A Computer Security Risk Analysis Of Firms Quoted In The Nairobi Stock Exchange.

BY

CYRUS KIPLIMO SANG

A Management Research Project Submitted
In Partial Fulfillment Of The Requirements
For The Degree Of Master Of Business And Administration (MBA)
Faculty of Commerce
University Of Nairobi.

October 2001

DECLARATION

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

Signed ______________________ Date 5th November 2001

CYRUS KIPLIMO.SANG

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

Signed ______________________ Date 8.11.01

MR. JULIUS KIPNG'ETICH.
Lecturer, Department of Management Science,
Faculty of Commerce, University of Nairobi.

DEDICATION

To my dear parents,
Christopher and Joan,
and siblings,
Crispus, Edwin, Alfred, Debra and Samson,
for their love and support.

ACKNOWLEDGEMENT

My sincere gratitude goes to all those individuals who in their own special ways contributed to the success of this study.

Most of all, I would like to thank my supervisor Mr. Julius Kipng'etich for his tireless guidance, support and patience throughout the project.

To my lecturers for the knowledge, wisdom and advice.

To my classmates for the valuable time and knowledge we shared, and the lessons in life we learnt together.

To my parents Christopher and Joan, and my siblings for the support, prayers and undying dedication to my well being through the successes and the many challenges we have faced together as a family.

To all my friend who I cannot name all here, for your continued encouragement, advice and support, thank you very much.

Abstract.

As computer literacy trend continues to grow, and there is no reason to believe that it won't, the statistical number of people capable of computer crime will increase substantially. While this fact paints a pretty grim picture of the future of information systems security, there is no need to get paranoid since the body of knowledge currently available is adequate to deal with to deal with these problems.

This study aims to determine the security posture of firms quoted on the Nairobi Stock Exchange. Out of a total of 54 companies only 34 responded to the questionnaires. This can be attributed to the fact that the study focused on security, which is a sensitive area.

This study had three basic objectives, these are:

1. To determine the current status of Information Technology resources within the organizations.
2. To determine the extent to which these organization's information systems are exposed to computer security risks.
3. To determine if there are sectoral differences with regard to exposure to computer security risks.

To meet these objectives data was collected using questionnaires and analyzed using various statistical tools including descriptive statistics, factor analysis, and discriminant analysis.

The findings of the study suggested that most of the organizations have made heavy investments in Information Technology. However very few have an Information Technology professional at the executive board level.

The findings of this study also indicates that the Finance and Investments sector and the Commercial and Allied sector have the most secure systems since their vulnerability levels to the susceptibilities considered in this study are all acceptable. The Agricultural sector has the most insecure system compared with the other sectors and is susceptible to six vulnerability areas.

TABLE OF CONTENTS

Declaration……………………………………………………………………**II**
Acknowledgement………………………………………………………………**IV**
Abstract…………………………………………………………………………..**V**
List of Tables…………………………………………………………………..**VII**

Chapter One: Introduction………………………………………………………**1**
1.1: Background of Study……………………………………………………..1
1.2: Statement of the Problem…………………………………………………6
1.3: Objectives of the Study…………………………………………………..8
1.4: Importance of the Study…………………………………………………8

Chapter Two: Literature Review…………………………………………………**9**
2.1: Common Threats to Computer Systems………………………………..9
2.2: Internet Security……………………………………………………………13
2.3: Previous Studies and Findings……………………………………………16
Chapter Three: Research Methodology…………………………………**18**
3.1: Population of Study…………………………………………………………18
3.2: Data Collection Method……………………………………………………19
3.3: Data Analysis Techniques…………………………………………………..20

Chapter Four: Results and Data Analysis……………………………………**22**
4.1: Summary of Responses………………………………………………….22
4.2: Status of IT Resources in the Organizations…………………………..23
4.3: Risk Analysis………………………………………………………………..35
4.4: Factor Analysis…………………………………………………………..…39
4.5: Discriminant Analysis…………………………………………………..….45
4.6: Perceived Security Risk Related Problems………………………………49

Chapter Five: Summary and Conclusions……………………………………**52**
5.1: Conclusions on Status of IT Resources…………………………………52
5.2: Conclusions on Risk, Factor and Discriminant Analysis…………..53
5.3: Conclusions on Perceived Risk…………………………………………55
5.4: Recommendations……………………………………………………………56
5.5: Limitations of the Study………………………………………………...57
5.6: Suggestions for Further Research………………………………………57

Appendices……………………………………………………………………**58**
Appendix I - Listed of Companies on the Nairobi Stock Exchange. …58
Appendix II – Questionnaire……………………………………………...60
Appendix III – List of Vulnerabilities………………………………………68
Appendix IV – Cover Letter…………………………………………………69

References and Bibliography……………………………………………**70**

LIST OF TABLES.

Page.

Table 3.1: Number of Companies listed in the NSE....................................18
Table 4.1: Summary of Responses..22
Table 4.2.1: Ownership of Companies...23
Table 4.2.2: First Computer Installation...24
Table 4.2.3: Number of Computers..25
Table 4.2.4: IT Director's Position...27
Table 4.2.5: Investments in Computer Systems...27
Table 4.2.6: Previous Year IT Budget...28
Table 4.2.7: Acquisition Policy for Hardware and Software...........................29
Table 4.2.8: Internet and World Wide Web Access......................................30
Table 4.2.9: Computer Security Policy..30
Table 4.2.10: Security Reviews..31
Table 4.2.11: Security Budgets..32
Table 4.2.12: Computer Literacy...33
Table 4.2.13: Information Systems...34
Table 4.2.14: IT Strategic Plan..35
Table 4.3.1: Vulnerability Levels..36
Table 4.4.1: List of Variables..39
Table 4.4.2: Correlation Matrix..40
Table 4.4.3: Principal Component Analysis Output......................................41
Table 4.4.4: Initial Factor Loadings Matrix...42
Table 4.4.5: Varimax Rotated Factor Matrix...43
Table 4.4.6: Factors and Vulnerabilities..44
Table 4.4.7: Vulnerability Level per Factor...45
Table 4.5.1: Standardized Canonical Discriminant Function Coefficients............46
Table 4.5.2: Discriminant Loadings...47
Table 4.5.3: Mean Discriminant Scores...48
Table 4.5.4: Confusion Matrix of Actual Versus Predicted Group Membership....48
Table 4.6.1: Perceived Security Risk Related Problems.................................49

Chapter One

Introduction.

1.1. Background of Study.

" Risk Analysis helps establish a good security posture; Risk Management keeps it that way."(Jenkins,1998).

Survival in today's highly competitive business world depends to a greater extent on an organizations ability to adapt to the volatility of changing pressures brought on by the often, unpredictable swings in socio-economic, technological, and political conditions. With the advent of the Personal Computer (PC), organizations quickly discovered that individuals and groups using PC's responded faster to these dynamic situations.

Organizations rapidly embraced the dream of higher efficiency, increased staff productivity and a sharper competitive edge provided by microprocessor[1] armed field representatives and PC equipped headquarters staff as part of the overall strategy of maximizing value to the shareholder.

Individuals realized that this was an opportunity to free them from the highly structured and formalized manner of processing information and place the power of the microchip[2] on their desk and at their fingertips. The lid to a Pandora box had been opened. The personal computer and distributed processing had come of age. Fresh and new ideas, new companies, careers, industries, problems and solutions were waiting in the wings to make their debut.

Given the high level of competition between suppliers of personal computers and the

[1] A Microprocessor is the central unit of a computer that contains the logical elements of manipulating data and performing arithmetical or logical operations on it.

[2] A Microchip is a small piece of silicon that contains the essential elements of a central processor including the control logic, instruction decoding, and arithmetic processing circuitry.

seemingly endless parade of hardware[3] and software[4] upgrades, computers have become affordable to more organizations and individuals. The problem of computer security[5] and control begins to take root and grow because any serious breach may mean the very end of the organization.

Because the relative cost of computers is so low, without the proper controls, they can easily be purchased out of existing budgets and never show up as a distinct line item.

There is, however, a need to implement security and control measures early in the game. Otherwise you may face the very difficult task of trying to regain control and change the behavior patterns of people who have long been out of control.
If allowed to continue unchecked and without direction, people will purchase those PC's that they think are the best ones for their job at hand. Naturally, without expertise in the hardware, software and communications areas, they can easily make the wrong system selection and before long the organization can find itself with a great many PC's from different vendors utilizing different operating systems requiring diverse security administration procedures.

This can present the Information Systems Manager with a compatibility nightmare when it comes to securing logical access controls[6], audit packages, encryption[7] systems and so on. In addition, there can be a very significant backup and disaster recovery contingency planning problem to deal with, as a result of multi-vendor systems operating in a multi-platform environment.

Fast in the heels of this potential problem, the user soon convinces other users that the organization should seriously consider the installation of a Local Area Network[8] (LAN). Now in addition to the problem of

[3] Hardware is the physical computer equipment, for example, mechanical, magnetic, electrical, or electronic devices.

[4] Software refers to the stored set of instructions which govern the operation of a computer system and make the hardware run.

[5] Computer security is the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information resources (including hardware, software, firmware, data, information, and telecommunications).

[6] Logical access controls are the system-based means by which the ability to do something with a computer resource is explicitly enabled or restricted in some way.

[7] Encryption is the conversion of data into code form for security purposes during data communications. The data is reconverted at the receiving end.

[8] A Local Area Network is a system for linking terminals, programs, storage, and graphic devices at multiple workstations over relatively small geographical areas for rapid communications and resource sharing.

providing security at the local department level in one building, we are now significantly increasing our risk exposure with the introduction of one or more user networks located anywhere in the world subject to the wide array of operational security threats[9] and vulnerabilities[10] at each of those locations.

Over the second half of the 20th Century, the world has seen dramatic changes to the role of information in the human experience. Information has become the dominant component of almost all aspects of society. Of crucial importance in facilitating this change were technological and social trends that have impacted almost every aspect of our lives. We have witnessed the development of more efficient means of information processing that have significantly changed our ability to obtain, transmit and evaluate data. Simultaneously, we have become more aware of other cultures and peoples, a change which has made the world smaller but our horizons broader.

For the business world, these trends have been of radical significance. In order to be competitive in today's information based marketplace, a company must provide immediate access to facts about its products, strategies and basic financial indicators.

This means that the relevant information must be available globally and immediately to a widely dispersed employee base and partners.

The solution to these needs is through intranets[11] and extranets[12].

