performance measures. Secondly, improving information sharing on threats and vulnerabilities. Information sharing is a key element in developing comprehensive and practical approaches to defending against cyber and physical attacks, which could threaten the organisation's welfare. Information sharing needs to be enhanced both within the organisations and between organisations in the same sector.

Thirdly, improving analysis and warning capabilities. More robust analysis and warning capabilities, including an effective methodology for strategic analysis and framework for collecting needed threat and vulnerability information, are still needed to identify threats and provide timely warnings. Such capabilities need to address both cyber and physical threats. Fourthly, lack of senior management attention to information security. Management should be involved in information security program development, implementation and review. Fifth,

inadequate accountability for job and program performance related to IT security. Proper job descriptions should be developed with roles and responsibilities clearly defined. These should be used to review employee performance. Proper mechanisms should be put into place to facilitate periodic, comprehensive information system security program review/assessment.

Sixth, limited security training for general users, IT professionals, and security professionals. Regular comprehensive training programs should be developed for all involved with the necessary level of detail. Seventh, inadequate integration of security into the capital planning and investment control process; poor security for contractor-provided services. Proper planning and budgeting should be done for information system security planning. Eighth, limited capability to detect, report, and share information on vulnerabilities or to detect intrusions, suspected intrusions, or virus infections. Installation of the available tools and systems to assist in detection and reporting these possible threats and finally, some aspects of information system security thought to be more critical than others are quite demanding or challenging to implement. Forums should be created where ideas can be shared on how to implement certain countermeasures that are difficult or complex to implement.

The primary goal of an information security program is to manage risk to information and information systems. The program's plan is to develop ways to lower current risk through administrative, environmental/physical and technical measures. The challenge is identifying risks, ranking them by severity, deciding on a way to manage them. There is a multiphased approach to an information security program. It includes assessing risk, establishing policies, deploying countermeasures to risk, educating the population regarding the risks and solutions, and monitoring and reporting on the progress of the program. This is highly recommended.

CHAPTER 3: STUDY METHODOLOGY

3.1 Research Design

The research design used for the study was exploratory. Such a study design was used because it gives preliminary knowledge in the security of computer-based information systems in manufacturing companies in Kenya.

3.2 Population of the Study

The population for this study comprised all large, private manufacturing companies operating in Kenya. Public sector, small and medium manufacturing companies were excluded from this study. Public sector refers to those companies in which the government holds majority shares and co-operative societies.

A criterion adapted by Aosa (1992) was used to define the size of a company, so as to determine whether it was large or small. Aosa defined the size of a company on the basis of three criteria: number of employees, total turnover and turnover per an employee. He then set threshold values for these criteria to help determine the size of a manufacturing company. To qualify for large, the company had to have: 50 or more employees; have a total sales turnover of at least Kshs 3,000,000 per annum and finally, have sales turnover per employee of at least Kshs 60,000 per annum.

This criterion was deemed to be adequate for the study to be undertaken, because it is a combination of the three most widely used measurement parameters which have been used by different researchers worldwide to classify or categorise companies based on their size (Aosa, 1992).

The sampling frame was constructed from 3 different registers (directories) of manufacturers, so as to be exhaustive:

1) The Directory of Industries published by the Kenya Industrial Research and Development Institute (KIRDI) (1997).

2) The Register of Industries, Ministry of Industry (1988).

3) The Members' List of the Kenya Association of Manufacturers (2002).

By using the three directories, the researcher was able to come up with a list that included as many firms as possible to ensure that the sample was drawn from as conclusive a population as possible. In total, about 650 companies were expected. From these companies, the Public sector companies, small companies and those that have been closed or that have identifiable multiple entries were excluded. This left a total of 200 companies from which a sample was drawn.

3.3 Sampling

Firstly, stratified sampling was used on the basis of classification of manufacturing companies by industry as defined in the Directory of Industries published by the Kenya Industrial Research and Development Institute. KIRDI classification was used because it is comprehensive and is accepted by manufacturing firms in Kenya as being comprehensive.

The KIRDI Directory classifies Manufacturing Companies by Industry as follows:

- Building
- Medical and Hospital
- Engineering and Electrical
- Food, Beverages and Tobacco
- Textile, weaving apparel and leather industries
- Wood and Wood products
- Paper products, Printing and Publishing
- Chemical Petroleum, Rubber and Plastic Products
- Non-Metallic mineral products
- Fabricated metal products, machinery and equipment
- Other manufacturing Industries

The use of KIRDI's classification of manufacturing companies by industry ensured that the final sample had representatives from each category. Then judgemental sampling was applied within each stratum or category to select firms with computer based information systems. This way, manufacturing companies without computer-based information systems were excluded from the study.

The sample size selected was 120 Large Private Manufacturing firms; this is because the number was manageable given time and cost constraints. The firms selected were large private manufacturing firms with headquarters in Nairobi. The firms within Nairobi were selected because they were easily within reach. Further, it is in Nairobi that the ICT policy guidelines are set on the company's practice, for firms with headquarters in Nairobi.

Appendix 1 shows a list of the manufacturing firms that were sampled.

3.4 Data Collection Method

The information required for the study was collected using a questionnaire. The questionnaire comprised both open-ended and close-ended questions. Questions were developed after the study of literature, brainstorming, reviewing class notes and past projects in information systems security.

The questionnaire shown in Appendix 3 is divided into four sections. Section A was used to collect demographical data, identify systems in operation, and identify various information system security threats experienced by manufacturing firms in Kenya. Section B was used to identify countermeasures or approaches undertaken by manufacturing firms in Kenya, in comparison to the best practices of information system security. Section C was used to collect data on the relative importance attached to the different types of security measures or approaches. And finally, Section D was used to collect data on the challenges in implementing a comprehensive information system security program in manufacturing firms in Kenya.

The questionnaire was administered through the 'drop and pick-later' method. The questionnaire was administered to the Information Systems/ Information Technology managers or their appointed assistants who with the managers were expected to have the knowledge being sought and they could fill it in at their own convenience in terms of time.

3.5 Data Analysis Techniques

In Sections A and B, data collected was analysed through the use of descriptive statistics such as frequency tables, proportions, percentages and measure of relative position. The purpose of this analysis was to establish whether there were any similarities amongst information systems

security measures implemented by the manufacturing firms and secondly to establish whether the demographic factors had any impact on information systems security measures implemented by the manufacturing firms.

In Section C and D, data collected was analysed through the use of factor analysis. The general objective of factor analysis was to summarise a (large) set of the variables by creating a smaller number of variates or factors that are defined in the terms of the original variables. This small number of variates is derived such that the maximum amount of information available in the original variables is retained in the smaller number of factors. The findings in respect to Sections C and D were subjected to this analysis in view of the numbers of variables. The purpose of this analysis was to establish the most important information systems security measures from the respondents' point of view and thereafter to establish the most common challenges from the respondents' point of view that are encountered by large private manufacturing firms as they implement information systems security measures.

Further analysis was performed on the basis of key demographic factors like number of branches, number of employees, turnover. These were then used to profile the respondents.

CHAPTER 4: DATA ANALYSIS AND FINDINGS

4.1 Introduction

This chapter presents the results of the analysis and findings of the study. A total of 120 questionnaires were distributed as indicated in the Table 4.1. Questionnaires were distributed to the sample that had representatives from each manufacturing industry/class to ensure that the results would be rich and truly representative of all the large private manufacturing firms in Kenya. Out of these, 100 were successfully completed and returned. The final sample of 100 firms was broadly representative of the population of large private manufacturing firms in Kenya. The 100 successfully completed and returned questionnaires, represent an overall response rate of 82%. This represents a very good response rate since more than 80% of the questionnaires were returned given the sensitive nature of the information gathered. These were used as the basis for the data analysis and the findings of the study.

Table 4.1 Classification of manufacturing companies by industry, KIRDI

Classification By Industry	Number of questionnaires issued	Number returned and usable	Percentage Response Rate
Building	11	8	73%
Medical and Hospital	11	10	90%
Engineering and Electrical	11	10	90%
Food, Beverages and Tobacco	11	10	90%
Textile, weaving apparel and leather industries	11	10	90%
Wood and Wood products	11	8	73%
Paper products, Printing and Publishing	11	10	90%
Chemical Petroleum, Rubber and Plastic Products	11	10	90%
Non-Metallic mineral products	11	10	90%
Fabricated metal products, machinery and equipment	11	10	90%
Other manufacturing Industries	10	4	40%
TOTAL	**120**	**100**	**82%**

4.2 Demographic Characteristics

The demographic characteristics of the sample, which include ownership of the firms, numbers of years the firms have been in operation, number of customers, number of employees, number of branches and total average turnover are summarised in this section. This demographical information provides an invaluable basis for understanding the general characteristics of manufacturing sector and will aid in determining whether or not demographic factors affect the implementation of computer based information systems security measures.

4.2.1 Ownership of Organisation

The respondent's firms were analysed in terms of ownership. This was aimed at establishing the ownership of the respondent firms. Table 4.2.1 indicates that 52% of the manufacturing firms are wholly locally owned, while the rest (48%) are split almost 50-50 between wholly foreign owned and jointly owned.

Table 4.2.1 Ownership of Organisation

Ownership of organisation		Frequency	Percent
	Wholly foreign owned	23	23.0
	Wholly locally owned	52	52.0
	Jointly owned	25	25.0
	Total	100	100.0

Thus it can be seen that the ownership of the large private manufacturing firms number is not a factor in the implementation of computer based information systems and their security measures, since all the firms have computer based information systems.

4.2.2 Years of Operation of Respondent Firms

The number of years of operation of the respondent firms ranged from 0 to over 50. The results in Table 4.2.2 indicate that 10-19 years category had the highest number of respondents, 25%, followed by the over 50 years category which had 20% of the respondents.

Table 4.2.2 Years of Operation of Respondent Firms

Years of operation		Frequency	Percent
	0-9 years	11	11.0
	10-19 years	25	25.0
	20-29 years	12	12.0
	30-39 years	16	16.0
	40-49 years	15	15.0
	Over 50 years	20	20.0
	Not stated	1	1.0
	Total	100	100.0

The distribution was fairly uniform and yet they all have computer based information systems. Thus it can be seen that the number of years of operation is not a factor in the implementation of computer based information systems and their security measures, since all the firms have computer based information systems.

4.2.3 Number of Customers

The results in Table 4.2.3 indicate that 43% of the respondents have over 2,001 customers.

Table 4.2.3 Number of Customers

Number of customers		Frequency	Percent
	0-400	26	26.0
	401-800	7	7.0
	801-1200	2	2.0
	1201-1600	2	2.0
	1601-2000	11	11.0
	Over 2001	43	43.0
	Not stated	9	9.0
	Total	100	100.0

As can be seen the number of customer is an important factor in the implementation of computer based information systems since the larger the customer base the greater the need to implement computer based information systems to handle the large volume of customer information and information systems security measures to protect these systems. It is also an indication of how important or core to the manufacturing firm's operations the computer based information systems are that keep all the customer data.

4.2.4 Number of Employees

The respondent firms were analysed in terms of number of employees. The results in Table 4.2.4 indicate that 25% of the respondents have between 51 and 100 employees and 37% have over 200 employees.

Table 4.2.4 Number of Employees

Number of employees		Frequency	Percent
	1-50 employees	18	18.0
	51-100 employees	25	25.0
	101-150 employees	14	14.0
	151-200 employees	5	5.0
	Over 200	37	37.0
	Not stated	1	1.0
	Total	100	100.0

Thus it can be seen that the number of employees is not a factor in the implementation of computer based information systems and their security measures, since all the firms have computer based information systems and also have a varying number of employees.

4.2.5 Number of Branches

Table 4.2.5 shows that majority (74%) of the respondent firms have only one branch.

Table 4.2.5 Number of Branches

Number of Branches		Frequency	Percent
	One branch	74	74.0
	2-5 branches	15	15.0
	6-9 branches	4	4.0
	Over 10 branches	4	4.0
	Not stated	3	3.0
	Total	100	100.0

As a result, the number of branches is not an important factor in the implementation of computer based information systems since all the respondents have computer based information systems and yet the majority (74%) have only one branch. However, it is worth noting that as a result of this, information system security risks brought about by having Wide Area Networks are minimal in this sector and thus information systems security measures should also be concentrated greatly towards this with some flexibility for growth to cover Wide Area Networks as the firms grow and open more branches.

4.2.6 Total Average Turnover

The results in Table 4.2.6 indicate that 52% of the respondents have a total average annual income of between 0-100 million.

Table 4.2.6 Total Average Annual Income

Total average annual income		Frequency	Percent
	0-100 million	52	52.0
	between 100 million and 1 billion	10	10.0
	between 1 and 4 billion	8	8.0
	over 4 billion	11	11.0
	Not stated	19	19.0
	Total	100	100.0

The manufacturing sector has grown over time both in terms of its contribution to the country's GDP and employment. The results indicate that the firms will have more money to invest in information systems, which also means the introduction of the need for information system security.

4.3 Analysis of IT Resources in the Organisation

The analysis of IT resources in the firms are summarised in this section. This analysis indicates the general characteristics of the organisations in relation to information systems in operation and will aid in a better understanding of the firms from an IT perspective and in determining whether or not these IT factors affect the implementation of computer based information systems security measures.

4.3.1 Level of Computer-Based Information system Utilization

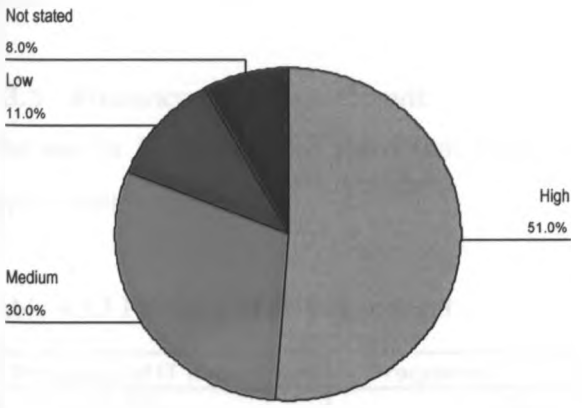
The results in Table 4.3.1 indicate that most of the respondents (51%) have a high level of computer-based information systems utilisation.

Table 4.3.1 Level of computer-based information utilization

Level of computer-based information utilization		Frequency	Percent
	High	51	51.0
	Medium	30	30.0
	Low	11	11.0
	Not stated	8	8.0
	Total	100	100.0

This indicates that the manufacturing firms have seen the value of IS/IT in computerising activities within the firms and thus also see the value in protecting these systems through the implementation of information systems security measures.