As most companies are quickly realizing, the most effective way to take advantage of these solutions is by combining them into a new communications paradigm: the Enterprise Network (EN)[13]. The EN crosses networking backbones, services and applications to lay a foundation on which information is distributed and stored, for internal as well as external uses.

[9] A threat is an entity or event with the potential to harm the system.

[10] A vulnerability is a condition or weakness in (or absence of) security procedures, technical control, physical controls, or other controls that could be exploited by a threat.

[11] Intranets are LANs that use the protocol used by Internet (i.e. TCP/IP- Transmission Control Protocol/Internet Protocol), and are for the sole use of people within one organization.

[12] Extranets are intranets that allow for connections to specific parties outside the organization.

[13] The Enterprise Network is a collective entity that unifies all aspects of a company's communications infrastructure by encompassing different information technologies

Lying at the heart of the EN is the capability to control exactly what information is available to whom and when. Security mechanisms, therefore, play an integral role (Rembaum, 1999).

Rembaum (1999), notes that the proliferation of the Internet[14] has broken down traditional boundaries to international communication. It has linked peoples and worlds otherwise separated by physical and emotional barriers, and it has provided an inexpensive yet quite reliable means for inter-organizational information sharing and data transfer.

Evans (1994) argues that security has always been an important factor in the computer environment, but in the past has often not received the attention it merits. Computer systems are widely used, are becoming more complex and more information is being held on computer files, in short, we are coming to rely upon them for the success of our businesses. For this reasons security requires greater attention from computer professionals. Computer systems must be secure, not only against accidental failure during running, but also against deliberate misuse and improper access of data.

Generally we are concerned with the threat to the information held on the computer system. According to Evans (1994), these threats can be categorized into two classes, namely, accidental risks and deliberate risks. These threats can result in four types of losses:

- Loss of availability and reliability
- Loss of accuracy and integrity
- Loss of confidentiality and privacy
- Loss of business assets and fraud.

Accidental risks can be caused by: equipment malfunction or failure; natural hazards; failure of public utilities or ancillary equipment; and human errors.

Deliberate risks can result from: theft; illegal access; espionage; and sabotage.

[14] The Internet is a worldwide computer network linking countless thousands of computer networks, through a mixture of private and public data and telephone lines. Its component networks are individually run by government agencies, universities, commercial and voluntary organizations. No single organization owns or controls the Internet, though there is an Internet Society that co-ordinates and sets standards for its use. Networks are connected by gateways that effectively remove barriers so that one type of network can "talk" to a different type of network.

Equipment failure can vary from simple malfunction of a device to complete breakdown of a major assembly. All electromechanical devices have a lifetime and are bound to fail sooner or later hence affecting the continuity of information processing.

Natural hazard resulting from fire, water, sun, humidity, and dust can affect equipment and ancillaries; in particular the magnetic media is the most vulnerable. There is also the heat generated by the electrical equipment, which can be a potential hazard and hence should not be neglected.

The effects of failure of the public utilities such as electrical supplies and telecommunications can be far reaching unless adequate 'fail safe' procedures have been designed for the installation. Intermittency in the availability of the electrical supplies and communication circuits can have serious effects on the transfer of data unless adequate precautions against these contingencies have been arranged.

It must always be accepted that no manual procedure is entirely reliable and for that reason systems should be designed to minimize human intervention.
Always with the best of intentions, experienced operators, will call systems software to override checks and cautions provided in the program often with disastrous results. Carelessness in an output section, where a high volume of paper is usually present, can often nullify the effects of well-planned and executed procedures up to that point.

There has been a tendency to believe that information held within a computer installation is to some extent naturally secure by virtue of its great mass and by the peculiar nature of the media upon which it is stored. Adams (1994), notes that this may have been true of the past when the knowledge of computers was restricted and when computers were few and far between. The rapid growth of knowledge about computers, their proliferation and the development of freely available software packages makes this belief no longer true.

There are many ways perpetrators may deliberately gain access to the organizations data, these include:

- Temporary removal of stored information
- Copying of information in one form or another
- Deliberate mis-routing of information to unauthorized recipients
- Planted devices to record or retransmit electronic emissions from computer hardware.

Wilk (1993) argues that the increasing use of computers by commercial, government and law enforcement organizations has resulted in large concentrations of data and assets in a system, which has become the favorite target of dissident groups. The computer has occasionally been a target for anti-establishment rebels, anti-war protesters and rampaging students. This has resulted in a number of serious sabotage attacks on computer centers. The height of this activity was felt during 1970 when the U.S. Army Mathematics Research Center at the University of Wisconsin was bombed, resulting in the death of a research employee and the destruction of a 1.5 million dollar computer system complex with between 5 and 6 million dollars damage to the facility. Data which has been collected over a 20 year period and represented 1.3 million man hours of effort was also irretrievably lost (Wilk, 1993).

1.2. Statement Of the Problem

In the early days of computer systems development some sense of security was derived from the fact that a great deal of specialized knowledge and expensive equipment were required to penetrate computer systems (Wilk, 1983). However, in today's rapidly advancing technological world we can no longer use the umbrella of technical complexity to shield our organizations computer systems from manipulation by unauthorized persons. On the contrary the low cost and ease of usage of microprocessors in the hands of an increasingly knowledgeable adversary, tempted by the availability of cash at Automated Teller Machine's and the opportunity to convert Electronic Funds Transfer transactions to cash, coupled with a low probability of discovery, capture, conviction and punishment promise to make computer systems more vulnerable. According to Wilk (1983), sophisticated adversaries are constantly performing their own risk analysis of your computer systems: probing for soft spots, weaknesses and operational vulnerabilities, which they can convert to their own advantage.

The growing demand on business, technology and networking often result in conflicting demands being placed on a corporate network. Many times, the balance between data sharing, and security are in conflict. The need to add system components, system utilities, and functional capabilities can result in corporate network configurations growing in a haphazard, and often insecure manner.

The fears surrounding network security, made all the more acute with the recent wave of high profile successful hacks, and the search for cheaper means of connectivity have generated the need for organizations to assess their security posture.

According to Jenkins (1998), security measures cannot assure 100% protection against all threats. Therefore, risk analysis, which is the process of evaluating system vulnerabilities and the threats facing it, is an essential part of any risk management program.

A study by Richu (1989), on the security considerations for computer based financial information systems in Kenya, found that most of the risks perceived by the management of commercial banks and financial institutions were of a physical nature e.g. fire, power surges and floods. Other risks were not given sufficient considerations. The study also found that the major threat facing computerized systems was the company's own employees. The study concluded that the computer security systems were not adequate, and that most of the managers were unaware of the major potential risks their computerized systems faced.

The researcher in this study intends to widen the scope of this earlier study by conducting a risk analysis of the companies quoted in the Nairobi Stock Exchange(NSE).
Violino(1993) notes that financial systems are not the only ones at risk. Systems that control access to any resource are targets for example inventory systems.

The growing dependence and increased investment in computer based information systems by the companies listed on the NSE, as found out by Dizon (1999), creates the need to conduct a risk analysis to determine the level of vulnerabilities of their computer systems. The impact of down time on organizations that are dependent on computer based information systems can be significant. This is because it can lead to lost business opportunities, loss of customer confidence, the inability to make a decision and gradual deterioration of the organization. This process is further accelerated when online systems provide the majority of services to systems users and customers.

The researcher in this study intends to find answers to the following questions:

- What is the attitude of Information Systems Managers towards countermeasures against computer related security risks ?
- What are the vulnerability levels of the organizations computer systems to security risks ?
- What factors pose the most risk to computer systems as perceived by Information Systems Managers.

1.3. Objectives of the Study

1. To determine the current status of Information Technology resources within the organizations.
2. To determine the extent to which these organization's information systems are exposed to computer security risks.
3. To determine if there are sectoral differences with regard to exposure to computer security risks.

1.4. Importance of the Study

1. This study will provide an organizations management with an objective assessment of its information system security posture.
2. Risk analysis aids in developing a security strategy and provides the basis for establishing a cost-effective security program that minimizes the effects risk.
3. It will assist the government in developing regulations concerning Data protection and computer security
4. This study is expected to form a basis for further research in the area of computer security.
5. For manufacturers and vendors of computer equipment and accessories this will assist in determining the need for security products.

Chapter Two.

Literature Review.

2.1. Common Threats To Computer Systems.

Computer systems are vulnerable to many threats that can inflict various types of damage resulting in significant losses. This damage can range from errors harming database integrity[15] to fires destroying entire computer centers. Losses can stem, for example, from the actions of supposedly trusted employees defrauding a system, from outside hackers[16], or from careless data entry clerks. Precision in estimating computer security-related losses is not possible because many losses are never discovered, and others are "swept under the carpet" to avoid unfavorable publicity. The effects of various threats vary considerably: some affect the confidentiality or integrity of data while others affect the availability of a system.

To control the risks of operating an information system, managers and users need to know the vulnerabilities of the system and the threats that may exploit them. Knowledge of the threat environment allows the system manager to implement the most cost-effective security measures. In some cases, managers may find it more cost-effective to simply tolerate the expected losses. Such decisions should be based on the results of a risk analysis.

2.1.1. Errors and Omissions

Errors and omissions are an important threat to data and system integrity. These errors are caused not only by data entry clerks processing hundreds of transactions per day, but also by all types of users who create and edit data. Many programs, especially those designed by users for personal computers, lack quality control measures. However, even the most sophisticated programs cannot detect all types of input errors or omissions. A sound awareness and training program can help an organization reduce the number and severity of errors and omissions.

[15] Integrity is a quality of information; it is its goodness, honesty, reliability and freedom from unauthorized modification.

[16] A Hacker is a person who is intensely interested in and/or very knowledgeable about computer hardware and software, and can break into computers without authorization.

Users, data entry clerks, system operators, and programmers frequently make errors that contribute directly or indirectly to security problems. In some cases, the error is the threat, such as a data entry error or a programming error that crashes a system. In other cases, the errors create vulnerabilities. Errors can occur during all phases of the systems life cycle. A long-term survey of computer-related economic losses conducted by Robert Courtney, a computer security consultant and former member of the Computer System Security and Privacy Advisory Board, found that 65 percent of losses to organizations were the result of errors and omissions (Gaithersburg, 1992). This figure was relatively consistent between both private and public sector organizations.

Installation and maintenance errors are another source of security problems. For example, an audit by the United States President's Council for Integrity and Efficiency (PCIE) in 1988 found that every one of the ten mainframe computer sites studied had installation and maintenance errors that introduced significant security vulnerabilities (PCIE, 1988).