Figure 4.3.1 Level of computer-based information utilization



4.3.2 Computerised Functions Within the Organisation

An analysis of the functions computerised within large private manufacturing firms as shown in Table 4.3.2 indicated the following: 88% of the respondents have computerised their payroll, 86% of the respondents have computerised their stock ordering, 82% of the respondents have computerised their customer base management, 80% of the respondents have computerised their supplier base management, 81% of the respondents have computerised their payments management and 87% of the respondents have computerised their invoicing.

Table 4.3.2 Computerised Functions Within the Organisation

Computerized functions within the organization	Frequency	Percent
Computerized Payroll	88	88.0
Computerized Stock ordering	86	86.0
Customer base management	82	82.0
Supplier base management	80	80.0
Payments management	81	81.0
Invoicing	87	87.0
Computer Aided Design	20	20.0
Computer Aided Manufacturing	33	33.0
Royalties and typesetting	2	2.0
Elementary accounting	14	14.0
Distribution	9	9.0
Product service	19	19.0

These results indicate the most popular computerised functions, which are also very critical to the firms' operations. The results show a heavy use and dependence on computer based information systems within this sector and thus the need to protect these critical systems through the introduction of information systems security measures which most of the firms have already done.

4.3.3 Presence of IT Department

The results in Table 4.3.3 show that 83% of the respondents indicated that they have an IT department.

Table 4.3.3 Presence of IT Department

Presence of IT department		Frequency	Percent
	Yes	83	83.0
	None	17	17.0
	Total	100	100.0

This is a clear indication that the need for computing experts on-site to manage the computer based information systems and the information systems security measures has taken root across the manufacturing industry.

4.3.4 IT Department Position

The results in Table 4.3.4 indicate that 56% of the respondents said that the IT department was under the Finance department while only 21% of the respondents indicated that it was independent.

Table 4.3.4 IT Department Position

Position of IT deparment		Frequency	Percent
	Finance	56	56.0
	Independent	21	21.0
	Not stated	23	23.0
	Total	100	100.0

This shows that the level of importance given to the IT department is low as it is not seen as a separate entity but as a subset of Finance and may not be represented at the Board level. As a result, this may also impact on the introduction of the computer based information systems and their security measures.

4.3.5 IT Department Budget

The results in Table 4.3.5 indicate that 54% of the respondent firms have a separate IT budget while 34% do not.

Table 4.3.5 IT Department Budget

Organisation has Budget for IT department		Frequency	Percent
	Yes	54	54.0
	No	34	34.0
	Not stated	12	12.0
	Total	100	100.0

This indicates that organisations have put a lot of resources tied up in computer systems and hence the need to keep them secure through implementation of information systems security measures.

4.3.6 Ownership of the Information Systems Components

The results in Table 4.3.6 show that 50% of the respondents indicated that the ownership of hardware is in-house; with regards to software, 38% of the respondents indicated that the ownership is both in-house and outsourced; with regards to operations, 63% of the respondents indicated that the ownership is in-house only and with regards to preventive maintenance, 38% of the respondents indicated that the ownership is outsourced only.

Table 4.3.6 Ownership of the Information Systems Components

	In-House only		Out-Sourced		Both		Not stated	
Ownership of IS components	Frequency	Percent	Frequency	Percent	Frequency	Percent	Frequency	Percent
Hardware	50	50.0	11	11.0	25	25.0	14	14.0
Software	35	35.0	13	13.0	38	38.0	14	14.0
Operations	63	63.0	5	5.0	18	18.0	14	14.0
Preventive Maintenance	20	20.0	38	38.0	18	18.0	24	24.0

This indicates that most of the respondent firms prefer to own the hardware and perform the operations internally, while outsourcing preventive maintenance. Software however has an even spread with almost the same number of firms choosing to own while others choose both to own and to outsource. This analysis is important because outsourcing it means additional information systems security measures have to be in place to reduce risk brought about by third parties (for example preventive maintenance firms).

4.3.7 Types of Computer Networks in use

The results in Table 4.3.7 show that 98% of the respondents have a Local Area Network, very few have standalone computers. Only 46% of the respondents have a Wide Area Network since very few of the respondent firms have more than one branch. 85% of the respondents do not have wireless network services this could be because it is a new phenomenon and has not yet been widely adopted. The analysis also shows that 81% of the respondent companies indicated that they have access to the Internet and 50% of the respondents have an Intranet. This is a good indication in the sense that apart from providing the benefits of ICT to their staff, more than 50% of the firms are working towards leveraging of this technology from a business perspective for example e-commerce. However it should also be noted that these types of computer networks also create an additional avenue for information system security breach. The results also show that 68% of the respondents do not have an extranet. This maybe because they are not fully

aware of the benefits of an extranet which can be used to communicate with suppliers, customer and others external parties.

Table 4.3.7 Types of Computer Networks in use

	In use		Not in use	
Types of computer networks in the organization	Frequency	Percent	Frequency	Percent
Local area network (LAN)	98	98.0	2	2.0
Wide area network (WAN)	46	46.0	54	54.0
Wireless Network (e.g. 802.11)	15	15.0	85	85.0
Internet	81	81.0	19	19.0
Intranet	50	50.0	50	50.0
Extranet	32	32.0	68	68.0
Stand-alone PCs (Not on LAN)	10	10.0	90	90.0
Macs Network	2	2.0	98	98.0

4.3.8 Methods of Processing

With regards to methods of processing, the results in Table 4.3.8 indicate that 53% of the respondents have batch processing. This means that most manufacturing firms process transactions in a batch manner and only few transactions are processes online and even fewer are done real-time. Thus majority of the information systems security risks will be related to batch processing, subsequently, information system security measures implemented should focus on the same.

Table 4.3.8 Methods of Processing

Methods of processing in use (Online but not real time)	Frequency	Percent
Online but not real time	25	25.0
Real time online	39	39.0
Batch	53	53.0

4.3.9 Types of Access to Networks

With regards to types of access to networks, the results in Table 4.3.9 indicate that, there is an almost 50-50 split between those that provide remote dial-in access and those that do not. Of the respondent firms 79% support access to the network through the Internet this creates an additional avenue for information system security breach. This shows that there is increased information systems security threat since the firms permit access to their networks from external points. However, the results also show that 98% do not support or even have Virtual Private

Networks (VPNs), which is an indication that very few of the firms recognise the importance of a VPN and how secure it is if well designed and implemented.

Table 4.3.9 Types of Access to Networks

Types of access networks supported by Information System in the organization	Frequency	Percent
Remote dial-in access	51	51.0
Internet access	79	79.0
VIA VPN Access or VPN Dial Up	2	2.0

4.3.10 Rating of Computer Literacy Among Staff

The results in Table 4.3.10 indicate that 44% of the respondents rated their CEO computer literacy level as average. 48% of the respondents rated their top management computer literacy level as average. 48% of the respondents rated their middle management computer literacy level as above average. 44% of the respondents rated their lower management computer literacy level as above average. 44% of the respondents rated their other staff computer literacy level as poor.

Table 4.3.10 Rating of Computer Literacy Among Staff

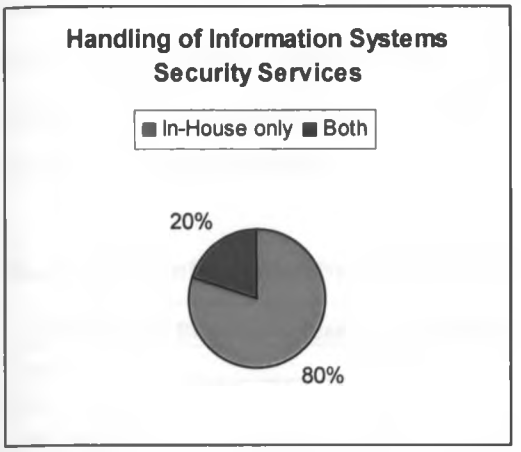
Rating of computer literacy among staff	Poor	Below Average	Average	Above Average	Excellent
Executive Director (CEO)	2.0	14.0	44.0	22.0	18.0
Top Management	0.0	16.0	48.0	25.0	11.0
Middle Management	14.0	0.0	29.0	48.0	9.0
Lower Management	16.0	20.0	13.0	44.0	7.0
Other Staff	44.0	11.0	16.0	13.0	16.0

This means that computer literacy is concentrated within management and majority of the other staff tend to be neglected. This indicates a gap or need for training so as to reduce the risk of information systems security breach due to lack of knowledge on the use of information systems and possible risks or threats.

4.3.11 Handling of Information systems security services

The results in figure 4.3.11 show that 80% of the respondents prefer to handle information systems security services in-house. While only 20% prefer to have it partial handled in-house and partially out-sourced. None of the respondents have their information systems security services purely outsourced. This maybe because information systems security is a sensitive area and most firms prefer to either develop internal competence or only outsource partially.

Figure 4.3.11 Handling of Information Systems Security Services



4.3.12 Information Systems Security Policy

The results in Table 4.3.12 show that 62% of the respondent firms indicated that they have a written and formal computer security policy. This is a clear indication that the manufacturing firms are serious about informing the staff on issues related to information systems security.

Table 4.3.12 Information Systems Security Policy

Presence of information systems security policy		Frequency	Percent
	Yes	62	62.0
	No	38	38.0
	Total	100	100.0

4.3.13 Information Systems Security Policy Update

The results in Table 4.3.13 show that the frequency of security reviews varies with 13% of the respondent firms preferring monthly review, 12% quarterly reviews, 8% semi-annual reviews and annual reviews 29%. Thus the review of security aspects is a matter of internal policy, although it is done at least once a year. However it is positive to observe that the policies are reviewed and updated at least once a year by most of the respondent manufacturing firms.

Table 4.3.13 Information Systems Security Policy Update

Frequency of updating information system security policy		Frequency	Percent
	Monthly	13	13.0
	Quarterly	12	12.0
	Semi-Annually	8	8.0
	Annually	29	29.0
	Not applicable	38	38.0
	Total	100	100.0

4.3.14 Information Systems Security Team or Department

The results in Table 4.3.14 show that 59% of the respondent firms indicated that they have an information system security team. This is a clear indication that the manufacturing firms are serious about the information systems security and have a team in place to implement and monitor security measures.

Table 4.3.14 Information Systems Security Team or Department

Presence of IS security team or department	Frequency	Percent
Yes	59	59.0
No	37	37.0
Not stated	4	4.0
Total	100	100.0

4.3.15 Composition of IS Security Team or Department

The results in Table 4.3.15 show that 69% of the respondent firms do not have members of other business departments in the information systems security team. As a result, their invaluable input is missing. This is a gap that needs to be addressed.

Table 4.3.15 Composition of Information Systems Security Team or Department

Inclusion of members of other business units/ department in IS security team	Frequency	Percent
Yes	25	25.0
No	69	69.0
Not stated	6	6.0
Total	100	100.0

4.3.16 Job Descriptions for IS Security Team Members

The results in Table 4.3.16 show that 53% of the respondents indicated that they job descriptions for information systems security team members. This is a small numbers. In order to have an effective information systems security team, the members need clear job descriptions so that they know their roles and functions. This needs to be addressed by manufacturing firms.

Table 4.3.16 Job Descriptions for IS Security Team Members

Whether IS security team members have specific job descriptions	Frequency	Percent
Yes	53	53.0
No	41	41.0
Not stated	6	6.0
Total	100	100.0

4.3.17 Information Systems Security Team Budget

The results in Table 4.3.17 show that 72% of the respondents indicated that they do not have information systems security budget arrangements. This is an obstacle because in order to implement efficient and effective information systems security measures, money is needed. This needs to be addressed by manufacturing firms so that a portion of the IT budget can be allocated to information systems security.

Table 4.3.17 Information Systems Security Team Budget

Budget allocation for IS security team	Frequency	Percent
Yes	22	22.0
No	72	72.0
Not stated	6	6.0
Total	100	100.0

4.3.18 Information Systems Code of Conduct/Ethics

The results in Table 4.3.18 show that 65% of the respondents indicated that they have an information systems code of conduct. This is good. This is a clear indication that the manufacturing firms are serious about information systems and have a code of conduct/ethics to guide employees on the dos and don'ts on the use of information systems the awareness of which is a form of information security.

Table 4.3.18 Information Systems Code of Conduct/Ethics

Does organisation have IS code of conduct		Frequency	Percent
	Yes	65	65.0
	No	30	30.0
	Not stated	5	5.0
	Total	100	100.0

4.3.19 Information Systems Code of Conduct/Ethics covers IS Security

The results in Table 4.3.19 show that 65% of the respondents indicated that they have an information systems code of conduct which covers security. This is good. This is a clear indication that the manufacturing firms are serious about information systems security and have included it in the information systems code of conduct/ethics to guide employees on the dos and don'ts on the use of information systems and the implementation of information systems security.

Table 4.3.19 Information Systems Code of Conduct/Ethics covers IS Security

Does code of conduct cover IS security		Frequency	Percent
	Yes	65	65.0
	No	24	24.0
	Not stated	11	11.0
	Total	100	100.0

4.3.20 Information Systems Assessment

The results in Table 4.3.20 show that 58% of the respondents indicated that their information systems are assessed. This shows that only half of the large private manufacturing firms have seen the value of assessing their information systems, while the other half have not. This is not good as the firms that do not assess their information systems on a regular basis tend to be more vulnerable to information systems security threats since the threats are ever changing and new ones keep developing with the ever changing technology.

Table 4.3.20 Information Systems Assessment

Assessing of organisation's IS		Frequency	Percent
	Yes	58	58.0
	No	34	34.0
	Not stated	8	8.0
	Total	100	100.0

4.3.21 Frequency of Information Systems Assessment

The results in Table 4.3.21 show that the frequency of information systems assessment varies with 15% assessing them monthly, 13% quarterly, 16% semi-annually and 14% annually. Of the total number of respondents, 42% did not indicate.

Table 4.3.21 Frequency of Information Systems Assessment

How often IS are assessed		Frequency	Percent
	Monthly	15	15.0
	Quarterly	13	13.0
	Semi-Annually	16	16.0
	Annually	14	14.0
	Not applicable	42	42.0
	Total	100	100.0

Thus the review of information systems is a matter of internal policy, although it is done at least once a year.

The assessment of information systems is an important aspect of information systems security since new loopholes can be determined and addressed.

4.3.22 Information Systems Assessment Conduction

The results in Table 4.3.22 show that 29% of the respondents stated that the assessment is mainly done by both in-house and third party organisations in combination while 20% stated in-house alone. Very few firms have assessment being undertaken by third-party firms only. This is because most firms believe that information systems assessment is a critical and confidential process, which is key to the information systems security.

Table 4.3.22 Information Systems Assessment Conduction

Who does assessment		Frequency	Percent
	In-House	20	20.0
	Third-party organisations	7	7.0
	Both	29	29.0
	Not stated	2	2.0
	Not applicable	42	42.0
	Total	100	100.0

4.4 Identifying Countermeasures to IS Security Threats

The analysis in this section identifies the countermeasures or information systems security measures put in place to curb information systems security threats and lower the level of risk. This section will provide a better understanding of what information system security measures have been implemented by the respondent firms and who is responsible for them.

4.4.1 Responsibility for the Security of the Computers

The results in Table 4.4.1 show that 29% of the respondents stated that the extent or degree to which the computer users themselves are responsible for the security of the computers is above Medium Responsibility. The extent or degree to which the ISPs are responsible was indicated as Not at All by 45% of the respondents which was the highest. The extent or degree to which the program or software vendors are responsible was indicated as Not at All by 45% of the respondents which was the highest. The extent or degree to which the hardware vendors are responsible was indicated as Not at All by 39% of the respondents which was the highest. The extent or degree to which the system administrators are responsible was indicated as Very Responsible for 75% of the respondents which was the highest. The extent or degree to which

the consultants are responsible for the security of the computers varies evenly with 27% indicating Not at All, which was the highest.

Table 4.4.1 Responsibility for the Security of the Computers

Extent of responsibility of people is computer security	Not at all	Minimal responsibility	Medium responsibility	Above medium responsibility	Very responsible	Not stated
Computer users	0.0	28.0	21.0	29.0	22.0	0.0
Internet Service Providers	45.0	6.0	4.0	8.0	29.0	8.0
Program/software vendors	45.0	0.0	6.0	13.0	28.0	8.0
Hardware vendors	39.0	17.0	13.0	12.0	19.0	0.0
System administrators	2.0	0.0	14.0	5.0	75.0	4.0
Consultants	27.0	5.0	25.0	8.0	20.0	15.0

With this analysis it can be observed that within manufacturing firms, computers users and system administrators are deemed to be Very responsible for the security of their computers. Others, that is, ISPs, software/program vendors, hardware vendors and consultant depending on the firm mainly have Minimal to Medium Responsibility for the security of their computers. However it is important for every individual to note that the security of the computer based information systems is their responsibility to the level at which they have access. In this way everyone has some level of responsibility towards the security of the systems.

4.4.2 Occurrence of Information Systems Security Incidents

The results in Table 4.4.2 show that with regards to information system security incidents that have occurred within the respondent's firms, the highest raking was computer virus attack with 97% of the respondents indicating it had occurred in their firms; second was hardware failure with 93% of the respondents indicating it had occurred in their firms; third was communication systems failure with 68% of the respondents indicating it had occurred in their firms. Others closely ranked were software failure, clerical/operator errors and misuse of computers by employees which were experienced by slightly more than 55% of the respondents. Others like fraud, denial of service, processes and procedures failure, storage facilities failure and environmental condition failure had been experienced by very few of the respondents, below 50%. As a result, information systems security measures should focus on these areas first then move on to prevent other possible threats from occurring.

Table 4.4.2 Occurrence of Information Systems Security Incidents

Occurrence of Information System security Incidents	Frequency	Percent
Fraud	33	33.0
Theft of proprietary information	3	3.0
Denial of service	38	38.0
Vandalism/sabotage	5	5.0
Computer virus attack	97	97.0
Misuse of computers by workers	55	55.0
Hardware failure	93	93.0
Software failure	64	64.0
Communication system failure	68	68.0
Processes and procedures failure	23	23.0
Clerical/ operator failure	64	64.0
Tapping of transmissions	3	3.0
Environmental conditions failure	11	11.0
Unauthorized access	6	6.0

4.4.3 Information Systems Security Measures Available

The results in Table 4.4.3 show that the respondent manufacturing firms have information system security measures in place. The 10 most common/available measures amongst the firms are: use of passwords (89% of the respondents), software licensing agreements for software installed (85% of the respondents), backup policies and procedures (82% of the respondents), different levels of access restriction (82% of the respondents), alternative source of power (78% of the respondents), Virus management process (77% of the respondents), Email logs/filters (76% of the respondents), Account deactivation on termination or transfer of employee (71% of the respondents), Temperature controlled room (71% of the respondents) and central policy document (69% of the respondents). This shows that the respondent firms recognise the importance of information systems security measures and have implemented a number of them.

Table 4.4.3 Information Systems Security Measures Available

Information System Security Measures Available	Frequency	Percent
A central policy/document core to IS security programme	69	69.0
Security reporting to senior management	33	33.0
Information systems code of conduct/ethics	67	67.0
Formal project management	58	58.0
Mechanisms to test for software fixes and proper configurations	55	55.0
Complete current systems and applications documentation	49	49.0
A centralised logging system to gather log files	51	51.0
Periodic review of system administrative logs	55	55.0
Remote Access policies and procedures	38	38.0
Formal information systems security audit standards	31	31.0
Periodic information systems security audits/reviews	45	45.0

Information System Security Measures Available (cont...)	Frequency	Percent
Training of employees on IS security	54	54.0
Implementation of Disaster Recovery Plans (DRP)	50	50.0
Back up policies and procedures	82	82.0
Off-site Backup	61	61.0
Procedures for destroying unneeded sensitive files	31	31.0
Encryption of information/data	41	41.0
Virus management processes	77	77.0
Periodic review of software inventory (Count checks)	55	55.0
Software licensing agreements for installed software	85	85.0
Periodic Review of Hardware inventory (count checks)	67	67.0
Third party service provider agreements (Consultants, vendors Etc)	60	60.0
Human resource policies/procedures for screening new employees	38	38.0
Environmental security measures(servers in locked room with system and keyboard locks)	56	56.0
Environmental security measures (Alternative sources of power)	78	78.0
Environmental security measures(Servers protected from smoke and fire damage)	64	64.0
Environmental security measures(Overhead water and potential flood are avoided in server room)	60	60.0
Environmental security measures (Temperature controlled room)	71	71.0
Environmental security measures(Humidity controlled room)	29	29.0
Technical security measures (Use of passwords)	89	89.0
Technical security measures (Different levels of access restrictions)	82	82.0
Technical security measures (Account deactivation on termination or transfer of employee)	71	71.0
Technical security measures (Alarms/Account lock if incorrect password more than 3 times)	57	57.0
Existence of Firewall(s)	53	53.0
Existence of E-mail log files	76	76.0
Existence of intrusion detection system	49	49.0

4.4.4 Information Systems Security Measures monitored for compliance

The results in Table 4.4.4 show that though the respondent manufacturing firms have information system security measures in place, very few firms, less than 50% of the respondents have any procedures in place to monitor for compliance of any measures. The only measures where more than 50% of the respondents have procedures in place to monitor for compliance are the use of password (52%) and backup policies and procedures (51%). This shows that the firms in this sector appreciate the need for information systems security measures and have implemented a number of them, though, they do not recognise the importance of having mechanisms in place to monitor for compliance and thus are not able to say that the measures are 100% effective.

Table 4.4.4 Information Systems Security Measures Monitored

Information System Security Measures in place to monitor for compliance	Frequency	Percent
A central policy/document core to IS security programme	29	29.0
Security reporting to senior management	27	27.0
Information systems code of conduct/ethics	28	28.0
Formal project management	34	34.0
Mechanisms to test for software fixes and proper configurations	46	46.0
Complete current systems and applications documentation	35	35.0
A centralised logging system to gather log files	24	24.0
Periodic review of system administrative logs	33	33.0
Remote Access policies and procedures	22	22.0
Formal information systems security audit standards	22	22.0
Periodic information systems security audits/reviews	35	35.0
Training of employees on IS security	32	32.0
Implementation of Disaster Recovery Plans (DRP)	25	25.0
Back up policies and procedures	51	51.0
Off-site Backup	25	25.0
Procedures for destroying unneeded sensitive files	22	22.0
Encryption of information/data	25	25.0
Virus management processes	48	48.0
Periodic review of software inventory (Count checks)	41	41.0
Software licensing agreements for installed software	32	32.0
Periodic Review of Hardware inventory (count checks)	41	41.0
Third party service provider agreements (Consultants, vendors Etc)	22	22.0
Human resource policies/procedures for screening new employees	8	8.0
Environmental security measures(servers in locked room with system and keyboard locks)	30	30.0
Environmental security measures (Alternative sources of power)	29	29.0
Environmental security measures(Servers protected from smoke and fire damage)	29	29.0
Environmental security measures(Overhead water and potential flood are avoided in server room)	27	27.0
Environmental security measures(Temperature controlled room)	37	37.0
Environmental security measures(Humidity controlled room)	21	21.0
Technical security measures (Use of passwords)	52	52.0
Technical security measures (Different levels of access restrictions)	46	46.0
Technical security measures (Account deactivation on termination or transfer of employee)	44	44.0
Technical security measures (Alarms/Account lock if incorrect password more than 3 times)	35	35.0
Existence of Firewall(s)	27	27.0
Existence of E-mail log files	27	27.0
Existence of intrusion detection system	27	27.0

4.5 Identifying Importance Attached to the Different Security Approaches

Factor analysis was performed on the results of the importance attached to the different information systems security approaches. Factor analysis is a technique applicable where there is a systematic interdependence among a set of observed or manifest variables and the researcher is interested in finding out something more fundamental or latent which creates commonality. Thus factor analysis seeks to resolve a large set of measured variables in terms of relatively few categories, known as factors.

Table 4.5 List of Components/Factors for Identifying Importance

1	Importance attached to central policy/document core to IS secuity programme
2	Importance attached to security reporting to senior management
3	Importance attached to information systems code of conduct/ethics
4	Importance attached to formal project management
5	Importance attached to mechanisms to test for software fixes and proper configurations
6	Importance attached to complete current systems and applications documentation
7	Importance attached to A centralised logging system to gather log files
8	importance attached to Periodic review of system administrative logs
9	Importance attached to Remote Access policies and procedures
10	Importance attached to Formal information systems security audit standards
11	Importance attached to Periodic information systems security audits/reviews
12	Importance attached to Training of employees on IS security
13	Importance attached to Implementation of Disaster Recovery Plans(DRP)
14	Importance attached to Back up policies and procedures
15	Importance attached to Off-site Backup
16	Importance attached to Procedures for destroying unneeded sensitive files
17	Importance attached to Encryption of information/data
18	Importance attached to Virus management processes
19	Importance attached to Periodic review of software inventory(Count checks)
20	Importance attached to Software licencing agreements for installed softwares
21	Importance attached to Periodic Review of Hardware inventory (count checks)
22	Importance attached to Third party service provider agreements(Consultants,vendors Etc)
23	Importance attached to Human resource policies/procedures for screening new employees
24	Importance attached to Environmental security measures(servers in locked room with system and keyboard locks)
25	Importance attached to Environmental security measures(Alternative sources of power)
26	Importance attached to Environmental security measures(Servers protected from smoke and fire damage)
27	Importance attached to Environmental security measures(Overhead water and potential flood are avoided in server room)
28	Importance attached to Environmental security measures(Temperature controlled room)
29	Importance attached to Environmental security measures(Humidity controlled room)
30	Importance attached to Technical security measures (Use of passwords)
31	Importance attached to Technical security measures (Different levels of access restrictions)
32	Importance attached to Technical security measures (Account deactivation on termination or transfer of employee)
33	Importance attached to Technical security measures (Alarms/Account lock if incorrent password more than 3 times)
34	Importance attached to Existence of Firewall(s)
35	Importance attached to Existence of E-mail log files
36	Importance attached to Existence of intrusion detection system

4.5.1 Correlation Matrix for Identifying Importance Attached to the Different Approaches

Each respondent indicated the level of importance attached to the different information systems security measures/approaches. The results can be seen in Table 4.5.1. The extraction method was the primary component analysis. The correlation matrix reveals that the following groups of variables were highly correlated positively:

- 1,3,13,14,18,21,26,28,34
- 2,5,27, 29
- 4,6,23
- 7,8,17,22,33,35
- 9,10,11,16,24,34,36
- 12,16
- 15,19,25
- 20,32
- 30,31