2.1.2. Fraud Theft.

Computer systems can be exploited for both fraud and theft both by "automating" traditional methods of fraud and by using new methods. For example, individuals may use a computer to skim small amounts of money from a large number of financial accounts, assuming that small discrepancies may not be investigated. Financial systems are not the only ones at risk. Systems that control access to any resource are targets (e.g., time and attendance systems, inventory systems, school grading systems, and long-distance telephone systems).

Insiders or outsiders can commit computer fraud and theft. Insiders (i.e., authorized users of a system) are responsible for the majority of fraud. A 1993 *InformationWeek*/Ernst and Young study found that 90 percent of Chief Information Officers viewed employees "who do not need to know" information as threats (Violino, 1993).

Since insiders have both access to and familiarity with the victim computer system, including what resources it controls and its flaws, authorized system users are in a better position to commit crimes. Insiders can be both general users (such as clerks) and technical staff members. An organization's former employees, with their knowledge of an organization's operations, may also pose a threat, particularly if their access is not terminated promptly.

In addition to the use of technology to commit fraud and theft, computer hardware and software may be vulnerable to theft. For example, one study conducted by Safeware Insurance found that $882 million worth of personal computers was lost due to theft in 1992 (*Infosecurity News*,1993).

2.1.3. Employee Sabotage

Employees are most familiar with their employer's computers and applications, including knowing what actions might cause the most damage, mischief, or sabotage. The downsizing of organizations in both the public and private sectors has created a group of individuals with organizational knowledge, who may retain potential system access (Sprouse, 1992). The number of incidents of employee sabotage is believed to be much smaller than the instances of theft, but the cost of such incidents can be quite high.

Sprouse (1992), in Sabotage in the American Workplace, reported that the motivation for sabotage can range from altruism to revenge.

As long as people feel cheated, bored, harassed, endangered, or betrayed at work, sabotage will be used as a direct method of achieving job satisfaction, the kind that never has to get the bosses' approval.

2.1.4. Loss of Physical and Infrastructure Support

The loss of supporting infrastructure includes power failures (outages, spikes, and brownouts), loss of communications, water outages and leaks, sewer problems, lack of transportation services, fire, flood, civil unrest, and strikes. A loss of infrastructure often results in system downtime, sometimes in unexpected ways.

2.1.5. Malicious Hackers.

The term malicious hackers, sometimes called crackers, refers to those who break into computers without authorization. They can include both outsiders and insiders. Much of the rise of hacker activity is often attributed to increases in connectivity in both government and industry. One 1992 study of a particular Internet site (i.e., one computer system) found that hackers attempted to break in once at least every other day (Bellovin,1993).

The hacker threat should be considered in terms of past and potential future damage. Although current losses due to hacker attacks are significantly smaller than losses due to insider theft and sabotage, the hacker problem is widespread and serious. One example of malicious hacker activity is that directed against the public telephone system.

2.1.6. Industrial Espionage

Industrial espionage is the act of gathering proprietary data from private companies or the government for the purpose of aiding another company (Charney, 1993). Industrial espionage can be perpetrated either by companies seeking to improve their competitive advantage or by governments seeking to aid their domestic industries. Foreign industrial espionage carried out by a government is often referred to as economic espionage. Since information is processed and stored on computer systems, computer security can help protect against such threats; it can do little, however, to reduce the threat of authorized employees selling that information.

2.1.7. Malicious Code

Malicious code refers to viruses[17], worms[18], Trojan horses[19], logic bombs[20], and other "uninvited" software. Sometimes mistakenly associated only with personal computers, malicious code can attack other platforms.

A 1993 study of viruses found that while the number of known viruses is increasing exponentially, the number of virus incidents is not (Kephart, 1993). The study concluded that viruses are becoming more prevalent, but only "gradually."

[17] A virus is a code segment replicates by attaching copies of itself to existing executable files, and usually causes damage to the data or hardware.

[18] A worm refers to computer program code, which is capable of automatic invisible self-replication to other machines, either via a network of communication links or through normal magnetic data storage media. Other worms also fill disk space with garbage. A worm will consume computer-time and space but will have no other detrimental side-effects.

[19] A Trojan refers to a special portion of computer program code, which may be attached to a bonafide program in such a way as to remain substantially undetected.

[20] A logic bomb is a program code introduced by an adversary that can modify, disrupt, or destroy a computer system /files at some pre-determined time, or after a particular sequence of operations.

The rate of PC-DOS virus incidents in medium to large North American businesses appears to be approximately 1 per 1,000 PCs per quarter; the number of infected machines is perhaps 3 or 4 times this figure if we assume that most such businesses are at least weakly protected against viruses (Kephart, 1993).

Actual costs attributed to the presence of malicious code have resulted primarily from system outages and staff time involved in repairing the systems. Nonetheless, these costs can be significant.

2.1.8. Foreign Government Espionage

In some instances, threats posed by foreign government intelligence services may be present. In addition to possible economic espionage, foreign intelligence services may target unclassified systems to further their intelligence missions. Some unclassified information that may be of interest includes travel plans of senior officials, civil defense and emergency preparedness, manufacturing technologies, satellite data, personnel and payroll data, and law enforcement, investigative, and security files. Guidance should be sought from the cognizant security office regarding such threats.

2.1.9. Threats to Personal Privacy

The accumulation of vast amounts of electronic information about individuals by governments, credit bureaus, and private companies, combined with the ability of computers to monitor, process, and aggregate large amounts of information about individuals have created a threat to individual privacy. The possibility that all of this information and technology may be able to be linked together has arisen as a specter of the modern information age.

2.2. Internet Security.

With the development and increased use of the Internet have come new communications opportunities, as well as challenging security problems. The Internet is an almost ideal means for information retrieval and exchange. It is cost- effective, easy to use and accessible in nearly every major city of the world. Similarly, the Internet is a shared media, to which millions of users are connected, and there are very few regulations on how it is to be used. And just as these traits make it an attractive method for honest activity, so too do they make it a very efficient medium for devious tasks such as data tampering, eavesdropping and theft.

These contradictory aspects of the Internet revolution seemingly place a tremendous hurdle in the way of the business community's embracing of the Internet.

Using the infrastructure of the Internet, intranets breakdown the walls within the organization, bringing all computers, software, and databases into a single system that enables employees to find information wherever it resides. These virtual corporate networks, however, are not without audit and security risks.

Whenever a company or individual is connected to the Internet, the individual is exposed to security threats. Insecurity problems on the Internet largely emanate from the technology used for accessing the Internet. To access the Internet, a Web browser[21] software is usually run on the users computer. The user's browser communicates with the browser running on the Web Server[22] at an Internet Service Provider's(ISPs)[23] office.

There are several common threats posed by using Web browsers and their enhancement features such as programming tools and plug-ins. These include privacy violations, malicious programs, the interception of sensitive or confidential information, and forged or redirected information.

2.2.1. Privacy Violations.

Probably the most common threat faced by users is the acquisitions by the third parties of personal information on freely given data. The type of information that may be collected by Web servers when you unwittingly visit a hostile web site include: information about your computer; your entire browser navigation history; your E-mail address; and other files on your computer, which may be read or copied to a remote system.

[21] A Web browser is a software application, which allows you to view information on the World Wide Web. The World Wide Web is a collection of linked documents or pages that span the Internet.

[22] A Web server is a powerful computer that enables browsers to access the resources of the Internet.

[23] Internet Service Providers are organizations, which maintain local area networks that are attached to the Internet and have dial up and leased line access via modems.

2.2.2. Malicious Programs.

Due to the complexity of the programming extensions added to many web browsers, there are numerous reports of security-related software bugs that may allow malicious Web based programs to damage or compromise your computer.

Usually, malicious Web-based programs attempt to: read, copy or destroy sensitive files; install software which may lead to further system compromise or capture of information; or cause the browser to crash or use excessive computer resources.

2.2.3. Electronic mail Insecurity.

Mail protocols that are used in e-mails are essentially a series of plain text commands, which mail servers use to send messages to each other. This is what makes e-mail insecure-plain-text communications that can easily be read, intercepted, modified or forged. Electronic mail is therefore not a secure service. For example, it is possible for unauthorized individuals to monitor the transmission of mail or to send counterfeit mail under your name.

2.2.4. Redirected Information.

Another area of concern, although not widely exploited, is the possibility that the users may visit web sites, which appear to be legitimate, but are in fact forged or redirected versions. The intent of such an attack would be to capture information provided by the visitor, such as credit card numbers or other confidential data.

2.3. Previous Studies and Findings

There have been a number of recent studies on computer security. Garry (1999), in the second annual Ernst & Young Global Information Security Survey canvassed the opinions of more than 4,254 companies in 29 countries spanning North and South America, Europe, Africa and Australasia. All the main industry groups were represented. The Key findings in this study are as follows:

- Information security risks are increasing. A total of 57 per cent of companies say their risks are higher now than a year ago; only 4 per cent say their risks have reduced. Among the business drivers that have increased information security risks are: the development and expanded roll-out of corporate intranets with Internet connectivity; the roll-out of e-commerce; the adoption of integrated enterprise-wide information systems to support business processes; the increased access to information, both upstream and downstream, in the supply chain.
- A total of 75 per cent of senior managers rate information security as "important" or "extremely important", but their concern is not reflected in organizational procedures: 30 per cent of companies have no formal policies and procedures relating to information security, and 23 per cent provide no awareness training.
- A total of 45 per cent of companies make no budget allowance for information security and 41 per cent have no budget for business continuity programmes.
- The most common causes of financial loss are system failure (76 per cent of companies), inadvertent errors (66 per cent), and viruses (49 per cent). There were less frequent reports of losses through malicious acts by employees (24 per cent), natural disasters (14 per cent) and malicious acts by outsiders (13 per cent).
- Companies are generally more concerned about external than internal threats. Hackers (53 per cent) and unauthorized users (49 per cent) are rated a greater threat than current employees/ authorized users (31 per cent). This is despite evidence that mischief or simple errors perpetrated by employees are responsible for most financial losses.
- Network security is a continuing concern: 78 per cent of organizations are not confident their network is safe from internal attack, while 50 per cent lack confidence about their security against external attack.
- Sixteen per cent of firms have suffered, or believe they may have suffered, at least one break-in via the Internet. Of those ,75 per cent had a firewall in place.

- Ninety per cent of organizations with a connection to the Internet rated their security as "poor" and 43 per cent assessed the security of their Internet-based services, such as e-mail and web access, as no better than "fair".
- Most organizations us firewalls (77 per cent) and passwords (67 per cent) as their main Internet security. Only 25 per cent have implemented any form of data encryption.