Table 4.5.1 Correlation Matrix for Identifying Importance

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Correlation	1	1	0.644	0.839	0.062	0.763	-0.038	0.113	0.185	0.625	0.65	0.65	0.624	0.886	0.933	0.19	0.556
	2	0.644	1	0.565	0.689	0.835	0.591	0.066	0.056	0.383	0.635	0.635	0.639	0.751	0.629	-0.03	0.672
	3	0.839	0.565	1	0.118	0.632	-0.018	0.532	0.576	0.836	0.868	0.868	0.694	0.813	0.747	0.534	0.772
	4	0.062	0.689	0.118	1	0.516	0.79	0.117	0.123	-0.012	0.308	0.308	0.243	0.287	0.035	-0.009	0.392
	5	0.763	0.835	0.632	0.516	1	0.178	-0.13	-0.065	0.27	0.448	0.448	0.661	0.749	0.773	0.25	0.485
	6	-0.038	0.591	-0.018	0.79	0.178	1	0.227	0.204	0.04	0.327	0.327	0.069	0.273	-0.132	-0.372	0.364
	7	0.113	0.066	0.532	0.117	-0.13	0.227	1	0.967	0.678	0.702	0.702	0.173	0.252	-0.076	0.412	0.615
	8	0.185	0.056	0.576	0.123	-0.065	0.204	0.967	1	0.672	0.702	0.702	0.156	0.286	-0.032	0.463	0.588
	9	0.625	0.383	0.836	-0.012	0.27	0.04	0.678	0.672	1	0.897	0.897	0.695	0.589	0.529	0.316	0.866
	10	0.65	0.635	0.868	0.308	0.448	0.327	0.702	0.702	0.897	1	1	0.624	0.697	0.548	0.332	0.894
	11	0.65	0.635	0.868	0.308	0.448	0.327	0.702	0.702	0.897	1	1	0.624	0.697	0.548	0.332	0.894
	12	0.624	0.639	0.694	0.243	0.661	0.069	0.173	0.156	0.695	0.624	0.624	1	0.632	0.65	0.26	0.804
	13	0.886	0.751	0.813	0.287	0.749	0.273	0.252	0.286	0.589	0.697	0.697	0.632	1	0.802	0.106	0.614
	14	0.933	0.629	0.747	0.035	0.773	-0.132	-0.076	-0.032	0.529	0.548	0.548	0.65	0.802	1	0.147	0.462
	15	0.19	-0.03	0.534	-0.009	0.25	-0.372	0.412	0.463	0.316	0.332	0.332	0.26	0.106	0.147	1	0.267
	16	0.556	0.672	0.772	0.392	0.485	0.364	0.615	0.588	0.866	0.894	0.894	0.804	0.614	0.462	0.267	1
	17	0.098	-0.053	0.51	-0.005	-0.141	0.038	0.937	0.948	0.597	0.62	0.62	0.065	0.128	-0.097	0.55	0.489
	18	0.891	0.556	0.674	-0.085	0.706	-0.216	-0.126	-0.102	0.442	0.46	0.46	0.565	0.738	0.955	0.124	0.346
	19	0.027	0.094	0.27	0.315	0.367	-0.147	0.238	0.304	-0.017	0.131	0.131	0.112	0.003	0.006	0.716	0.105
	20	0.294	0.171	0.337	-0.095	-0.178	0.3	0.602	0.528	0.513	0.536	0.536	0.036	0.381	0.153	-0.189	0.394
	21	0.659	0.569	0.698	0.295	0.778	-0.13	0.121	0.177	0.408	0.532	0.532	0.551	0.545	0.69	0.565	0.457
	22	0.055	0.162	0.454	0.191	-0.07	0.346	0.829	0.804	0.476	0.618	0.618	0.108	0.213	-0.104	0.458	0.53
	23	-0.157	0.49	0.09	0.727	0.1	0.778	0.458	0.359	0.138	0.429	0.429	0.118	0.132	-0.226	0.051	0.446
	24	0.64	0.641	0.73	0.154	0.364	0.297	0.469	0.414	0.836	0.866	0.866	0.651	0.656	0.582	0.107	0.819
	25	0.164	-0.111	0.471	-0.183	0.207	-0.523	0.295	0.308	0.308	0.189	0.189	0.409	0.079	0.154	0.876	0.25
	26	0.773	0.48	0.762	-0.015	0.664	-0.335	0.085	0.104	0.636	0.582	0.582	0.734	0.558	0.831	0.414	0.557
	27	0.578	0.933	0.524	0.581	0.729	0.489	0.021	-0.014	0.46	0.642	0.642	0.711	0.622	0.616	-0.042	0.69
	28	0.838	0.742	0.751	0.104	0.631	0.137	0.148	0.119	0.712	0.738	0.738	0.755	0.796	0.848	0.032	0.69
	29	0.338	0.807	0.407	0.542	0.592	0.445	0.011	-0.057	0.333	0.55	0.55	0.619	0.425	0.452	0.118	0.581
	30	0.586	0.204	0.336	-0.249	0.368	-0.338	-0.202	-0.203	0.119	0.131	0.131	0.168	0.412	0.646	0.09	-0.047
	31	0.531	0.123	0.264	-0.216	0.313	-0.324	-0.193	-0.186	0.075	0.086	0.086	0.116	0.382	0.602	0.107	-0.107
	32	0.524	0.174	0.365	-0.187	0.101	-0.019	0.221	0.191	0.36	0.381	0.381	0.108	0.476	0.487	-0.034	0.162
	33	0.117	0.024	0.456	-0.024	-0.196	0.08	0.83	0.759	0.656	0.679	0.679	0.144	0.142	0.025	0.413	0.512
	34	0.758	0.454	0.953	-0.019	0.535	-0.144	0.525	0.538	0.782	0.814	0.814	0.637	0.717	0.701	0.633	0.681
	35	0.105	0.061	0.476	-0.031	-0.188	0.08	0.857	0.787	0.678	0.706	0.706	0.164	0.106	0.013	0.387	0.563
	36	0.671	0.462	0.879	0.042	0.332	0.09	0.73	0.727	0.907	0.942	0.942	0.536	0.641	0.553	0.363	0.803

Table 4.5.1 Correlation Matrix for Identifying Importance (continued...)

		17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Correlation	1	0.098	0.891	0.027	0.294	0.659	0.055	-0.157	0.64	0.164	0.773	0.578	0.838	0.338	0.586	0.531	0.524	0.117	0.758	0.105	0.671
	2	-0.053	0.556	0.094	0.171	0.569	0.162	0.49	0.641	-0.111	0.48	0.933	0.742	0.807	0.204	0.123	0.174	0.024	0.454	0.061	0.462
	3	0.51	0.674	0.27	0.337	0.698	0.454	0.09	0.73	0.471	0.762	0.524	0.751	0.407	0.336	0.264	0.365	0.456	0.953	0.476	0.879
	4	-0.005	-0.085	0.315	-0.095	0.295	0.191	0.727	0.154	-0.183	-0.015	0.581	0.104	0.542	-0.249	-0.216	-0.187	-0.024	-0.019	-0.031	0.042
	5	-0.141	0.706	0.367	-0.178	0.778	-0.07	0.1	0.364	0.207	0.664	0.729	0.631	0.592	0.368	0.313	0.101	-0.196	0.535	-0.188	0.332
	6	0.038	-0.216	-0.147	0.3	-0.13	0.346	0.778	0.297	-0.523	-0.335	0.489	0.137	0.445	-0.338	-0.324	-0.019	0.08	-0.144	0.08	0.09
	7	0.937	-0.126	0.238	0.602	0.121	0.829	0.458	0.469	0.295	0.085	0.021	0.148	0.011	-0.202	-0.193	0.221	0.83	0.525	0.857	0.73
	8	0.948	-0.102	0.304	0.528	0.177	0.804	0.359	0.414	0.308	0.104	-0.014	0.119	-0.057	-0.203	-0.186	0.191	0.759	0.538	0.787	0.727
	9	0.597	0.442	-0.017	0.513	0.408	0.476	0.138	0.836	0.308	0.636	0.46	0.712	0.333	0.119	0.075	0.36	0.656	0.782	0.678	0.907
	10	0.62	0.46	0.131	0.536	0.532	0.618	0.429	0.866	0.189	0.582	0.642	0.738	0.55	0.131	0.086	0.381	0.679	0.814	0.706	0.942
	11	0.62	0.46	0.131	0.536	0.532	0.618	0.429	0.866	0.189	0.582	0.642	0.738	0.55	0.131	0.086	0.381	0.679	0.814	0.706	0.942
	12	0.065	0.565	0.112	0.036	0.551	0.108	0.118	0.651	0.409	0.734	0.711	0.755	0.619	0.168	0.116	0.108	0.144	0.637	0.164	0.536
	13	0.128	0.738	0.003	0.381	0.545	0.213	0.132	0.656	0.079	0.558	0.822	0.796	0.425	0.412	0.382	0.476	0.142	0.717	0.106	0.641
	14	-0.097	0.955	0.008	0.153	0.69	-0.104	-0.226	0.582	0.154	0.831	0.816	0.848	0.452	0.646	0.602	0.487	0.025	0.701	0.013	0.553
	15	0.55	0.124	0.716	-0.189	0.565	0.458	0.051	0.107	0.876	0.414	-0.042	0.032	0.118	0.09	0.107	-0.034	0.413	0.633	0.387	0.363
	16	0.489	0.346	0.105	0.394	0.457	0.53	0.446	0.819	0.25	0.557	0.69	0.69	0.581	-0.047	-0.107	0.162	0.512	0.681	0.563	0.803
	17	1	-0.117	0.423	0.484	0.219	0.807	0.324	0.338	0.406	0.128	-0.083	0.053	-0.077	-0.162	-0.159	0.165	0.8	0.533	0.851	0.704
	18	-0.117	1	0.005	0.182	0.629	-0.144	-0.268	0.522	0.178	0.82	0.555	0.831	0.402	0.804	0.719	0.583	0.033	0.686	0.03	0.524
	19	0.423	0.005	1	-0.383	0.638	0.224	0.153	-0.222	0.604	0.277	0.018	-0.16	0.099	-0.017	-0.011	-0.257	0.107	0.301	0.172	0.133
	20	0.484	0.182	-0.383	1	-0.132	0.581	0.282	0.627	-0.224	0.013	0.142	0.429	0.027	0.226	0.228	0.715	0.834	0.351	0.641	0.627
	21	0.219	0.629	0.638	-0.132	1	0.07	0.08	0.366	0.429	0.807	0.568	0.516	0.498	0.353	0.343	0.115	0.175	0.673	0.186	0.511
	22	0.807	-0.144	0.224	0.581	0.07	1	0.571	0.481	0.303	-0.062	0.097	0.15	0.221	-0.198	-0.195	0.202	0.717	0.509	0.754	0.609
	23	0.324	-0.268	0.153	0.282	0.08	0.571	1	0.349	-0.123	-0.16	0.48	0.086	0.556	-0.334	-0.304	-0.039	0.455	0.079	0.422	0.241
	24	0.338	0.522	-0.222	0.627	0.366	0.481	0.349	1	0.061	0.539	0.716	0.87	0.637	0.223	0.148	0.46	0.554	0.7	0.58	0.817
	25	0.406	0.178	0.604	-0.224	0.429	0.303	-0.123	0.061	1	0.446	-0.084	0.074	0.038	0.125	0.096	-0.075	0.248	0.578	0.255	0.27
	26	0.128	0.82	0.277	0.013	0.807	-0.062	-0.16	0.539	0.446	1	0.581	0.734	0.446	0.567	0.482	0.316	0.241	0.757	0.261	0.635
	27	-0.083	0.555	0.018	0.142	0.568	0.097	0.48	0.716	-0.084	0.581	1	0.792	0.899	0.201	0.111	0.148	0.114	0.443	0.145	0.479
	28	0.053	0.831	-0.16	0.429	0.516	0.15	0.086	0.87	0.074	0.734	0.792	1	0.656	0.521	0.423	0.532	0.252	0.721	0.284	0.71
	29	-0.077	0.402	0.099	0.027	0.498	0.221	0.556	0.637	0.038	0.446	0.899	0.656	1	0.117	0.037	0.04	0.163	0.419	0.198	0.364
	30	-0.162	0.804	-0.017	0.226	0.353	-0.198	-0.334	0.223	0.125	0.567	0.201	0.521	0.117	1	0.928	0.758	0.072	0.445	0.038	0.273
	31	-0.159	0.719	-0.011	0.228	0.343	-0.195	-0.304	0.148	0.096	0.482	0.111	0.423	0.037	0.928	1	0.827	0.13	0.382	0.005	0.195
	32	0.165	0.583	-0.257	0.715	0.115	0.202	-0.039	0.48	-0.075	0.316	0.148	0.532	0.04	0.758	0.827	1	0.474	0.458	0.371	0.487
	33	0.8	0.033	0.107	0.634	0.175	0.717	0.455	0.554	0.248	0.241	0.114	0.252	0.163	0.072	0.13	0.474	1	0.554	0.942	0.731
	34	0.533	0.686	0.301	0.351	0.673	0.509	0.079	0.7	0.578	0.757	0.443	0.721	0.419	0.445	0.382	0.458	0.554	1	0.557	0.866
	35	0.851	0.03	0.172	0.641	0.186	0.754	0.422	0.58	0.255	0.261	0.145	0.284	0.198	0.038	0.005	0.371	0.942	0.557	1	0.784
	36	0.704	0.524	0.133	0.627	0.511	0.609	0.241	0.817	0.27	0.635	0.479	0.71	0.364	0.273	0.195	0.487	0.731	0.866	0.784	1

4.5.2 Total Variance Explained for Identifying Importance Attached to the Different Approaches

Table 4.5.2 shows all the factors extracted from the analysis along with their Eigen values, the percent of variance attributed to each factor and the cumulative variance of the factor and the previous factors. The first 6 factors were the only ones with Eigen values greater than 1. The first factor, central policy document core to IS security program, accounts for 43.8% of the variance, the second, security reporting to senior management, accounts for 19.2% of the variance, the third, information systems code of conduct/ethics, accounts for 13% of the variance, the fourth, formal project management, accounts for 10.2% of the variance, the fifth, mechanisms to test for software fixes and proper configurations, accounts for 4.6% of the variance and the sixth, complete current system and application documentation, accounts for 3.2% of the variance. This shows that these six have the highest importance attached to them by the respondents.

Table 4.5.2 Total Variance Explained for Identifying Importance

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	15.802	43.895	43.895	15.802	43.895	43.895	11.607	32.241	32.241
2	6.934	19.260	63.154	6.934	19.260	63.154	9.231	25.642	57.883
3	4.713	13.092	76.247	4.713	13.092	76.247	4.233	11.760	69.643
4	3.678	10.216	86.463	3.678	10.216	86.463	3.850	10.695	80.338
5	1.690	4.694	91.157	1.690	4.694	91.157	3.834	10.651	90.989
6	1.160	3.222	94.379	1.160	3.222	94.379	1.220	3.389	94.379
7	.667	1.852	96.230						
8	.432	1.201	97.432						
9	.255	.707	98.139						
10	.161	.447	98.586						
11	.140	.388	98.974						
12	.116	.322	99.296						
13	7.650E-02	.213	99.508						
14	6.148E-02	.171	99.679						
15	3.977E-02	.110	99.789						
16	3.225E-02	8.959E-02	99.879						
17	2.060E-02	5.721E-02	99.936						
18	1.170E-02	3.250E-02	99.969						
19	8.112E-03	2.253E-02	99.991						
20	2.310E-03	6.417E-03	99.998						
21	8.447E-04	2.347E-03	100.000						
22	1.494E-15	4.149E-15	100.000						
23	6.161E-16	1.711E-15	100.000						
24	5.834E-16	1.621E-15	100.000						
25	2.921E-16	8.113E-16	100.000						
26	1.661E-16	4.614E-16	100.000						
27	-7.212E-33	-2.003E-32	100.000						
28	-1.441E-17	-4.003E-17	100.000						
29	-1.398E-16	-3.884E-16	100.000						
30	-2.476E-16	-6.879E-16	100.000						
31	-2.987E-16	-8.296E-16	100.000						
32	-4.015E-16	-1.115E-15	100.000						
33	-5.473E-16	-1.520E-15	100.000						
34	-6.910E-16	-1.919E-15	100.000						
35	-8.805E-16	-2.446E-15	100.000						
36	-2.082E-15	-5.785E-15	100.000						

Extraction Method: Principal Component Analysis.

4.5.3 Component Matrix for Identifying Importance Attached to the Different Approaches

Once the factors have been extracted, it is possible to calculate the loading of the importance on each factor. The higher the absolute value of the loading the more the importance is attached to the factor. Table 4.5.3 shows that only 4 factors have been extracted. The gaps on the table represent loadings that are less than 0.5, the use of gaps makes reading the table easier.

Table 4.5.3 Component Matrix for Identifying Importance

	Component			
	1	2	3	4
Importance attached to central policy/document core to IS security programme	0.8			
Importance attached to security reporting to senior management	0.697		0.603	
Importance attached to information systems code of conduct/ethics	0.939			
Importance attached to formal project management			0.79	
Importance attached to mechanisms to test for software fixes and proper configurations	0.616	-0.589		
Importance attached to complete current systems and applications documentation			0.878	
Importance attached to A centralised logging system to gather log files	0.555	0.795		
importance attached to Periodic review of system administrative logs	0.552	0.755		
Importance attached to Remote Access policies and procedures	0.864			
Importance attached to Formal information systems security audit standards	0.947			
Importance attached to Periodic information systems security audits/reviews	0.947			
Importance attached to Training of employees on IS security	0.735			
Importance attached to Implementation of Disaster Recovery Plans (DRP)	0.8			
Importance attached to Back up policies and procedures	0.729	-0.63		
Importance attached to Off-site Backup				0.668
Importance attached to Procedures for destroying unneeded sensitive files	0.862			
Importance attached to Encryption of information/data		0.781		
Importance attached to Virus management processes	0.674	-0.663		
Importance attached to Periodic review of software inventory (Count checks)				0.821
Importance attached to Software licensing agreements for installed software				-0.732
Importance attached to Periodic Review of Hardware inventory (count checks)	0.677			0.507
Importance attached to Third party service provider agreements (Consultants, vendors)	0.502	0.739		
Importance attached to Human resource policies/procedures for screening new employees			0.675	
Importance attached to Environmental security measures (servers in locked room with system and keyboard locks)	0.865			
Importance attached to Environmental security measures Alternative sources of power)			-0.53	0.638
Importance attached to Environmental security measures (Servers protected from smoke and fire damage)	0.752			
Importance attached to Environmental security measures(Overhead water and potential flood are avoided in server room)	0.698		0.57	
Importance attached to Environmental security measures(Temperature controlled room)	0.85			
Importance attached to Environmental security measures(Humidity controlled room)	0.59		0.551	
Importance attached to Technical security measures (Use of passwords)		-0.573		
Importance attached to Technical security measures (Different levels of access restrictions)		-0.529		
Importance attached to Technical security measures (Account deactivation on termination or transfer of employee)				-0.654
Importance attached to Technical security measures (Alarms/Account lock if incorrect password more than 3 times)	0.575	0.649		
Importance attached to Existence of Firewall(s)	0.91			
Importance attached to Existence of E-mail log files	0.592	0.678		
Importance attached to Existence of intrusion detection system	0.924			

Extraction Method: Principal Component Analysis.

4.5.4 Rotated Component Matrix for Identifying Importance Attached to the Different Approaches

Factor rotation is done to reduce the number of factors on which the variables under investigation have high loadings. This changes nothing but makes interpretation of the analysed data easier. From the Rotated matrix in Table 4.5.4, it can bee seen that:

- Variables 1,2,3,5,9,12,13,14,16,18,24,26,27,28, 34 load heavily on factor 1 (Component1)

- Variables 7,8,10,11,17,20,22,33,35,36 load heavily on factor 2 (Component 2)
- Variables 4,6,23,29 load heavily on factor 3 (Component 3)
- Variables 15,19,21,25 load heavily on factor 4 (Component 4)

Table 4.5.4 Rotated Component Matrix for Identifying Importance

	Component					
	1	2	3	4	5	6
1) Importance attached to central policy/document core to IS security programme	0.872					
2) Importance attached to security reporting to senior management	0.723		0.673			
3) Importance attached to information systems code of conduct/ethics	0.8					
4) Importance attached to formal project management			0.917			
5) Importance attached to mechanisms to test for software fixes and proper configurations	0.767					
6) Importance attached to complete current systems and applications documentation			0.865			
7) Importance attached to a centralised logging system to gather log files		0.96				
8) Importance attached to Periodic review of system administrative logs		0.923				
9) Importance attached to Remote Access policies and procedures	0.703	0.662				
10) Importance attached to Formal information systems security audit standards	0.673	0.679				
11) Importance attached to Periodic information systems security audits/reviews	0.673	0.679				
12) Importance attached to Training of employees on IS security	0.862					
13) Importance attached to Implementation of Disaster Recovery Plans(DRP)	0.803					
14) Importance attached to Back up policies and procedures	0.879					
15) Importance attached to Off-site Backup				0.856		
16) Importance attached to Procedures for destroying unneeded sensitive files	0.721	0.54				
17) Importance attached to Encryption of information/data		0.924				
18) Importance attached to Virus management processes	0.788				0.571	
19) Importance attached to Periodic review of software inventory (count checks)				0.922		
20) Importance attached to Software licensing agreements for installed software		0.711		-0.522		
21) Importance attached to Periodic Review of Hardware inventory (count checks)	0.623			0.631		
22) Importance attached to Third party service provider agreements (Consultants, vendors Etc)		0.863				
23) Importance attached to Human resource policies/procedures for screening new employees			0.825			
24) Importance attached to Environmental security measures (servers in locked room with system and keyboard locks)	0.718	0.515				
25) Importance attached to Environmental security measures (Alternative sources of power)				0.776		
26) Importance attached to Environmental security measures (Servers protected from smoke and fire damage)	0.804					
27) Importance attached to Environmental security measures (Overhead water and potential flood are avoided in server room)	0.747		0.573			
28) Importance attached to Environmental security measures (Temperature controlled room)	0.885					
29) Importance attached to Environmental security measures (Humidity controlled room)	0.564		0.591			0.518
30) Importance attached to Technical security measures (Use of passwords)					0.886	
31) Importance attached to Technical security measures (Different levels of access restrictions)					0.933	
32) Importance attached to Technical security measures (Account deactivation on termination or transfer of employee)					0.846	
33) Importance attached to Technical security measures (Alarms/Account lock if incorrect password more than 3 times)		0.907				
34) Importance attached to Existence of Firewall(s)	0.692	0.515				
35) Importance attached to Existence of E-mail log files		0.922				
36) Importance attached to Existence of intrusion detection system	0.621	0.741				

4.5.5 Isolation of Factors for Identifying Importance Attached to the Different Approaches

Factor isolation involves isolating each factor based on factor loadings. The results can be seen in Table 4.5.5, which shows factor isolation based on a minimum correlation of 0.59.

Factor 1 indicates that most variables have been grouped under this factor due to their similarity. These include: importance attached to central policy/document core to IS security programme, importance attached to security reporting to senior management, importance attached to information systems code of conduct/ethics, importance attached to mechanisms to test for software fixes and proper configurations, importance attached to Remote Access policies and procedures, importance attached to Training of employees on IS security, importance attached to Implementation of Disaster Recovery Plans(DRP), importance attached to Back up policies and procedures, importance attached to Procedures for destroying unneeded sensitive files, importance attached to Virus management processes, importance attached to Environmental security measures (servers in locked room with system and keyboard locks), importance attached to Environmental security measures (servers protected from smoke and fire damage), importance attached to Environmental security measures (Overhead water and potential flood are avoided in server room), importance attached to Environmental security measures (Temperature controlled room) and importance attached to Existence of Firewall(s).

Factor 2 indicates a focus on importance attached to a centralised logging system to gather log files, importance attached to Periodic review of system administrative logs, importance attached to Formal information systems security audit standards, importance attached to Periodic information systems security audits/reviews, importance attached to Encryption of information/data, importance attached to Software licensing agreements for installed software, importance attached to Third party service provider agreements (consultants, vendors and others), importance attached to Technical security measures (Alarms/Account lock if incorrect password more than 3 times), importance attached to Existence of E-mail log files and importance attached to Existence of intrusion detection system.

Factor 3 concentrates on importance attached to formal project management, importance attached to complete current systems and applications documentation, importance attached to Human resource policies/procedures for screening new employees and importance attached to Environmental security measures (Humidity controlled room).

Factor 4 revolves around importance attached to Off-site Backup, importance attached to Periodic review of software inventory (Count checks), importance attached to Periodic Review of Hardware inventory (count checks) and importance attached to Environmental security measures (Alternative sources of power).

It is thus clear that though there were 36 factors indicated in the questionnaire most factors were grouped together under factors 1 and 2, and the rest were distributed under factor 3 and 4. Thus bringing a final four factors.

Table 4.5.5 Isolation of Factors for Identifying Importance

Factor	Variables
1	• Importance attached to central policy/document core to IS security programme • Importance attached to security reporting to senior management • Importance attached to information systems code of conduct/ethics • Importance attached to mechanisms to test for software fixes and proper configurations • Importance attached to Remote Access policies and procedures • Importance attached to Training of employees on IS security • Importance attached to Implementation of Disaster Recovery Plans(DRP) • Importance attached to Back up policies and procedures • Importance attached to Procedures for destroying unneeded sensitive files • Importance attached to Virus management processes • Importance attached to Environmental security measures (servers in locked room with system and keyboard locks) • Importance attached to Environmental security measures (servers protected from smoke and fire damage) • Importance attached to Environmental security measures (Overhead water and potential flood are avoided in server room) • Importance attached to Environmental security measures (Temperature controlled room) • Importance attached to Existence of Firewall(s)
2	• Importance attached to a centralised logging system to gather log files • Importance attached to Periodic review of system administrative logs • Importance attached to Formal information systems security audit standards • Importance attached to Periodic information systems security audits/reviews • Importance attached to Encryption of information/data • Importance attached to Software licensing agreements for installed software • Importance attached to Third party service provider agreements (consultants, vendors and others) • Importance attached to Technical security measures (Alarms/Account lock if incorrect password more than 3 times) • Importance attached to Existence of E-mail log files • Importance attached to Existence of intrusion detection system
3	• Importance attached to formal project management • Importance attached to complete current systems and applications documentation • Importance attached to Human resource policies/procedures for screening new employees • Importance attached to Environmental security measures (Humidity controlled room)
4	• Importance attached to Off-site Backup • Importance attached to Periodic review of software inventory (Count checks) • Importance attached to Periodic Review of Hardware inventory (count checks) • Importance attached to Environmental security measures (Alternative sources of power)

4.6 Challenges in Implementing Information Systems Security

Table 4.6 List of Components/Factors for Challenges

1	Developing a comprehensive IS security program is time consuming
2	Inadequate legislation governing IS security
3	Lack of documented guidelines on how to prepare as IS security policy
4	Lack of proper IS security planning
5	Lack of a budget for IS security planning
6	Lack of budget for IS security implementation
7	Lack of information sharing on threats and vulnerabilities within the organisation
8	Lack of information sharing on threats and vulnerabilities between same sector organisations
9	Lack of procedures of collecting evidence after a breach of IS security
10	Lack of warning capabilities on threat and vulnerability information addressing threats to information sytems
11	Inadequate senior management attention to information security
12	Inadequate accountability for job and program performance related to I.T security
13	Lack of proper mechanisms to facilitate periodic information system security program review
14	Limited security training for general users
15	Limited security training for IT professionals
16	Lack of security guidelines for contractor-provided services
17	Some aspects of information system security are complex to impliment

Table 4.6 shows a list of the components or factors for challenges in implementing information systems security. It shall act as the key for a better understanding of Section 4.6.

4.6.1 Correlation Matrix for Challenges in implementing Information Systems Security

Each respondent indicated the challenges in implementing information systems security the results can be seen in Table 4.6.1. The extraction method was the primary component analysis. The correlation matrix reveals that variable 1,3 and 17 are weakly correlated with the other variables. However, the following groups of variables were highly correlated positively:

- 2,4,5,6,7,9,11,12,14,15
- 8,10,13,16

Table 4.6.1 Correlation Matrix for Challenges

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Correlation	1	1	-0.008	-0.252	-0.135	-0.37	-0.428	-0.079	-0.347	-0.357	-0.187	-0.308	-0.371	-0.294	-0.184	-0.211	-0.15	0.241
	2	-0.008	1	0.214	0.855	0.574	0.521	0.644	0.249	0.573	0.305	0.4	0.757	0.39	0.691	0.637	0.069	0.603
	3	-0.252	0.214	1	0.258	0.248	0.206	0.624	0.52	0.553	0.627	0.376	0.326	0.445	0.357	0.37	0.383	-0.059
	4	-0.135	0.855	0.258	1	0.765	0.693	0.682	0.464	0.718	0.394	0.524	0.861	0.615	0.898	0.734	0.274	0.472
	5	-0.37	0.574	0.248	0.765	1	0.93	0.717	0.786	0.794	0.638	0.544	0.753	0.759	0.838	0.767	0.534	0.226
	6	-0.428	0.521	0.206	0.693	0.93	1	0.64	0.738	0.774	0.598	0.499	0.742	0.691	0.775	0.724	0.479	0.183
	7	-0.079	0.644	0.624	0.682	0.717	0.64	1	0.777	0.735	0.784	0.656	0.729	0.826	0.783	0.812	0.672	0.126
	8	-0.347	0.249	0.52	0.464	0.786	0.738	0.777	1	0.799	0.886	0.594	0.564	0.895	0.715	0.756	0.84	-0.15
	9	-0.357	0.573	0.553	0.718	0.794	0.774	0.735	0.799	1	0.796	0.558	0.731	0.745	0.804	0.82	0.511	0.254
	10	-0.187	0.305	0.627	0.394	0.638	0.598	0.784	0.886	0.796	1	0.487	0.496	0.75	0.634	0.716	0.747	-0.073
	11	-0.308	0.4	0.376	0.524	0.544	0.499	0.656	0.594	0.558	0.487	1	0.8	0.768	0.613	0.807	0.65	-0.129
	12	-0.371	0.757	0.326	0.861	0.753	0.742	0.729	0.564	0.731	0.496	0.8	1	0.73	0.812	0.858	0.461	0.161
	13	-0.294	0.39	0.445	0.615	0.759	0.691	0.826	0.895	0.745	0.75	0.768	0.73	1	0.824	0.86	0.882	-0.172
	14	-0.184	0.691	0.357	0.898	0.838	0.775	0.783	0.715	0.804	0.634	0.613	0.812	0.824	1	0.839	0.549	0.291
	15	-0.211	0.637	0.37	0.734	0.767	0.724	0.812	0.756	0.82	0.716	0.807	0.858	0.86	0.839	1	0.684	0.093
	16	-0.15	0.069	0.383	0.274	0.534	0.479	0.672	0.84	0.511	0.747	0.65	0.461	0.882	0.549	0.684	1	-0.494
	17	0.241	0.603	-0.059	0.472	0.226	0.183	0.126	-0.15	0.254	-0.073	-0.129	0.161	-0.172	0.291	0.093	-0.494	1

4.6.2 Total Variance Explained for Challenges in implementing Information Systems Security

Table 4.6.2 shows all the factors extracted from the analysis along with their Eigen values, the percent of variance attributed to each factor and the cumulative variance of the factor and the previous factors. The first 4 factors were the only ones with Eigen values greater than 1. The first factor, developing a comprehensive IS security program is time consuming, accounts for 60.39% of the variance, the second, inadequate legislation governing IS security, accounts for 14.79% of the variance, the third, lack of documented guidelines on how to prepare IS security policy, accounts for 7.03% of the variance and the fourth, lack of proper IS security planning, accounts for 5.88% of the variance. This shows that these four are the greatest challenges to implementing information systems security as indicated by the respondents.