A wide- ranging study such as this provides many lessons as to how companies should approach the pressing issue of information security. Garry (1999), argues that no organization can afford to build risk-free systems, but it is the responsibility of senior management (not IT personnel) to decide what levels of risk are acceptable and to commit resources to ensure a uniform level of security across all key systems. The extent to which organizations can follow best practice solutions will depend to some degree on financial resources, but management should not treat this as purely a budget issue. It is not a question of investing in expensive software or hardware to "fix" the problem. Good security relies on a chain of related events, carefully planned and coordinated, some of which involve little or no cost. At the start of the chain must be the commitment and involvement of senior management. They are the only people able to assess information security in an overall business context. They should recognize that security is an enabler of new business services, products and delivery systems which , if operated in a secure environment, will deliver a sustainable competitive advantage.

Another study was conducted in the United Kingdom and Ireland on nearly 15,000 finance directors (or equivalent) of organizations with an annual turnover in excess of 10 million Sterling Pounds by KPMG, a leading audit and consulting firm, with the objective of gaining information about attitudes towards computer security and measures taken to secure information, White(1996). The study found that, in general , the contents of the security policies in these organizations reflected the still prevailing view that security policies are primarily concerned with physical and logical security, and PC issues such as viruses and software copying. Yet according to White(1996), to address information security adequately the information requirements of the organization must be clearly understood – which implies both the classification of information as assets, and a security culture, with a clear allocation of security responsibility and the means to record and react to incidents.

Chapter Three.

Research Methodology

The Chapter describes the research design of the study.

3.1. Population of Study

The population of the study consists of all the firms that are currently listed in the Nairobi Stock Exchange (NSE).

The choice of these companies was based on the fact that they are fairly large and well established and hence deemed to have substantial investment in Information Technology(IT). This is supported in a study by Dizon(1999).

These Companies also represent a cross-section of the economic sectors and hence will provide a greater scope of study.

Since the population was not considered too large, it was decided that no sampling would be done and instead the entire population will be studied.

The population consists of 54 Companies as listed in Appendix 1.
The list is further summarized by sector in Table 5.1 below.

Table 3.1: Number of Companies listed in the NSE (as at May 2000)

SECTOR	NUMBER OF COMPANIES
Industrial & Allied	18
Finance & Investment	13
Commercial & Allied	14
Agricultural	9
Total	**54**

3.2. Data Collection Method

The information sought in this study is to be collected using a structured and undisguised questionnaire to gather primary data. The questionnaire consists of both open-ended and close-ended questions. The questions were developed from the study of pertinent literature.

The questionnaire consists of three sections (See Appendix II).

Section A will be used to gather general information about the organization in relation to the systems in operation.

Section B will be used to gather the Information Systems Managers attitude toward various computer security countermeasures. The countermeasures are obtained from the literature reviewed. The manager's attitudes towards these countermeasures will be used to determine the current level of vulnerability. The countermeasures are scaled on a likert-type-scale.

Several studies have shown that there is a relationship between an individual's attitude or beliefs and behavior. Festinger (1957), in his cognitive dissonance theory, says that there is a tendency for individuals to seek consistency among their cognitions (i.e. beliefs and opinions). Festinger's theory is further supported by a study by Cooper,Zanna, and Taves (1978), which found that individuals exhibit attitude change to appear more consistent with their behaviors.

The cognitive dissonance theory proposed by Festinger (1957) is not the only means of explaining the relationship between attitude and behavior. Some researchers favour the self-perception theory, first presented by Bem (1967). Bem's theory of self-perception states that when a persons attitudes pertaining a particular subject or behavior are weak, that individual will recall how they behaved in the past, under unbiased circumstances, and thus infer their true attitude.

A study by Kiesler, Nisbett, and Zanna (1969), concluded that while individuals infer attitudes from their behavior, this would only occur if they assume that a link exists between their behavior and believes. Further a study by Fazio, Herr and Olney (1984), indicates that, as Bem's (1967), self perception theory assumes, freely performed behavior is highly reflective of an individuals attitude toward the subject matter in question.

Based on these studies the researcher proposes to use the attitude of Information Systems Managers towards various countermeasures to determine the vulnerability level of their computer systems to security risks.

Section C will be used to gather information regarding the Information Systems Manager's perception of which factor causes the most risk to their Information System. According to Wilk (1993), there are seven major areas of concern where security problems can be found, i.e., personnel, hardware, software, communications, physical building facilities, practices and procedures, laws and regulations.

The "drop and pick later" method of administering the questionnaire will be suitable for the respondents with head offices in Nairobi, for those with head offices outside Nairobi the questionnaire will be mailed, in both cases follow up will be done through telephone calls.

3.3. Data Analysis Techniques

Data collected in section A of the questionnaire will be analyzed through the use of descriptive statistics such as frequency table's, proportions, percentages, and cross tabulations. These will be used to profile the Companies.

Responses to section B will be used to perform the risk analysis in order to determine the current level of vulnerability. This analysis is based on the axiom: 'As countermeasures increase, vulnerability decreases.'

A list of vulnerabilities is given in appendix III. These vulnerabilities are paired with specific countermeasures for the analysis process. Each countermeasure has a minimum weight of 1, and a maximum weight of 5. The total weight of the countermeasures determines the systems level of vulnerability.

The ranking of countermeasures by the Information Systems Managers determine if the system's level of vulnerability is low or high. Vulnerability levels range from a minimum of 3.0 to a maximum of 18.0. The acceptable and desirable vulnerability level for a system is 7.5.
The countermeasures decrease vulnerability from a maximum of 18.0 towards a minimum of 3.0.

The results of the vulnerability levels will further be analyzed using factor analysis to group together those vulnerabilities that are highly correlated. The results will be presented through the use of descriptive statistics

Discriminant analysis will be used to determine whether the variables used in the vulnerability analysis can be used to predict group/sector membership.

Data collected in section C of the questionnaire will be analyzed through the use of descriptive statistics, such as mean and mode.

Chapter Four.

Results and Data Analysis.

This Chapter contains the analysis and findings of the of the research study.

4.1. Summary of Responses.

A total of 54 questionnaires were distributed to the respondents. Out of these, 34 questionnaires were successfully completed and returned, which represents a response rate of 62.9%. These were used as the basis for the data analysis and the findings of the study.

The companies quoted on the Nairobi Stock Exchange are categorized into 4 groups or sectors. These are Industrial and Allied sector, Finance and Investments sector, Commercial and Allied sector, and Agricultural sector. This grouping will be used in the analysis of the findings.

Table 4.1 below gives a summary of responses.

Table 4.1 : Summary of Responses

Sector	No. of Companies	Responded	Percentage (%)	Did not Respond	Percentage (%)
Industrial & Allied	18	8	44.4	10	55.6
Finance & Investment	13	11	84.6	2	15.4
Commercial & Allied	14	10	71.4	4	28.6
Agricultural	9	5	55.6	4	44.4
Combined	**54**	**34**	**62.9**	**20**	**37.1**

The table above indicates that the highest response rate was in the Finance and Investments sector with a response rate of 84.6%. The Industrial and Allied sector had the lowest rate of response at 44.4%.

. Status of IT Resources in the Organizations.

The responses to question's 1 to 15 of Section A in this study are summarized using descriptive statistics. This analysis gives the general characteristics of the organizations in relation to the information systems in operation.

4.2.1. Ownership of Companies.

The companies that responded to the questionnaires are either locally owned or jointly owned, none are wholly foreign owned. Most of the companies that responded (67.6%) are jointly owned as shown in Table 4.2.1 below.

Table 4.2.1 : Ownership of Companies.

Sector	Industrial & Allied		Finance & Investment		Commercial & Allied		Agricultural		Combined	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
1. Ownership										
a) foreign owned	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
b) locally owned	2	25.0	5	45.5	3	30.0	1	20.0	11	32.4
c) jointly owned	6	75.0	6	54.5	7	70.0	4	80.0	23	67.6

4.2.2. First Computer Installation.

All the respondents' computer installations are more than five years old. Most of them (58.8%) have had computer installations for more than 15 years as shown in Table 4.2.2 below. This indicates that these organizations have been using computers for long and have thus used computer systems to build mission critical applications. Therefore these organizations rely on computer systems for their Day-to-day operations.

Table 4.2.2 : First Computer Installation.

Sector	Industrial & Allied		Finance & Investment		Commercial & Allied		Agricultural		Combined	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
2. First computer installation										
a) less than 5 yrs ago	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
b) between 5-10 yrs	2	25.0	2	18.2	2	20.0	2	40.0	8	23.5
c) between 10-15 yrs	0	0.0	3	27.3	2	20.0	1	20.0	6	17.6
d) more than 15 yrs	6	75.0	6	54.5	6	60.0	2	40.0	20	58.8

4.2.3. Number of Computers.

There is very low usage of mainframe computers (20.6%) among the respondent companies as shown in Table 4.2.3 below . Those in the agricultural sector reported none.

Half of the companies (50.0%) indicated that they have between 1 and 10 minicomputers. However about a third (29.4%) indicated that they have no minicomputers. Only companies in the finance and investment sector indicated that they have more than 30 minicomputers. This can be explained from the fact that most financial institutions such as banks require powerful computer systems to run their applications.

All the respondent companies have desktop personal computers (PC's), with 79.4% indicating that they have more than 30 computers.