Table 4.6.2 Total Variance Explained for Challenges

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	10.267	60.391	60.391	10.267	60.391	60.391	5.324	31.317	31.317
2	2.515	14.795	75.186	2.515	14.795	75.186	4.901	28.830	60.147
3	1.196	7.038	82.225	1.196	7.038	82.225	3.033	17.839	77.986
4	1.001	5.887	88.111	1.001	5.887	88.111	1.721	10.125	88.111
5	.846	4.978	93.089						
6	.306	1.798	94.887						
7	.240	1.415	96.302						
8	.210	1.237	97.538						
9	.140	.823	98.361						
10	7.353E-02	.433	98.793						
11	6.374E-02	.375	99.168						
12	4.938E-02	.290	99.459						
13	3.617E-02	.213	99.672						
14	2.277E-02	.134	99.806						
15	1.961E-02	.115	99.921						
16	1.030E-02	6.060E-02	99.981						
17	3.146E-03	1.850E-02	100.000						

Extraction Method: Principal Component Analysis.

4.6.3 Component Matrix for Challenges in implementing Information Systems Security

Once the factors have been extracted, it is possible to calculate the loading of the challenges on each factor. The higher the absolute value of the loading the more the challenge contributes to the factor. Table 4.6.3 shows that only 4 factors have been extracted. The gaps on the table represent loadings that are less than 0.5, the use of gaps makes reading the table easier.

Table 4.6.3 Component Matrix for Challenges

	Component			
	1	2	3	4
Developing a comprehensive IS security program is time consuming			.763	
Inadequate legislation governing IS security	.642	.667		
Lack of ducumented guidelines on how to prepare as IS security policy	.511			-.547
Lack of proper IS security planning	.800	.518		
Lack of a budget for IS security planning	.884			
Lack of budget for IS security implementation	.835			
Lack of information sharing on threats and vulnerabilities within the organisation	.893			
Lack of information sharing on threats and vulnerabilities between same sector organisations	.867			
Lack of procedures of collecting evidence after a breach of IS security	.896			
Lack of warning capabilities on threat and vulnerability information addressing threats to information sytems	.797			
Inadequate senior management attention to information security	.756			
Inadequate accountability for job and program performance related to I.T security	.873			
Lack of proper mechanisms to facilitate periodic information system security program review	.914			
Limited security training for general users	.913			
Limited security training for IT professionals	.931			
Lack of security guidelines for contractor-provided services	.706	-.610		
Some aspects of information system security are complex to impliment		.890		

Extraction Method: Principal Component Analysis.

a 4 components extracted.

4.6.4 Rotated Component Matrix for Challenges in implementing Information Systems Security

From the Rotated matrix in Table 4.6.4, it can bee seen that:

- Variables 2, 4,5,6,12,14,17 load heavily on factor 1 (Component1)
- Variables 8,11,13,15,16 load heavily on factor 2 (Component 2)
- Variables 3,7,9,10, load heavily on factor 3 (Component 3)

Table 4.6.4 Rotated Component Matrix for Challenges

	Component			
	1	2	3	4
Developing a comprehensive IS security program is time consuming				-.949
Inadequate legislation governing IS security	.920			
Lack of ducumented guidelines on how to prepare as IS security policy			.870	
Lack of proper IS security planning	.899			
Lack of a budget for IS security planning	.641			
Lack of budget for IS security implementation	.598			
Lack of information sharing on threats and vulnerabilities within the organisation	.522	.547	.576	
Lack of information sharing on threats and vulnerabilities between same sector organisations		.648	.602	
Lack of procedures of collecting evidence after a breach of IS security	.583		.586	
Lack of warning capabilities on threat and vulnerability information addressing threats to information sytems			.767	
Inadequate senior management attention to information security		.758		
Inadequate accountability for job and program performance related to I.T security	.715	.536		
Lack of proper mechanisms to facilitate periodic information system security program review		.814		
Limited security training for general users	.732			
Limited security training for IT professionals	.585	.685		
Lack of security guidelines for contractor-provided services		.904		
Some aspects of information system security are complex to impliment	.765	-.522		

4.6.5 Isolation of Factors for Challenges in implementing Information Systems Security

Factor isolation involves isolating each factor based on factor loadings. The results can be seen in Table 4.6.5, which shows factor isolation based on a minimum correlation of 0.576.

Factor 1 indicates that most variables have been grouped under this factor due to their similarity. These include: inadequate legislation governing IS security, lack of proper IS security planning Lack of a budget for IS security planning, lack of a budget for IS security implementation, inadequate accountability for job and program performance related to IT security, limited security training for general users and some aspects of information system security are complex to implement.

Factor 2 indicates a focus on lack of information sharing on threats and vulnerabilities between same sector organisations, inadequate senior management attention to information systems security, lack of proper mechanisms to facilitate periodic information system security program review, limited security training for IT professionals and lack of security guidelines for contractor-provided services.

Factor 3 concentrates on lack of documented guidelines on how to prepare an IS security policy, lack of information sharing on threats and vulnerabilities within the organisation, lack of procedures for collecting evidence after a breach of IS security and lack of warning capabilities on threat and vulnerability information addressing threats to information systems

It is thus clear that though there were 17 factors indicated in the questionnaire most factors were grouped together under factors 1,2 and 3. Thus bringing a final three factors.

Table 4.6.5 Isolation of Factors for Challenges

Factor	Variables
1	• Inadequate legislation governing IS security • Lack of proper IS security planning • Lack of a budget for IS security planning • Lack of a budget for IS security implementation • Inadequate accountability for job and program performance related to IT security • Limited security training for general users • Some aspects of information system security are complex to implement
2	• Lack of a information sharing on threats and vulnerabilities between same sector organisations • Inadequate senior management attention to information systems security • Lack of proper mechanisms to facilitate periodic information system security program review • Limited security training for IT professionals • Lack of security guidelines for contractor-provided services
3	• Lack of documented guidelines on how to prepare an IS security policy • Lack of information sharing on threats and vulnerabilities within the organisation • Lack of procedures for collecting evidence after a breach of IS security • Lack of warning capabilities on threat and vulnerability information addressing threats to information systems

CHAPTER 5: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

In this chapter the results are summarised, then conclusions arrived at from the research findings are discussed in light of the objectives of the study and finally, recommendations made. The study sought to identify information system security measures or approaches implemented in large manufacturing firms in Kenya; determine the relative importance attached to the information system security measures or approaches in large manufacturing firms in Kenya and finally to identify challenges to implementing information system security in large manufacturing firms in Kenya. The data was collected from a sample of large private manufacturing firms that had representatives from each industry. The data was analysed primarily by the use of descriptive statistical measures such as frequency tables and factor analysis.

5.2 Summary and Conclusions

The manufacturing sector is a fast growing sector. This can be shown by the fact that it has firms that are owned by local and foreign investors and those that are jointly owned by both. Most of the firms have over 2000 customers, over 200 employees and an annual turnover of 1 to 100 million Kenya shillings.

Also noted during the study is that within this fast growing sector the implementation of computer based information systems has taken root. This can be exhibited by the fact that a number of functions within manufacturing firms are computerised, the most common being payroll, stock ordering, customer base management, supplier base management, payments management and invoicing. These are mainly used in a batch-processing manner. The frequency with which these information systems are assessed varies from firm to firm, however the most common is annually.

5.2.1 Identification of IS Security measures implemented

The study shows that to support the computer based information systems, most of the firms have an IT department, which has its own budget. However, the position of the IT department in the organisational hierarchy is not very favourable since over 50% of the respondent firms indicated

that it is under the Finance department. This shows that the IT department is seen only as a support department as opposed to being a strategic department. As a result, it is not represented at the board level and is not autonomous. This sometimes hampers its ability to function effectively since IT and Finance are two separate functions each playing a different role within the firm and in the event of a disagreement or conflict, Finance will be in a position to overrule IT.

In terms of investment, more than 50% of the firms have an IT departmental budget. This indicates that there is continued heavy investment in information technology by these firms. However, very few of these firms allocate a specific/certain amount to the IS security team or function which means that this crucial and critical function has to compete with other IT/IS functions for resources. This has been seen to hamper growth and development in information systems security leading to further exposure from information systems security risk perspective, since funds needed to update the information systems security measures to keep up with the dynamic technology may not be availed.

This notwithstanding, the manufacturing firms have reduced their risk somewhat by taking into consideration the ownership aspect of the information systems. Most manufacturing firms own their own hardware, operations and software and only outsource functions like preventive maintenance. This reduces risk brought about by third parties who may not be clear on the firm's information systems security measures and controls.

The presence of an information systems security team in most of the firms also shows their inclination to reduce risks. However the composition of the information systems security team does not include members from other business units therefore missing their invaluable contribution to this process. Further to this, only about 50% of the manufacturing firms have given this information systems security team's members job descriptions and thus are unable to evaluate their performance. In 50% of the manufacturing firms, this team is governed by a written and formal information systems security policy which is only annually updated, which may not be sufficient given the dynamism of IT.

In terms of network use, most of the large private manufacturing firms have a local area network, an intranet and provide Internet access. This implies that there is technology in place to enrich

them with knowledge on different issues in general and specific issues pertaining to their work. It also indicates a positive move within the manufacturing sector towards readying itself for e-commerce. However, it should be noted that this exposes the manufacturing firm's corporate networks to computer viruses and other malicious codes that are spread through the Internet especially through electronic mail, which is the highest threat observed in this sector.

This observation implies that very few of the information systems/technology managers place little emphasis on anti-virus management. This is a loophole that can lead to destruction of pertinent data, thus hampering the operations of the firm and by extension affecting confidentiality, integrity, availability and assurance of the data. The other high vulnerability areas include hardware failure, communication system failure and operator/clerical errors.

As a countermeasure, the firms have implemented a variety of information systems security measures which include the use of password, email log filters, account closure if an employee is terminated or reassigned, provision of different levels of access, having alternative sources of power, virus management processes and procedures, backup policies and procedures and software license management. However less than 50% of the firms have put mechanisms or procedures in place to check for compliance and to monitor the effectiveness of these measures.

In addition to this, security measures on their own cannot prevent information system security incidents from happening. Most of the large private manufacturing firms seem to have concentrated computer literacy and training within the management levels only, neglecting other levels of staff. This indicates a gap, which needs to be filled. Some manufacturing firms have an information system code of conduct or ethics that covers security. However, the lack of company-wide training means that the users feel that the responsibility of caring for the equipment rests to a great extent with the systems administrators.

5.2.2 Relative importance attached to the IS Security measures

The relative importance attached to the information systems security measures was based mainly on: First, past experience, where the firms implement measures and controls to prevent a repetition of a past information system security breach. This means that past threats and their countermeasures are given high ranking. Second, adherence to information systems security

policy, such that if a certain security measure is ranked highly within the policy, then relative importance attached to the security measure is also high.

Third, most of the manufacturing firms have only one branch and perform a lot of batch processing. These are important considerations when implementing information system security measures, since threats related to this and their countermeasures are given high ranking in terms of importance. Fourth, others like hardware inventory checks and alternative source of power were seen as being obvious or standard for example computers are purchased with an uninterruptible power supply and thus were given low importance.

The highest ranking information systems security measures were importance attached to: central policy/document core to IS security programme, security reporting to senior management, information systems code of conduct/ethics, mechanisms to test for software fixes and proper configurations, remote access policies and procedures, training of employees on IS security, implementation of Disaster Recovery Plans(DRP), back up policies and procedures, procedures for destroying unneeded sensitive files, virus management processes, environmental security measures (servers in locked room with system and keyboard locks; protected from smoke and fire damage and overhead water and potential floods), and existence of Firewall(s).

The second highest ranking information systems security measures were importance attached to: a centralised logging system to gather log files, periodic review of system administrative logs, formal information systems security audit standards, periodic information systems security audits/reviews, encryption of information/data, software licensing agreements for installed software, third party service provider agreements (consultants, vendors and others), technical security measures (Alarms/Account lock if incorrect password more than 3 times), existence of E-mail log files and existence of intrusion detection system.

The third highest ranking information systems security measures were importance attached to: formal project management, complete current systems and applications documentation and Human resource policies/procedures for screening new employees.

The lowest ranking information systems security measures were importance attached to: off-site Backup, periodic review of software inventory (Count checks), periodic review of hardware inventory (count checks) and alternative sources of power.

The overall goal in the respondents' minds with regards to information systems security measures is to implement measures that can efficiently and effectively protect as many of the computer based information systems within the firm as possible (for example an anti-virus can be installed on several computers), from specific threats or a combination of threats, within the budget. It should be noted however that even though the measures were ranked in terms of importance, the respondents indicated that all the measures had some level of importance.

5.2.3 Challenges to implementing IS Security measures

According to the respondents, the main challenges to implementing information systems security were: first, developing a comprehensive IS security program is time consuming. Second, inadequate legislation governing IS security. Third, lack of documented guidelines on how to prepare IS security policy. Fourth, lack of proper IS security planning and fifth, lack of a budget for IS security implementation. This shows that these four are the greatest challenges to implementing information systems security as indicated by the respondents.

The second highest ranking challenges were: inadequate accountability for job and program performance related to IT security, limited security training for general users and some aspects of information system security are complex to implement, lack of a information sharing on threats and vulnerabilities between same sector organisations, inadequate senior management attention to information systems security, lack of proper mechanisms to facilitate periodic information system security program review, limited security training for IT professionals and lack of security guidelines for contractor-provided services.

The lowest ranking challenges were: lack of documented guidelines on how to prepare an IS security policy, lack of information sharing on threats and vulnerabilities within the organisation, lack of procedures for collecting evidence after a breach of IS security and lack of warning capabilities on threat and vulnerability information addressing threats to information systems. These were ranked the lowest because there are several books and supplier product

demonstrations that can aid to fill in this gap and also because internal policy can hamper information flow.

It should be noted however that even though the challenges were ranked in terms of the extent to which they are faced or continue to be faced, the respondents indicated that all the challenges listed in the questionnaire were faced to some extent.

5.3 Recommendations

The growing dependence of the organisations on computers-based systems means that the information they hold is a valuable corporate asset and as such, it must be the primary focus of corporate security. Consequently, anything that prevents the continuous access to this information jeopardises the firm's ability to conduct business in a timely and profitable manner. The protection of information requires the firm to identify information assets, classify them, define access, establish ownership, determine vulnerabilities and the consequences of compromise. These requirements can be managed through the development of information systems security policies.

The researcher proposes the following in order to reduce risks and enhance control and availability of information systems within large private manufacturing firms in Kenya: first, examine the organisation's short and long range strategic needs and develop policies regarding the establishment of guidelines on the use of computer systems. Integrate security into the capital planning and investment control process; proper planning and budgeting should be done for information system security planning.

Second, top management must authorise the establishment of the information security team and provide it with the necessary authority and resources to ensure compliance with information security procedures. In addition to this, management should be involved in information security program development, implementation and review. The comprehensive information system security program should address specific roles, responsibilities, and relationships for all entities; clearly defining interim objectives and milestones; setting time frames for achieving objectives; and establishing performance measures. In terms of the reporting structure, it should be noted that if the department reports too low in the organisation, the scope and authority of the

department would be too limited to be effective. In some cases the reporting location may also case conflicts of interest. Ideally, it should report directly to the CEO or president. On an annual basis short-term objectives should be identified to move the department toward meeting the long-term goals of security for the organisation. Short-term objectives may be installation of a new product or the creation of a process to monitor some aspect of security.

Third, the firms need to address the mentioned areas of susceptibility, with a view of reducing the vulnerability levels in order to minimise the repeated occurrence of the incidences reported.

Fourth, develop an overall information system security program to include all information processing systems.

Fifth, define and set procurement guidelines regarding justification and approval procedures for the purchase of all computer systems components for example hardware, software, communications.

Sixth, establish a pre-approved list of computer systems components and vendors. Standardise on one or two company brands; but have several sources of supply, particularly for hardware.

Seventh, guidelines must be provided regarding the connectivity of Local and Wide Area Networks, shared databases and up/down line loading with the servers from an operational and security perspective. Clearly articulate that compliance with software copyright laws and licensing agreements must be adhered to by all.

Eighth, in recommending controls and alternative solutions to minimise or eliminate identified risks, the following factors should be addressed: effectiveness of recommended options, legislation and regulation, organisational policy, and safety and reliability.

Ninth, proper contingency planning measures should be put in place and always tested and reviewed.

Tenth, constant review of management, operational and technical security controls.

Eleventh, develop regular comprehensive training programs of information systems security education, training and awareness across all staff lines in the organisation (general users, IT professionals, and security professionals).

Twelfth, the government must provide proper security policy legislation and regulation in order to leverage IT investment in this sector.

Thirteenth, improve information sharing on threats and vulnerabilities. Information sharing is a key element in developing comprehensive and practical approaches to defending against cyber and physical attacks, which could threaten the organisation's welfare. Information sharing needs to be enhanced both within the organisations and between organisations in the same sector. Forums should be created where ideas can be shared on how to implement certain countermeasures that are difficult or complex to implement. Also the use of VPNs and other known technologies can aid in reducing the level of risk.

Fourteenth, improve analysis and warning capabilities. More robust analysis and warning capabilities, including an effective methodology for strategic analysis and framework for collecting needed threat and vulnerability information, are still needed to identify threats and provide timely warnings. Such capabilities need to address both cyber and physical threats.

Prevention is the most effective approach to averting security problems. If an organisation has weak information systems security measures in place, how can they be strengthened? How much money does it take to create and maintain a strong information system security program? This cannot be easily answered. However, one thing is clear, a security program must have 3 things in order to be strong and successful: first, a well-defined mission, second, good relationships within the organisation and third, intelligent, knowledgeable security professionals.

5.4 Limitations of the Study

The study had certain limitations that should be taken into consideration when interpreting the findings.

First, the nature of this study required divulging security related information; as a result, some of the members in the sample considered it too sensitive and declined to respond to the questionnaire. If more members in the sample would have responded perhaps the results would have been richer.

Second, those who responded may not have given the exact security position given the sensitive nature of the information. If all the respondents gave an exact security position perhaps the results would have been richer.

Third, the study did not incorporate end-user views only IT managers and their assistants. Perhaps richer responses would have been obtained if end-user views were incorporated.

Fourth, there was lack of prior adequate information on information systems security in manufacturing, which would have provided a strong foundation for the study.

Finally, the time constraint made it impossible to collect more diverse data and increase the sample size. If more diverse data was collected and the sample size was increased, perhaps the results would have been richer.

5.5 Recommendations for further research

In the process of carrying out this research, a number of issues were not considered due to the limitations mentioned above. In addition to this, there are extensions to the study that can be undertaken given different scenarios or situations. These include:

First, to carry out a cross sectional analysis of information systems security in the manufacturing sector as whole.

Second, a detailed survey on Computer based Information systems security policies and programs implemented by government–owned manufacturing firms. .

Third, a risk analysis can also be done in relation to the implementation of Internet for the use of E-Commerce as a medium for trading by manufacturing firms in Kenya.

Fourth, the impact of computer crime to the growth of IT in the manufacturing sector in Kenya.

CHAPTER 6: REFERENCES AND BIBLIOGRAPHY

Aosa, E. (1992). '*An Empirical Investigation of Aspects of Strategy Formulation and Implementation within Large, Private Manufacturing Companies in Kenya'*, Unpublished Ph. D. Thesis. University of Strathclyde, Glasgow-Scotland.

Auerbach Publishers (a division of Warren Gorham and Lamont) (1995). *'Data Security Management'*, Boston, MA.

Bigsten, A. and Kimuyu, P. (2002). *'Structure and Performance of Manufacturing in Kenya (Studies in the African Economies)'*, Hampshire, England: Palgrave Macmillan

Brand, R. L. (1989). '*Coping With the Threat of Computer Security Incidents: A Primer from Prevention Through Recovery'*.

British Standards Institute (1993). *'A Code of Practice for Information Security Management'*.

Caelli, W., Longley, D., and Shain, M. (1991). '*Information Security Handbook'*, New York, NY: Stockton Press.

Carroll, J. M. (1995). '*Computer Security, Butterworth-Heinemann'*, Newton, MA

Dykman, C. A. (ed.) and Davis, K.C. (asc. ed.) (1992). '*Control Objectives -- Controls in an Information Systems Environment: Objectives, Guidelines, and Audit Procedures'*, 4th Edition, Carol Stream, IL: The EDP Auditors Foundation, Inc.

Fites, P. and Kratz, M. (1993). '*Information Systems Security: A Practitioner's Reference'*, New York, NY: Van Nostrand Reinhold.

GAO report number GAO-03-564T '*Information Security: Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures'*, April 08, 2003.

Gabrielson, B. C. (1995). '*INFOSEC Engineering, Security Engineering Services*', Chesapeake Beach, MD.

Institute of Internal Auditors Research Foundation (1991). *System Auditability and Control Report*. Altamonte Springs, FL: The Institute of Internal Auditors.

Jaikumar, V. (March 10, 2003). *'Manufacturing Firms Expect Modest IT Budget Increases Emphasis is on integration, supply chain and customer-facing projects'. COMPUTERWORLD* – Chicago.

KenCell Communications Ltd. (2002). '*Risk Management report: Fraud in GSM'.*

Kenya Association of Manufacturers (2002). '*The Members Register'.*

Kenya Government Ministry of Industry (1988). '*The Register of Industries'.*

Kenya Industrial Research and Development Institute (1997). '*The Directory of Industries'.*

Kephart, J. O. and White, S. R. (1993). *'Measuring and Modeling Computer Virus Prevalence,'* Proceedings, 1993 IEEE Computer Society Symposium on Research in Security and Privacy (ay 1993): 14.

Laudon K.C. and Laudon J.P. (2002). *'Management Information systems: Organisation and technology in the Networked Enterprise'*, New Jersey: Prentice Hall Ltd.

Lunt, T.(1992). '*Automated Audit Trail Analysis for Intrusion Detection'*, Computer Audit *Update*, April 1992. pp. 2-8.

Maiwald, E. and Sieglein, W. (2002). '*Security Planning and Disaster Recovery'*, New Delhi: Tata McGraw-Hill Publishing Company Ltd.

National Aeronautics and Space Administration (March 1990). '*Guidelines for Development of Computer Security Awareness and Training (CSAT) Programs'*. Washington, DC. NASA Guide 2410.1.

NIST's Computer Systems Laboratory publishes the *CSL Bulletin* series, 2002.

National Institute of Standards and Technology (October, 1994). '*Guideline for the Use of Advanced Authentication Technology Alternatives'*. Federal Information Processing Standard Publication 190.

National Research Council (1991). *Computers at Risk: 'Safe Computing in the Information Age'*. Washington, DC: National Academy Press.

National Research Council (1989). '*Growing Vulnerability of the Public Switched Networks: Implication for National Security Emergency Preparedness'*. Washington, DC: National Academy Press.

Nuegent, W., Gilligan, J., Hoffman, L., and Ruthberg, Z., (1985). '*Technology Assessment: Methods for Measuring the Level of Computer Security'*. Special Publication 500-133. Gaithersburg, MD: National Institute of Standards and Technology.

O'Brien, J. A. (1999). *'Management Information systems: Managing Information Technology in the Internetworked Enterprise'*. Boston, MA: Richard D. Inc.

Organisation for Economic Co-operation and Development (1992). '*Guidelines for the Security of Information Systems'*. Paris.

Pfleeger, C. P. (1989). '*Security in Computing'*. Englewood Cliffs, NJ: Prentice Hall.

Pfleeger, C., Pfleeger S., and Theofanos M., (1989). *'A Methodology for Penetration Testing.' Computers and Security.* 8(7), pp. 613-620.

Piller, C. (1993). '*Special Report: Workplace and Consumer Privacy Under Siege', MacWorld*, July 1993, pp. 1-14.

Richu, P. G. (1989*). 'Security Considerations for Computer Based Financial Systems in Kenya: The Case of Banks and Financial Institutions'*. Unpublished MBA Thesis. University of Nairobi.

Russell, D., and Gangemi, G.T. Sr. (1991). '*Computer Security Basics'*. Sebastopol, CA: O'Reilly and Associates, Inc.

Ruthberg, Z., and Tipton, H., (eds) (1993). *Handbook of Information Security Management*. Boston, MA: Auerbach Press.

Ruthberg, Z., Fisher, B., Perry W., Lainhart, J., Cox J., Gillen, M., and Hunt D., (2000). '*Guide to Auditing for Controls and Security: A System Development Life Cycle Approach'*. Special Publication 500-153. Gaithersburg, MD: National Institute of Standards and Technology.

Sager, I., Hamm, S., Gross, N., Carey, J., and Hoff, R. (February 21, 2000), '*Cyber Crime.' Business Week.*

U.S. General Accounting Office, Information Security (Sept. 24, 1996): Opportunities for Improved OMB Oversight of Agency Practices, GAO/AIMD-96-110. Washington, D.C.

Wasilwa, M. O. (2003). *'A Survey of Computer Security Vulnerability in the Banking Industry in Kenya,'* Unpublished MBA Thesis. University of Nairobi.

CHAPTER 7: APPENDICES

7.1 Appendix 1: List of Manufacturing Firms

1. AFRICAN HIGHLAND PRODUCE CO.
2. AFRO PLASTICS KENYA
3. ALFA FINE FOODS
4. ALPHA FOODS LTD
5. ALPINE COOLERS
6. ASSOCIATED BATTERY MANUFACTURE
7. ASSOCIATED MOTORS
8. ATHI RIVER MABLE AND GRANITE
9. ATHI RIVER MINNING
10. B.A.T
11. BAMBURI
12. BAYER
13. BETA HEALTHCARE
14. BEVERAGE SERVICES KENYA LTD
15. BIDCO INDUSTRIES
16. BIO FOODS PRODUCTS
17. BONAR EAST AFRICA
18. BROOKSIDE
19. BULK PHARMACEUTICALS
20. CABLES PLASTICS LTD
21. CADBURYS SCHWEPPES KENYA LTD
22. CAR AND GENERAL LTD
23. COCA COLA
24. COLGATE PALMOLIVE
25. COLOUR PRINT
26. COSMOS LTD
27. CROWN FOODS LTD
28. CROWN PAINTS
29. CUSSONS
30. DAWA PHARMACEUTICALS
31. DELMONTE
32. EAST AFRICA PACKAGING
33. EAST AFRICA PORTLAND CEMENT
34. EAST AFRICA SPECTRA
35. EAST AFRICAN CABLES
36. EAST AFRICAN GROWERS
37. EAST AFRICAN STANDARD
38. ELYS CHEMICAL INDUSTRIES
39. EVEREADY
40. EXCEL CHEMICALS LTD
41. FARMERS CHOICE
42. FIRESTONE EAST AFRICA LTD
43. GENERAL PRINTERS
44. GLAXO SMITHKLINE
45. GLOBAL ALLIED INDUSTRIES
46. GOLDEN BISCUITS
47. GRANGE PACK
48. HACO INDUSTRIES
49. HENKEL KENYA LTD
50. HOUSE OF MANJI
51. IT ANONYMOUS
52. JAMBO BISCUITS

53. KARTASI INDUSTRIES
54. KENAFRIC
55. KENPOLY MANUFACTURERS
56. KENTAINERS
57. KENYA BREWERIES LTD
58. KENYA CO-OPERATIVE CREAMERIES
59. KENYA KNITTING & WEAVING LTD
60. KENYA LITURATURE BUREAU
61. KENYA PLANTERS CO.OP UNION
62. KENYA TEA PACKERS (KETEPA)
63. KENYA WINES (KWAL)
64. KILIMANJARO PACKERS
65. KUGURU FOODS COMPLEX (SOFTA)
66. LAB AND ALLIED
67. LONDON DISTILLERS
68. LONGHORN
69. LYONS MAID
70. MABATI ROLLING MILLS
71. MAMBA TANKS
72. MASTERMIND TOBACCO
73. NAIROBI BOTTLERS
74. NAIROBI PLASTICS
75. NATION NEWSPAPER
76. NESTLE FOODS LTD
77. ORBIT CHEMICAL INDUSTRIES
78. PEMBE MILLERS
79. PICANA
80. PREMIER OIL MILLS
81. PROCTOR AND ALLAN
82. RECKITT AND BECKISER
83. REGAL PHARMACEUTICAL
84. ROTO MOULDERS
85. SADOLIN PAINTS
86. SARA LEE
87. SHELL CHEMICAL INDUSTRIES
88. SPIN KNIT LTD
89. SPINNERS AND SPINNERS
90. STANDARD NEWSPAPERS
91. SUPA LOAF BAKERIES
92. TETRA PAK
93. TOTAL KENYA
94. TRU FOOD LTD
95. TWIGA CHEMICALS INDUSTRIES
96. UNGA LIMITED
97. UNILEVER KENYA
98. WILHAM KENYA LTD
99. WIRE PRODUCTS
100. WRIGLEY

7.2 Appendix 2: Introduction Letter

VERONICA M. K. OGETO,
UNIVERSITY OF NAIROBI,
FACULTY OF COMMERCE,
DEPARTMENT OF MANAGEMENT SCIENCE,
P. O. BOX 30197,
NAIROBI.