Table 4.2.3 : Number of Computers

Sector	Industrial & Allied		Finance & Investment		Commercial & Allied		Agricultural		Combined	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
3. Number of computers										
a) mainframes										
none	6	75.0	8	72.7	8	80.0	5	100.0	27	79.4
1 – 10	2	25.0	3	27.3	2	20.0	0	0.0	7	20.6
11 - 20	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
21 – 30	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
more than 30	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
b) minicomputers										
none	3	37.5	0	0.0	4	40.0	3	60.0	10	29.4
1 – 10	5	62.5	5	45.5	6	60.0	1	20.0	17	50.0
11 - 20	0	0.0	2	18.2	0	0.0	0	0.0	2	5.9
21 – 30	0	0.0	0	0.0	0	0.0	1	20.0	1	2.9
more than 30	0	0.0	4	36.4	0	0.0	0	0.0	4	11.8
c) desktop PC's										
none	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
0 – 10	2	25.0	0	0.0	0	0.0	2	40.0	4	11.8
11 - 20	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
21 – 30	0	0.0	1	9.1	2	20.0	0	0.0	3	8.8
more than 30	6	75.0	10	90.9	8	80.0	3	60.0	27	79.4
d) laptop PC's										
none	1	12.5	0	0.0	1	10.0	2	40.0	4	11.8
0 – 10	5	62.5	8	72.7	8	80.0	3	60.0	24	70.6

Sector	Industrial & Allied		Finance & Investment		Commercial & Allied		Agricultural		Combined	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
11 - 20	1	12.5	1	9.1	0	0.0	0	0.0	2	5.9
21 – 30	0	0.0	1	9.1	0	0.0	0	0.0	1	2.9
more than 30	1	12.5	1	9.1	1	10.0	0	0.0	3	8.8
e) notebooks	5	62.5	5	45.5	7	70.0	4	80.0	21	61.8
none	2	25.0	3	27.3	3	30.0	0	0.0	8	23.5
0 – 10	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
11 - 20	0	0.0	2	18.2	0	0.0	0	0.0	2	5.9
21 – 30	1	12.5	1	9.1	0	0.0	1	20.0	3	8.8
more than 30										

4.2.4. IT Director's Position.

Most of the respondent companies (88.2%) indicated that they do not have the position of the IT Director as shown in Table 4.2.4. Companies in the industrial and allied sector, and the agricultural sector have no IT Director. The commercial and allied sector has the highest number of IT Directors. For the companies that do not have this position, most (46.7%) have an IT Manager taking charge of IT department. Other titles for the person in charge of the IT department include Computer Manager, Business Systems Manager, Systems Manager, M.I.S Manager, Group IT Manager, Information Systems Manager, Executive Manager IT, Chief Manager IT, Senior Manager IT, Financial Controller/Director, Company Secretary.

Table 4.2.4 : IT Director's Position.

Sector	Industrial & Allied		Finance & Investment		Commercial & Allied		Agricultural		Combined	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
4. IT Director position exists										
a) Yes	0	0.0	1	9.1	3	30.0	0	0.0	4	11.8
b) No	8	100.0	10	90.9	7	70.0	5	100.0	30	88.2

4.2.5. Investments in Computer Systems.

Most of the respondent companies (67.7%) have investments of more than KShs 50 million, with 20.6% indicating that they have invested more than KShs 250 million. Majority of those with investments above KShs 250 million are in the industrial and allied sector and the finance and investments sector as shown in Table 4.2.5 below. This therefore indicates that these companies have put a lot of resources in computer systems and hence the need to keep them secure.

Table 4.2.5 : Investments in Computer Systems.

Sector	Industrial & Allied		Finance & Investment		Commercial & Allied		Agricultural		Combined	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
5. Investments in computer system. (in million Kshs)										
a) less than 50m	3	37.5	2	18.2	2	20.0	4	80.0	11	32.4
b) between 50-100m	2	25.0	1	9.1	7	70.0	0	0.0	10	29.4
c) between 100-150	1	12.5	2	18.2	1	10.0	0	0.0	4	11.8

Sector	Industrial & Allied		Finance & Investment		Commercial & Allied		Agricultural		Combined	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
d) between 150-200	0	0.0	2	18.2	0	0.0	0	0.0	2	5.9
e) between 200 –250	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
f) more than 250	2	25.0	4	36.4	0	0.0	1	20.0	7	20.6

2.6. Previous Year IT Budget.

Most of the respondents (52.9%) indicated a high IT budget of KShs 10 million for the previous year as shown in Table 4.2.6 below. This indicates that there is continued heavy investment in computer systems by these companies.

Table 4.2.6 : Previous Year IT Budget.

Sector	Industrial & Allied		Finance & Investment		Commercial & Allied		Agricultural		Combined	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
6. Previous year IT Budget (in million Kshs)										
a) less than 1m	3	37.5	0	0.0	0	0.0	3	60.0	6	17.6
b) between 1 – 5m	0	0.0	2	18.2	6	60.0	1	20.0	9	26.5
c) between 5 – 10m	0	0.0	1	9.1	0	0.0	0	0.0	1	2.6
d) more than 10m	5	62.5	8	72.7	4	40.0	1	20.0	18	52.9

4.2.7. Acquisition Policy for Hardware and Software.

Most of the respondent companies (88.2%) indicated that they have an acquisition policy for purchase of hardware and software as shown in Table 4.2.7 below.

Table 4.2.7 : Acquisition Policy for Hardware and Software.

Sector	Industrial & Allied		Finance & Investment		Commercial & Allied		Agricultural		Combined	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
7.Acquisition policy for hardware and software exists.										
a) Yes	7	87.5	11	100.0	9	90.0	3	60.0	30	88.2
b) No	1	12.5	0	0.0	1	10.0	2	40.0	4	11.8

4.2.8. Internet and World Wide Web Access.

All the respondent companies indicated that they have access to the internet as shown in Table 4.2.8 below.

Table 4.2.8 : Internet and World Wide Web Access.

Sector	Industrial & Allied		Finance & Investment		Commercial & Allied		Agricultural		Combined	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
8. Internet and www access exists.										
c) Yes	8	100.0	11	100.0	10	100.0	5	100.0	34	100.0
d) No	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0.

4.2.9. Computer Security Policy.

Most of the respondent companies (64.7%) indicated that they have a written and formal computer security policy exists as shown in Table 4.2.9. However most of the companies(60.0%) in the agricultural sector indicated that they do not have a formal security policy.

Table : 4.2.9 : Computer Security Policy.

Sector	Industrial & Allied		Finance & Investment		Commercial & Allied		Agricultural		Combined	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
9. Written and formal computer security policy exists.										
a) Yes	5	62.5	8	72.7	7	70.0	2	40.0	22	64.7
b) No	3	37.5	3	27.3	3	30.0	3	60.0	12	35.3

2.10. Security Reviews.

he frequency of security reviews varies evenly with some preferring monthly reviews (29.4%), others uarterly reviews (17.6%), and others annually (29.4%) as shown in Table 4.2.10 below. However 20.6% of e respondents do not have a preferred frequency and perform reviews as and when need arises. Very few 2.9%) perform reviews bi-annually.

Table 4.2.10 : Security Reviews.

Sector	Industrial & Allied		Finance & Investment		Commercial & Allied		Agricultural		Combined	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
10. Frequency of security reviews.										
a) monthly	3	37.5	4	36.4	2	20.0	1	20.0	10	29.4
b) quarterly	2	25.0	1	9.1	2	20.0	1	20.0	6	17.6
c) bi-annually	0	0.0	1	9.1	0	0.0	0	0.0	1	2.9
d) annually	2	25.0	2	18.2	4	40.0	2	40.0	10	29.4
e) other	1	12.5	3	27.3	2	20.0	1	20.0	7	20.6

4.2.11. Security Budgets.

Most of the respondent companies (55.9%) indicated that they have annual security budget arrangements as shown in Table 4.2.11 below. However fewer companies (40.0%) in the agricultural sector indicated that they have annual security budgets.

Table 4.2.11: Security Budgets.

Sector	Industrial & Allied		Finance & Investment		Commercial & Allied		Agricultural		Combined	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
11. Annual security budget exists.										
a) Yes	5	62.5	7	63.6	5	50.0	2	40.0	19	55.9
b) No	3	37.5	4	36.4	5	50.0	3	60.0	15	44.1

4.2.12. Computer Literacy.

Most respondent indicated that most of their staff, both management and non-management, have either good or excellent computer literacy levels. This is shown below in Table 4.2.12. where 73.5% of the management staff, and 79.4% of non-management staff have either good or excellent literacy levels. This is therefore an indicator of high usage rates.

Table 4.2.12 : Computer Literacy.

Sector	Industrial & Allied		Finance & Investment		Commercial & Allied		Agricultural		Combined	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
12. Computer literacy rating of staff.										
a) Management										
Excellent	4	50.0	1	9.1	2	20.0	0	0.0	7	20.6
Good	2	25.0	8	72.7	4	40.0	4	80.0	18	52.9
Fair	1	12.5	2	18.2	4	40.0	1	20.0	8	23.5
Poor	1	12.5	0	0.0	0	0.0	0	0.0	1	2.9
b) Non-management										
Excellent	2	25.0	1	9.1	1	10.0	0	0.0	4	11.8
Good	4	50.0	8	72.7	7	70.0	4	80.0	23	67.6
Fair	1	12.5	2	18.2	2	20.0	1	20.0	6	17.6
Poor	1	12.5	0	0.0	0	0.0	0	0.0	1	2.9

4.2.13. Information Systems.

All the respondents indicated that they have Transaction Processing Systems in use as shown in Table 4.2.13 below. Most of them (76.5%) indicated that they have Management Information Systems in use. Few (29.4%) indicated they use Decision Support Systems with the agricultural sector reporting no usage. Usage of both Executive Information Systems and Expert Systems is low (17.6%), with the commercial and allied sector reporting no usage. Strategic Information Systems also have low usage (20.6%) with the commercial and services sector indicating no usage, however the industrial and allied sector indicates a relatively high usage of 50.0%.

Table 4.2.13 : Information Systems.

Sector	Industrial & Allied		Finance & Investment		Commercial & Allied		Agricultural		Combined	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
13. Information systems in use.										
a) Transaction Processing Systems	8	100.0	11	100.0	10	100.0	5	100.0	34	100
b) Management Information Systems	8	100.0	8	72.7	7	70.0	3	60.0	26	76.5
c) Decision Support Systems	4	50.0	2	18.2	4	40.0	0	0.0	10	29.4
d) Executive Information Systems	2	25.0	3	27.3	0	0.0	1	20.0	6	17.6
e) Expert Systems	3	37.5	2	18.2	0	0.0	1	20.0	6	17.6
f) Strategic Information Systems	4	50.0	2	18.2	0	0.0	1	20.0	7	20.6

4.2.14. IT Strategic Plan.

Most of the respondent (85.3%) indicate that they have a formal strategic plan for their information technology as shown in Table 4.2.14 below.

Table 4.2.14 : IT Strategic Plan.

Sector	Industrial & Allied		Finance & Investment		Commercial & Allied		Agricultural		Combined	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
14. Formal strategic plan for IT exists.										
a) Yes	7	87.5	10	90.9	9	90.0	3	60.0	29	85.3
b) No	1	12.5	1	9.1	1	10.0	2	40.0	5	14.7

4.3. Risk Analysis.

To perform the risk analysis the respondents were asked to rank the countermeasures in Section B of the questionnaire (Appendix II). These countermeasures were used in the analysis to determine the systems level of vulnerability as described in Section 5.3. The maximum acceptable vulnerability level is 7.5; any score above this indicates that the vulnerability level is high and the system is susceptible to security violations.