To whom it may concern,

I am a postgraduate student in the faculty of Commerce, University of Nairobi, pursuing a Master of Business Administration degree programme. I am undertaking a research on Computer-Based Information Systems Security Implemented by Large Private Manufacturing Companies in Kenya. It is aimed at exploring the various information system security measures or approaches implemented by manufacturing companies in Kenya, the relative importance attached to the different security measures or approaches and finally, the challenges to implementing information system security in manufacturing companies in Kenya.

You have been selected as one of the respondent. I therefore request you to fill in the attached questionnaire. The information from the questionnaire is needed purely for academic research purposes and will therefore be treated with the utmost confidentiality. In no way will your name or the name of your manufacturing firm appear in the final report.

A copy of the final report can be made available to you upon request.

If you require any further information, please do not hesitate to contact me via the above address.

Thank you for your valuable co-operation.

Yours Faithfully,

Veronica Ogeto
MBA STUDENT

7.3 Appendix 3: Questionnaire

SECTION A: DEMOGRAPHIC CHARACTERISTICS

1) What is the ownership of your organisation? (*Mark (X) against only one)*
   Wholly foreign owned [ ]
   Wholly locally owned [ ]
   Jointly owned (foreign and locally owned) [ ]

2) How many years has your organisation been in operation in Kenya? _____

3) How many customers does your organisation have? _____

4) How many employees does your organisation have? _____

5) How many branches does your organisation have? _____

6) What is the total average annual turnover of your organisation in shillings? _____

7a) What is the level of Computer-based Information Systems utilisation in your organisation's operations?
   High [ ] Medium [ ] Low [ ]

b) What functions within your organisation are computerised?
   Payroll [ ]
   Stock Ordering [ ]
   Customer base Management [ ]
   Supplier base Management [ ]
   Payments Management [ ]
   Invoicing [ ]
   Computer Aided Design [ ]
   Computer Aided Manufacturing [ ]
   Other, Specify _____
   _____

8a) Do you have an Information Technology (IT) or Information Systems (IS) Department within your organisation? (*Mark (X) against only one)*
   Yes [ ] No (If 'No', skip to 9) [ ]

b) What is the position of the Information Technology department relative to other departments in the organisational hierarchy (e.g. is it under Finance or is it independent)?

_____

_____

c) Does your organisation have a budget for the IT or IS department? (*Mark (X) against only one)*
   Yes [ ] No [ ]

9) Indicate the ownership of your organisation's information systems components (*Mark (X) against only one)*

	Information Systems	In-House Only	Out-Sourced	Both
1	Hardware			
2	Software			
3	Operations			
4	Preventive Maintenance			
5	Other – Please specify			
6				
7				
8				
9				
10				

10) What types of computer networks does your organisation use? (*Mark (X) against all that apply)*

Local area network (LAN) [ ]
Wide area network (WAN) [ ]
Wireless network (e.g., 802.11) [ ]
Internet [ ]
Intranet [ ]
Extranet [ ]
Stand-alone PCs (not on LAN) [ ]
Other, Specify _____

11) What methods of processing does your organisation use? (*Mark (X) against all that apply).*

Online but not real-time [ ]
Real-time Online [ ]
Batch [ ]
Other. Specify _____

12) Which of the following types of access to networks does your organization's information systems support? (*Mark (X) against all that apply).*

Remote dial-in access [ ]
Access to networks through Internet [ ]
Other, Specify _____

13) Please answer the following question by *Marking (X)* in the box that best describes how would you rate computer literacy within your organisation for the following categories of staff? Use a 5 point scale where 5=excellent and 1=poor.

Categories Of Staff	Poor 1	Below Average 2	Average 3	Above Average 4	Excellent 5
Executive Director/CEO					
Top Management					
Middle Management					
Lower Management					
Other Staff					

14) How are information systems security services handled in your organisation? *(Mark (X) against only one).*

In-house only [ ] Contracted out only (e.g. Third Party) [ ] Both [ ]

15a) Does your organisation have an Information Systems Security policy? *(Mark (X) against only one).*

Yes [ ] No (If 'No', skip to 16) [ ]

b) How often is the information system security policy updated? (*Mark (X) against only one).*

Monthly [ ]
Quarterly [ ]
Semi-Annually [ ]
Annually [ ]
Any other (Specify) _____

16a) Does your organisation have an information systems security team or department? (*Mark (X) against only one).*

Yes [ ] No (If 'No', skip to 17) [ ]

b) Does the Information Systems security team or department include members of each business unit/department? *(Mark (X) against only one).*

Yes [ ] No [ ]

c) Do the members of the information systems security team or department have specific job descriptions? *(Mark (X) against only one).*

Yes [ ] No [ ]

d) Does the information systems security team or department have a budget? *(Mark (X) against only one).*

Yes [ ] No [ ]

17a) Does your organisation have an Information Systems Code of Conduct/Ethics? (*Mark (X) against only one).*
Yes [ ] No (If 'No', skip to 18) [ ]

b) Does the code cover information systems security? (*Mark (X) against only one).*
Yes [ ] No [ ]

18 Are your organisation's information systems assessed? *(Mark (X) against only one).*
Yes [ ] No (If 'No', skip to 19) [ ]

b) How often are your information systems assessed? (*Mark (X) against only one).*
Monthly [ ]
Quarterly [ ]
Semi-Annually [ ]
Annually [ ]
Any other (Specify) _____

c) Is the assessment conducted in-house or by third-party organisations? (*Mark (X) against only one).*
In-house [ ] Third-party organisations [ ] Both [ ]

SECTION B: IDENTIFYING COUNTERMEASURES TO INFORMATION SYSTEM SECURITY THREATS

19) Please answer the following questions by ticking in the box that best describes the degree or extent to which the people below are responsible for the security of the computers in your organisation. Use a 5 point scale where 5= Very Responsible and 1= Not at All.

	Not at All 1	Minimal Responsibility 2	Medium Responsibility 3	Above Medium Responsibility 4	Very Responsible 5
The computer users themselves					
The Internet Service Providers					
Program/Software vendors					
Hardware vendors					
The system administrators					
Consultants					
Others – Please specify					

20) Which of the following information system security incidents have occurred in your organisation? (*Mark (X) against all that apply)*

	Information System Security Incidents	Occurred? *(Mark (X) only if Yes - else leave blank)*
1	Embezzlement	
2	Fraud	
3	Theft of proprietary information	
4	Denial of service (to Internet connection or e-mail service)	
5	Vandalism or sabotage (electronic)	
6	Computer virus Attack	
7	Misuse of computers by employees	
8	Hardware Failure	
9	Software Failure	
10	Storage Facility Failure	
11	Communication Systems failure	
12	Processes and Procedures failure	
13	Clerical/Operator Errors	
14	Tapping of Transmissions	
15	Environmental Conditions Failure	
16	Unauthorised Access	
17	Others – Please specify	
18		
19		

21) Of the following information system security measures which ones are **available** within your organisation? And which ones have **systems/procedures in place to monitor for compliance**? (*Mark (X) against all that apply within the relevant columns).*

	Information System Security Measures	Available? *(Mark (X) only if Yes - else leave blank)*	Have Systems/ Procedures To Monitor For Compliance? *(Mark (X) only if Yes - else leave blank)*
1	A central policy/document that is the core of the information system security programme		
2	Security reporting to senior management		
3	Information Systems Code of Conduct/Ethics		
4	Formal project management or evaluation process for all new technology initiatives		
5	Mechanisms to test for software fixes and proper configurations		
6	Complete current systems and applications documentation		
7	A centralised logging system to gather log files		
8	Periodic review of system administrative logs		
9	Remote Access policies and procedures (authorisation, audit, etc..)		
10	Formal information systems security audit standards		
11	Periodic information systems security audits/review		
12	Training of employees in information systems security (User Awareness, Education)		
13	Implementation of Disaster recovery plan (DRP)		
14	Backup policies and procedures		
15	Off-site Backup		
16	Procedures for destroying unneeded sensitive files		
17	Encryption of information/data		
18	Virus management process (including Anti-virus software)		
19	Periodic review of Software inventory (count checks)		
20	Software Licensing Agreements for all software installed on servers and workstations		
21	Periodic review of Hardware inventory (count checks)		
22	Third party service provider agreements (consultants, vendors, etc.)		
23	Human Resource policies/procedures for screening new employees		
24	Physical/ Environmental security measures		
a)	Servers in a Locked Room with system and keyboard locks		
b)	Alternative source of power		
c)	Servers protected from smoke and fire damage		
d)	Overhead water and potential flood are avoided in the server room		
e)	Temperature Controlled Room		
f)	Humidity Controlled Room		
25	Technical security measures		
a)	Use of passwords		
b)	Different Levels of Access restrictions		
c)	Account deactivation on termination or transfer of employee		
d)	Alarms/Account lock if incorrect password more than 3 times		
26	Existence of a Firewall(s)		
27	Existence of E-mail logs/filters		
28	Existence of Intrusion detection system		
29	Other – Please specify		
30			
31			
32			

SECTION C: IDENTIFYING IMPORTANCE ATTACHED TO THE DIFFERENT APPROACHES

22) Within your organisation, what importance is attached to the following countermeasures? Use a 5 point scale where 5=Extremely important and 1= Not Important at all *(Mark (X) against all that apply within the relevant columns).*

	Information System Security Measures	Not Important at All 1	Minimal Importance 2	Medium Importance 3	Above Medium Importance 4	Extremely Important 5
1	A central policy/document that is the core of the information system security programme					
2	Security reporting to senior management					
3	Information Systems Code of Conduct/Ethics					
4	Formal project management or evaluation process for all new technology initiatives					
5	Mechanisms to test for software fixes and proper configurations					
6	Complete current systems and applications documentation					
7	A centralised logging system to gather log files					
8	Periodic review of system administrative logs					
9	Remote Access policies and procedures (authorisation, audit, etc..)					
10	Formal information systems security audit standards					
11	Periodic information systems security audits/review					
12	Training of employees in information systems security (User Awareness, Education)					
13	Implementation of Disaster recovery plan (DRP)					
14	Backup policies and procedures					
15	Off-site Backup					
16	Procedures for destroying unneeded sensitive files					
17	Encryption of information/data					
18	Virus management process (including Anti-virus software)					
19	Periodic review of Software inventory (count checks)					
20	Software Licensing Agreements for all software installed on servers and workstations					
21	Periodic review of Hardware inventory (count checks)					
22	Third party service provider agreements (consultants, vendors, etc.)					
23	Human Resource policies/procedures for screening new employees					
24	Physical/ Environmental security measures					
a)	Servers in a Locked Room with system and keyboard locks					
b)	Alternative source of power					
c)	Servers protected from smoke and fire damage					
d)	Overhead water and potential flood are avoided in the server room					
e)	Temperature Controlled Room					
f)	Humidity Controlled Room					
25	Technical security measures					
a)	Use of passwords					
b)	Different Levels of Access restrictions					
c)	Account deactivation on termination or transfer of employee					
d)	Alarms/Account lock if incorrect password more than 3 times					
26	Existence of a Firewall(s)					
27	Existence of E-mail logs/filters					
28	Existence of Intrusion detection system					
29	Other – Please specify					
30						

SECTION D: CHALLENGES IN IMPLEMENTING INFORMATION SYSTEMS SECURITY

23) To what extent did you face or continue to face the following challenges in implementing Information Systems Security in your organisation? Use a 5 point scale where 5=Great Extent and 1= None (No Extent at all) (*Mark (X) against all that apply within the relevant columns).*

	Information System Security Challenges	None (No Extent at all) 1	Minimal Extent 2	Moderate Extent 3	Above Moderate Extent 4	Great Extent 5
1	Developing a comprehensive information system security policy/program is time consuming					
2	Inadequate legislation governing information system security					
3	Lack of documented guidelines on how to prepare an information system security policy					
4	Lack of proper information system security planning					
5	Lack of a budget for information system security planning (capital planning)					
6	Lack of a budget for information system security implementation					
7	Lack of information sharing on threats and vulnerabilities within the organisation					
8	Lack of information sharing on threats and vulnerabilities between same sector organisations					
9	Lack of procedures of collecting evidence after a breach of information system security					
10	Lack of warning capabilities on threat and vulnerability information addressing threats to information systems					
11	Inadequate senior management attention to information security					
12	Inadequate accountability for job and program performance related to I.T. security					
13	Lack of proper mechanisms to facilitate periodic, information system security program review					
14	Limited security training for general users					
15	Limited security training for IT professionals					
16	Lack of security guidelines for contractor-provided services					
17	Some aspects of information system security are complex to implement					
18	Others (specify and rate)					
19						
20						

********** End ******** Thank you for your time and participation **********