4.3.1 Vulnerability Analysis.

All areas of vulnerability that were evaluated are shown in Table 4.3.1 below. The vulnerabilities that have an asterisk exceed the maximum acceptable level.

Table 4.3.1: Vulnerability Levels.

Sector	Industrial & Allied	Finance & Investment	Commercial & Allied	Agricultural	Combined
Vulnerabilities	Level	Level	Level	Level	Level
a) Susceptibility to communication technology.	6.0	5.6	6.2	6.8	6.15
b) Susceptibility to inter/intranetwork user activity.	4.6	3.9	4.1	7.2	4.95
c)Susceptibility to hardware failure or configuration change.	6.5	4.2	5.3	7.8*	5.95
d)Susceptibility to environmental hazards.	5.5	3.9	4.6	7.0	5.25
e)Susceptibility to key person dependency.	6.9	4.5	6.0	6.8	6.05
f)Susceptibility to improper handling of storage media.	5.9	4.6	4.9	5.8	5.30

Sector	Industrial & Allied	Finance & Investment	Commercial & Allied	Agricultural	Combined
Vulnerabilities	Level	Level	Level	Level	Level
g)Susceptibility to lack of awareness of computer security issues.	5.6	4.1	6.1	7.8*	5.90
h)Susceptibility to unauthorized physical access.	6.9	3.7	6.5	8.0*	6.28
I)Susceptibility to unauthorized programmatic access.	4.6	3.5	4.6	6.6	4.83
j)Susceptibility to loss of data or software files.	4.6	3.5	3.5	5.2	4.20
k)Susceptibility to unauthorized information theft or disclosure.	4.9	4.9	6.0	7.8*	5.90
l)Susceptibility to failure and instability of electrical power sources	6.6	3.7	4.9	6.0	5.30
m)Susceptibility to fire	6.4	4.4	5.8	7.8*	6.10
n)Susceptibility to user operator errors.	5.6	4.5	5.5	7.0	5.65
o)Susceptibility to software flaws or inadequacies.	8.3*	3.5	5.8	7.0	6.15
p)Susceptibility to theft of system resources.	5.4	4.3	4.5	7.8*	5.50

In the Industrial and Allied sector majority of the vulnerability levels are acceptable apart from susceptibility to software flaws or inadequacies, which has a vulnerability level of 8.3.

In the Finance and Investment sector all the vulnerability levels range from 3.5 to 5.6 and are acceptable since they are below the maximum acceptable level of 7.5.

In the Commercial and Allied sector all the vulnerability levels are also acceptable since they are below the maximum acceptable level of 7.5. However the levels are higher compared to those in the Finance and Investment sector, and they range from 4.1 to 6.5.

The Agricultural sector has the highest vulnerability levels compared to the other sectors. There are six areas where the vulnerability levels are above the maximum acceptable level. These are:

- Susceptibility to hardware failure or configuration change.
- Susceptibility to lack of awareness of computer issues.
- Susceptibility to unauthorized physical access.
- Susceptibility to unauthorized information theft or disclosure.
- Susceptibility to fire.
- Susceptibility to theft of system resources.

This therefore means that computer systems in the Agricultural sector are more susceptible to security violation and other harmful activities.

However across all the sectors the average vulnerability levels are all acceptable and range from 4.20 to 6.28.

4.4. Factor Analysis.

Factor analysis was performed on the results of the vulnerability analysis. Since the number of vulnerabilities is not large all of them will be treated as variables as shown in the Table 4.4.1. For the factor analysis the actual weight of the countermeasures was used and not the vulnerability level.

Table 4.4.1: List of Variables.

Vulnerabilities	Variable Number.	Mean Weight	Std Dev
a) Susceptibility to communication technology.	1	11.94	2.88
b) Susceptibility to inter/intranetwork user activity.	2	13.38	2.52
c) Susceptibility to hardware failure or configuration change.	3	12.41	2.72
d) Susceptibility to environmental hazards.	4	13.06	3.00
e) Susceptibility to key person dependency.	5	12.15	2.58
f) Susceptibility to improper handling of storage media.	6	12.82	1.78
g) Susceptibility to lack of awareness of computer security issues.	7	12.41	2.79
h) Susceptibility to unauthorized physical access.	8	12.09	3.41
I) Susceptibility to unauthorized programmatic access.	9	13.44	2.06
j) Susceptibility to loss of data or software files.	10	14.00	1.39
k) Susceptibility to unauthorized information theft or disclosure.	11	12.35	2.74
l) Susceptibility to failure and instability of electrical power sources	12	12.91	2.45
m) Susceptibility to fire	13	12.23	3.34
n) Susceptibility to user operator errors.	14	12.56	2.18
o) Susceptibility to software flaws or inadequacies.	15	12.09	3.54
p) Susceptibility to theft of system resources.	16	13.12	3.06

The correlation matrix of the variables above is shown in Table 4.4.2. below.

Table 4.4.2. Correlation Matrix.

Var	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1															
2	.437	1														
3	.475	.603	1													
4	.235	.525	.616	1												
5	.331	.503	.776	.530	1											
6	.187	.554	.253	.415	.282	1										
7	.462	.582	.602	.657	.629	.434	1									
8	.179	.485	.531	.735	.476	.540	.713	1								
9	.183	.689	.453	.705	.482	.442	.535	.562	1							
10	.159	.673	.416	.659	.295	.561	.529	.522	.622	1						
11	.494	.730	.630	.583	.510	.546	.668	.625	.567	.429	1					
12	.055	.456	.378	.654	.408	.502	.539	.692	.666	.541	.541	1				
13	.310	.417	.569	.738	.442	.353	.693	.814	.407	.463	.563	.594	1			
14	.493	.606	.748	.653	.637	.229	.693	.580	.551	.419	.586	.366	.707	1		
15	.390	.540	.727	.669	.702	.439	.744	.772	.464	.572	.650	.622	.729	.600	1	
16	.090	.445	.550	.803	.526	.309	.603	.628	.615	.526	.475	.602	.687	.667	.600	1

The simple pair wise correlation matrix above reveals that: variable 1 and 6 are weakly correlated with the other variables; variables 8, 12, 13, and 15 were found to be highly correlated positively; variables 5, 7, 14, and 15 were also found to be highly correlated positively.

Performing a principal components analysis generates the result shown on Table 4.4.3 below, that shows the communalities and the eigenvalues.

Table 4.4.3 : Principal Component Analysis Output.

Variable	Communality	Factor	Eigenvalue	% of Variance	Cumulative %
1	.866	1	9.149	57.2	57.2
2	.881	2	1.561	9.8	66.9
3	.852	3	1.214	7.6	74.5
4	.855	4	.852	5.3	79.8
5	.934	5	.658	4.1	84.0
6	.822	6	.518	3.2	87.2
7	.758	7	.401	2.5	89.7
8	.876	8	.350	2.2	91.9
9	.839	9	.315	2.0	93.9
10	.748	10	.253	1.6	95.5
11	.761	11	.228	1.4	96.9
12	.766	12	.150	0.9	97.8
13	.919	13	.122	0.8	98.6
14	.868	14	.106	0.7	99.2
15	.854	15	.071	0.4	99.7
16	.837	16	.051	0.3	100.0

The communalities for each variable indicates the proportion of the variance of the variable that is due to the factors, for example 91.9% of the variance in variable 13 is due to the factors. The eigenvalues express the variances extracted by the factors, for example factor 1 explains 57.2% of the total variation.

The principal component analysis extracted 5 factor and the initial factor loadings are shown in Table 4.4.4 below.

Table 4.4.4 : Initial Factor Loadings Matrix.

Variable	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5
1	.431	.669	.344	.184	.285
2	.760	.059	.494	-.233	.042
3	.778	.421	-.090	-.159	-.188
4	.857	-.189	-.205	-.119	.166
5	.712	.339	-.137	-.202	-.502
6	.573	-.348	.511	.291	-.164
7	.842	.137	-.031	.165	.038
8	.832	-.217	-.176	.324	-.019
9	.750	-.274	.169	-.421	.036
10	.697	-.362	.266	-.163	.187
11	.794	.139	.293	.149	-.047
12	.724	-.452	-.059	.088	-.158
13	.801	-.015	-.347	.317	.238
14	.797	.347	-.168	-.176	.229
15	.856	.092	-.118	.228	-.215
16	.774	-.187	-.374	-.221	.119

To extract the principal components the initial factor matrix was orthogonally rotated to maximize the variance using varimax rotation. The varimax rotated factor matrix is shown in Table 4.4.5 below.

Table 4.4.5: Varimax Rotated Factor Matrix.

Variable	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5
1	.080	.018	.174	.085	.906
2	.076	.654	.308	.397	.441
3	.341	.254	.726	.049	.376
4	.686	.545	.251	.125	.087
5	.240	.179	.901	.125	.129
6	.162	.286	.038	.837	.111
7	.580	.237	.368	.291	.381
8	.770	.188	.228	.437	.071
9	.254	.803	.271	.235	.029
10	.321	.699	.014	.381	.110
11	.322	.292	.352	.487	.459
12	.548	.379	.217	.489	-.187
13	.890	.132	.158	.149	.252
14	.526	.397	.429	-.128	.483
15	.602	.119	.530	.388	.215
16	.687	.516	.309	-.037	-.046

From the final varimax rotated matrix above we can see that:

- Variable 4, 7, 8, 12, 13, 14, 15, and 16 load heavily on Factor 1.
- Variable 2, 9, and 10 load heavily on Factor 2.
- Variable 3 and 5 load heavily on Factor 3.
- Variable 6 and 11 load heavily on Factor 4.
- Variable 1 loads heavily on Factor 5

The factors and the vulnerabilities they represent are summarized in Table 4.4.6 below.

Table 4.4.6: Factors and Vulnerabilities.

Factor	Vulnerabilities.
1	• Susceptibility to environmental hazards. • Susceptibility to lack of awareness of computer security issues. • Susceptibility to unauthorized physical access. • Susceptibility to failure and instability of electrical power sources • Susceptibility to fire • Susceptibility to user operator errors. • Susceptibility to software flaws or inadequacies. • Susceptibility to theft of system resources.
2	• Susceptibility to inter/intranetwork user activity. • Susceptibility to unauthorized programmatic access. • Susceptibility to loss of data or software files.
3	• Susceptibility to hardware failure or configuration change. • Susceptibility to key person dependency.
4	• Susceptibility to improper handling of storage media • Susceptibility to unauthorized information theft or disclosure.
5	• Susceptibility to communication technology.

The combined vulnerability levels in Table 4.3.1 were then used to determine the mean vulnerability level for each of the factors as shown in Table 4.4.7. below.

Table 4.4.7: Vulnerability Level per Factor.

Factor	Mean Vulnerability Level
1	5.8
2	4.7
3	6.0
4	5.6
5	6.2

The table above indicates that factor 5 has the highest vulnerability level of 6.2 this is however below the maximum acceptable vulnerability level of 7.5.

4.5. Discriminant Analysis.

Discriminant analysis was used to determine whether the variables used in the vulnerability analysis could be used to predict group/sector membership.

The mean score and standard deviations on Table 4.3.2.1 above were used for the analysis.

The analysis process generated three canonical discriminant functions. This is consistent with the rule that states that 'if there are more variables than groups, then the number of discriminant functions will at most be equal to the number of groups minus one'.

The standardized canonical discriminant function coefficients are summarized in Table 4.5.1 below.

Table 4.5.1: Standardized Canonical Discriminant Function Coefficients

Variable	Function 1	Function 2	Function 3
1	.107	-.644	-.284
2	-.212	-.242	.941
3	.582	1.052	.589
4	-.099	-.643	.489
5	-.340	-.680	-.539
6	.856	-.158	.208
7	-.638	.933	-.145
8	-.151	-.003	-1.087
9	-.356	1.585	-.195
10	.021	.011	.157
11	-1.998	.060	-.346
12	1.526	-.608	-.080
13	-.998	.727	.610
14	1.196	-.259	-.373
15	1.812	.177	.004
16	-.644	-.954	.195

To assess the importance of the variables in discriminating between groups, the simple pairwise correlation between the discriminating variables and the canonical discriminant functions was calculated and is summarized in Table 4.5.2 below. The variables are ordered by size of correlation within function.

Table 4.5.2: Discriminant Loadings.

Variable No.	Factor 1	Factor 2	Factor 3
9	.060	.504	.142
7	.055	.465	-.096
8	.146	.425	-.182
3	.154	.411	.195
15	.283	.386	-.032
11	-.544	.375	.042
14	.064	.360	.067
13	.091	.317	.046
4	.087	.301	.207
5	.160	.261	-.102
12	.243	.257	.007
6	.138	.160	.150
1	.007	.129	-.011
10	.183	.352	.508
2	.033	.408	.435
16	.064	.168	.177

The loadings suggest that variable 9 is the most important variable in discriminating between the four sectors when using function 2. Similarly when using function 3 variable10 is the most important. From the loadings we can also see that 13 out of the 16 variables have the largest absolute correlation to function 2. Hence function 2 is the most suitable for classifying the respondents into their respective sectors.

Using the canonical functions generated above, the mean discriminant score for each sector was calculated and the results summarized it Table 4.5.3 below. This can be used to classify the respondent companies into their respective sector. The respondent will be categorized according to how close their discriminant score is to the mean discriminant score of the group. For example, using function 2, if a respondent has a discriminant score of 1.0 it most likely belongs to the Finance and Investments sector.

Table 4.5.3: Mean Discriminant Scores.

	Mean Discriminant Score		
Sector	**Function 1**	**Function 2**	**Function 3**
Agriculture	0.497	-2.008	-0.657
Commercial & Allied	0.681	-0.342	0.771
Finance and Investments	1.433	0.985	-0.348
Industrial & Allied	-3.132	0.328	-0.074

The accuracy of using the discriminant functions to classify the respondents was evaluated using the confusion matrix of actual versus predicted group membership shown in Table 4.5.4. below.

Table 4.5.4: Confusion Matrix of Actual Versus Predicted Group Membership.

	Predicted Group/Sector Membership			
Actual Group **(Sector)**	Agriculture	Commercial & Allied	Finance and Investments	Industrial & Allied
Agriculture	80.0%	20.0%	0.0%	0.0%
Commercial & Allied	10.0%	70.0%	20.0%	0.0%
Finance and Investments	0.0%	18.2%	81.8%	0.0%
Industrial & Allied	0.0%	0.0%	12.5%	87.5%

The percentage of grouped cases correctly classified is 79.41%

From the above statistics it is safe to conclude that the discriminant functions can be used to predict sector/group membership.

4.6. Perceived Security Risk Related Problems.

Table 4.6.1: Perceived Security Risk Related Problems

Sector	Industrial & Allied		Finance & Investment		Commercial & Allied		Agricultural		Combined	
	Ranking		Ranking		Ranking		Ranking		Ranking	
Security Problem	Mean	Mode	Mean	Mode	Mean	Mode	Mean	Mode	Mean	Mode
a) Personnel and other people problems	5.8	2	6.4	9	6.5	5	6.4	6	6.2	10
b) Hardware failure.	6.5	9	6.0	9	6.5	10	4.2	3	6.1	8
c) Software failure.	7.0	9	5.7	8	6.5	10	3.4	3	6.0	3
d) Communication systems failure.	6.5	7	6.1	7	6.3	5	4.0	2	6.0	10
e) Physical building facilities.	5.2	6	4.4	1	4.5	5	2.4	3	4.4	3
f) Practices and procedures.	6.1	4	4.6	9	6.0	5	5.2	6	5.6	10
g) Laws and regulations.	5.5	9	4.9	3	3.8	1	2.2	1	4.3	1

The perceived security risks were ranked on a scale of 1 to 10, where the least risk is ranked 1 and the highest risk is ranked 10. The analysis is based on the mean rank and the modal rank.

On average majority of the respondents indicated moderate risks ranked between 4.3 and 6.2 for the security related problems as shown in Table 4.6.1 above. The industrial and allied sector had mean ranks ranging from 5.2 to 7.0, hence indicating moderate risks from the security related problems. The finance and investments sector had mean ranks ranging from 4.4 to 6.4, hence also indicating moderate risks from the security related problems. The commercial and allied sector had mean ranks ranging from 3.8 to 6.5,similarly indicating moderate risks from the security related problems. The agricultural sector had the lowest mean ranks with most ranging from 2.4 to 4.2, hence indicating relatively lower risks from the security related problems.

However, personnel related problems, communication systems failure, and practices and procedures have a modal score of 10 indicating that many of the respondents consider these problems to pose the highest risk to their computer systems.

In the commercial and allied sector the problems of hardware failure and software failure had a modal score of 10, indicating that these are perceived as highest risk problems in this sector.

Across the sectors the problem of laws and regulations is considered to be of least risk with a modal score of 1.

4.5. Computer Security Problems Actually Experienced By The Organizations.]

The respondents indicated that they have faced various computer related security threats, with most indicating that the most common is virus attacks. These virus attacks are usually through the electronic mail (e-mail) system used by the employees in these organizations. Since all the companies indicated that they have access to the Internet, then they are equally exposed to these threat.

The other security related problems experienced include:

- Theft of computers and computer parts.
- Fraudulent manipulation of financial transactions.
- Lightening strikes
- Accidental damage to computer equipment.
- Poor communication links.
- Limited incidences of hacking.
- Software and database corruption.
- Power outages.
- Password violations so as to access restricted applications.
- Improper segregation of duties.
- Network failure.

However some of the respondents indicated that they have never experienced any serious computer security related problem

Chapter Five.

Summary and Conclusions.

In this chapter the conclusions arrived at from the research findings are discussed in light of the objectives of the study.

5.1. Conclusions on Status of IT Resources.

The study indicates that the companies quoted on the Nairobi Stock Exchange have been using computers for more than 5 years, with 76.4% having used computers for the past 10 years. This therefore means that they most likely have computer-based information systems upon which they have over time built their mission critical applications and hence is a strategic asset that has to be secured at all times to ensure continuity of business.

Companies in the Industrial and Allied sector, Finance and Investment sector, and the Commercial and Allied sector indicated that they have mainframe computers, this can be explained from the fact that majority of these companies i.e. 75.0%, 54.5%, and 60.0% respectively, have had computer installations for more than 15 years. These companies also have the high usage of minicomputers, meaning that they could be moving their operations from the mainframe-based servers to minicomputer-based servers.

In terms of investments in computer systems 67.7% of the companies have investments of more than KShs 50 million, and 52.9% indicated that they had an IT budget of more than KShs 10 million for the previous year. This indicates that there is continued heavy investment in information technology by these companies. The Finance and Investment sector has the highest level of Investments with 72.8% of the companies having more than 100 million in computer systems.

Although most of the companies have made heavy investments in information technology, it is surprising that they do not have a information technology professional at the executive board level since 88.2% of the respondent companies indicated that they do not have the post of IT Director.

All the respondent companies have access to the Internet; this means they are exposed to computer viruses that are spread through the Internet especially through electronic mail.

In terms of policy formulation most of the respondents indicated that they had a policy for hardware and software acquisition (88.2%), and computer security policy (64.7%).
The frequency of security reviews varies evenly with some preferring monthly reviews (29.4%), others quarterly reviews (17.6%), and others annually (29.4%). This means that 76.5% have a defined frequency for reviewing the security posture of their organizations.

Slightly over half (55.9%) of the companies indicated that they have annual security budgets, this is close to the percentage (52.9%) of those companies that have IT budgets of over KShs 10 million. Comparing the sectors further supports this. In the Industrial and Allied sector 62.5% of the companies have an IT budget of over KShs 10 million and 62.5% have security budgets; in the Finance and Investments sector 72.7% of the companies have IT budgets of over KShs 10 million and63.6% have security budgets; in the Commercial and Allied sector 40.0% of the companies have an IT budget of over KShs 10 million and 50.0% have security budgets. Therefore there appears to be a relationship between those that have high IT budgets of over KShs 10 million and those who have security budgets.

Most of the information systems are used mainly for Transaction Process Systems (100%) and for Management Information Systems (76.5%). The use of Decision Support Systems (29.4%), Executive Information Systems (17.6%), Expert Systems (17.6%), and Strategic Information Systems (20.6%) is quite low meaning the use of specialist information systems is not widespread.

5.2. Conclusion on Risk, Factor and Discriminant Analysis.

The findings of this study indicates that the Finance and Investments sector and the Commercial and Allied sector have the most secure systems since their vulnerability levels to the susceptibilities considered in this study are all acceptable.
The Agricultural sector has the most insecure system compared with the other sectors and is susceptible to six vulnerability areas.
Considering the combined vulnerability levels, the highest susceptibility area is unauthorized physical access to computer systems, this means that very few of the information systems managers do not consider restricted access to computer rooms and communication access points as well as the installation of security monitors and alarm systems to be important. This explains why some of the respondents have experienced thefts of computers and computer parts.

The other high vulnerability areas include: susceptibility to communication technology; susceptibility to key person dependency; susceptibility to fire; and susceptibility to software flaws or inadequacies. This explains why some of the problems experienced by these organization include:

- Fraudulent manipulation of financial transactions.
- Accidental damage to computer equipment.
- Poor communication links.
- Limited incidences of hacking.
- Software and database corruption.
- Password violations so as to access restricted applications.
- Network failure.

Therefore if these organizations addressed these areas of susceptibility the incidences reported should therefore be minimized.

The factor analysis extracted five factors to represent the16 variables.

The first factor (Factor 1) is susceptibility to human errors, unauthorized physical access, natural hazards and failure of public utilities. This factor is concerned with loss of business assets.

The second factor (Factor 2) is susceptibility to unauthorized logical access to computer resources. This factor is concerned with loss of confidentiality and privacy.

The third factor (Factor 3) is susceptibility to hardware failure and key person dependency. This factor is concerned with loss of availability and reliability.

The fourth factor (Factor 4) is susceptibility to loss and/or theft of organizational data and information. This factor is concerned with loss of accuracy and integrity.

The fifth factor (Factor 5) is susceptibility to communication technology. This factor is concerned with loss of availability and reliability.

From the analysis all the factors have vulnerability levels below the acceptable level. Factor 1 has the highest vulnerability of 6.2, followed by Factor 3 with a vulnerability level of 6.0. Factor 2 has the lowest vulnerability level. This therefore means that the respondent organizations need to put more effort on the countermeasures that address susceptibilities to human error, unauthorized physical access, natural hazards, failure of public utilities and communication technology.

Ultimately, it is a management decision as to whether or not the levels of vulnerability are acceptable. That is, in virtually all cases managers with the security responsibility for a system have the authority to accept or reject the current level of vulnerability for systems under their purview.

The results of discriminant analysis indicate that variables used in this study to determine the security posture of the respondents can be used to predict the sector to which a respondent belongs with an accuracy of 79.41%.

5.3. Conclusion on Perceived Security Risk.

In the Industrial and Allied sector most of the respondents indicated that there are three areas where there is high-perceived security risk these are: hardware failure; software failure; and laws and regulations. In the Finance and Investments sector most of the respondents indicated that there are four areas where there is high-perceived security risk these are: personnel related problems; hardware failure; software failure; and practices and procedures.

In the Commercial and Allied sector most of the respondents indicated that there are two areas where there is high-perceived security risk these are: hardware failure and software failure.

In the Agricultural sector most of the respondents indicated that there are two areas where there is moderate perceived security risk these are: personnel related problems and practices and procedures.

From the above analysis it can be concluded that most companies agree that personnel related problems, hardware failure, and software failure are perceived to pose the highest security risk. However the combined modal score shows that most companies perceived that the highest risk areas are: personnel related problems; hardware failure; communication systems failure; and practices and procedures. This therefore means that personnel related problems and hardware failures are the highest risk to an information system.

In conclusion, there is no simple answer to the problem of achieving overall information system security. It begins with the genuine awareness by top management, government leaders, users, vendors and systems managers of the need to provably secure information processing systems. Until that goal has been achieved, we will be unable to fulfill the promises of trustworthy open systems architecture and a secure worldwide network computing.

5.4. Recommendations.

The growing dependence on the organizations on computer-based systems means that the data they hold and the ability to process the same constitutes a major corporate asset. Therefore anything that denies the continued access to these assets jeopardizes their ability to conduct business in a timely and profitable manner.

As in most security problems, prevention is the most effective approach and can protect you from about 90% of the problem sources.

The researcher would therefore propose the following measures in order to reduce the risks and enhance control and therefore availability of the organizations computer systems:

- Examine the organizations short and long range strategic needs and develop policies regarding the establishment of guidelines on the use of computer systems.
- Top management must authorize the establishment of the information systems security function, if it does not exist, and provide it with the necessary authority and resources to ensure compliance with information security procedures.
- Establish a capacity planning function to evaluate the adequacy of hardware/software in each information systems operating environment from the perspective of both short and long term strategic planning.
- Develop an overall Information Security plan to include all information processing systems, from Personal Computers (PC's) to mainframes.
- Define and set purchasing guidelines regarding justification and approval procedures for the purchase of all computer systems components, e.g., hardware, software, communications etc.
- Establish a pre-approved list of PC systems components and vendors. Standardize on one or two company brands; but have several sources of supply, particularly for hardware.
- Guidelines must be provided regarding the connectivity of Local Area Networks (LAN's), Wide Area Networks (WAN's), 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.

- To minimize risk, an on-going program of information systems security education, training and awareness must be developed across all staff lines in the organization.

5.5. Limitations of the Study.

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

- Because the nature of this study required divulging security related information some of the members in the population of study considered these sensitive and declined to respond to the questionnaire. Those who responded might have not presented the true security position and therefore might have biased the findings of the study. This is the main limitation of this study.
- The study did not incorporate the views of the end-users of the computer systems.
- Time was also a constraining factor in this study. Due to the short time available for the study it was not possible to guide all the respondents through the questionnaires and therefore some of the questions would have been answered hurriedly.

5.6. Suggestions for Further Research.

This study focused on the managers in charge of information technology within these organizations. This study can be extended to include the end-users so as to find out the actual in-place countermeasures that have been implemented.

Since all the respondents indicated that they have access to the Internet, another area of study would be to find out the impact of the Internet on the organization's security posture.

The scope of this study could also be broadened by looking at privately owned large companies (according to KIRDI(1993) classification in the Kenya Directory of Manufacturing Industries i.e. 500 employees), the findings can be used to perform a comparative analysis against those companies quoted on the Nairobi Stock Exchange.

APPENDICES

APPENDIX I

COMPANIES LISTED ON THE NAIROBI STOCK EXCHANGE

AGRICULTURAL

BROOKE BOND
EAAGADS
G. WILLIAMSON
KAKUZI
KAPCHORUA
LIMURU TEA
REA VIPINGO
SASINI
THETA

COMMERCIAL &ALLIED

AFRICAN LAKES CORP
A.BAUMAN
CAR & GEN
CMC
EXPRESS
HUTCHINGS BIEMER
KENYA AIRWAYS
LONRHO MOTORS
MARSHALLS (E.A)
NATION MEDIA
PEARL DRY CLEANERS
TPS SERENA
STD NEWSPAPERS
UCHUMI

FINANCE & INVESTMENT

BARCLAYS BANK
CFC BANK
CITY TRUST
DIAMOND TRUST
HFCK
ICDC
JUBILEE
KCB
NATIONAL BANK

NIC BANK
PAN AFRICAN INS
STD CHARTERED

INDUSTRIAL & ALLIED

ATHI RIVER MINING
BAMBURI
BOC (K)
BRITISH AMERICAN
CARBACID
CROWN BERGER
DUNLOP
E.A. BREWERIES
E.A. CABLES
E.A. PACKAGING
E.A. PORTLAND
FIRESTONE E.A
KENYA ORCHADS
KENYA N. MILLS
KENYA OIL
KENYA POWER
TOTAL OIL
UNGA

APPENDIX II

QUESTIONARE

SECTION A

1. What is the ownership of the company? (tick one).

Wholly foreign owned [ ]
Wholly locally owned [ ]
Jointly owned [ ]

2. When did your Organization first install computers? (Tick one).

Less than 5 yrs ago [ ]
Less than 10 but more than 5 yrs ago [ ]
Less than 15 but more than 10 yrs ago [ ]
More than 15 yrs ago [ ]

3. How many of the following do you have? (tick in the appropriate box)

Mainframe	: 0 [ ]	1 – 10 [ ]	11 – 20 [ ]	21 – 30 [ ]	More than 30 [ ]
Minicomputer	: 0 [ ]	1 – 10 [ ]	11 – 20 [ ]	21 – 30 [ ]	More than 30 [ ]
Desktop PCs	: 0 [ ]	1 – 10 [ ]	11 – 20 [ ]	21 – 30 [ ]	More than 30 [ ]
Laptop PCs	: 0 [ ]	1 – 10 [ ]	11 – 20 [ ]	21 – 30 [ ]	More than 30 [ ]
Notebooks	: 0 [ ]	1 – 10 [ ]	11 – 20 [ ]	21 – 30 [ ]	More than 30 [ ]

4. Do you have the position of the IT Director ?

Yes [ ]
No [ ]

5. If "no" in question 5 above what is the title of the overall in charge of computer and information services?

Title --

6. Approximately how much (in Kshs) have you invested in your Computer System? (tick one)

Less than 50 million [ ]
Less than 100 million but more than 50 million [ ]

Less than 150 million but more than 100 million [ ]
Less than 200 million but more than 150 million [ ]
Less than 250 million but more than 200 million [ ]
More than 250 million [ ]

7. What was the IT budget of your company during the last financial year?

Less than KShs 1 million [ ]
Less than Kshs 5 million but more than Kshs 1million. [ ]
Less than Kshs 10 million but more than Kshs 5 million [ ]
More than Kshs 10 million. [ ]

8. Does your organization have an acquisition policy for hardware and software ?

Yes [ ]
No [ ]

9. Does your organization have access to the Internet and World Wide Web?

Yes [ ]
No [ ]

10. Does your institution have a written, formal computer security policy ?

Yes [ ]
No [ ]

11. How frequently are your computer security arrangements reviewed ?

Monthly [ ]
Quarterly [ ]
Bi-annually [ ]
Annually [ ]
Any Other (specify) ---------------------------------

12. Are there any annual budget allocations for the security of your computer systems?

Yes [ ]
No [ ]

13. How would you rate the computer literacy level within your organization for the following categories of staff ?
(Tick one)

a) Management: Excellent [ ] Good [ ] Fair [ ] Poor [ ]

Please explain your rating

....
....
....
....
....

b) Non-Management: Excellent [ ] Good [ ] Fair [ ] Poor [ ]

Please explain your rating

....
....
....
....
....

14. Which of the following Information Systems(IS) do you currently use within your organization? (tick if present)

a) Transaction Processing Systems (TPS) [ ]
b) Management Information Systems (MIS) [ ]
c) Decision Support Systems (DSS) [ ]
d) Executive Information System (EIS) [ ]
e) Expert Systems (ES) [ ]
f) Strategic Information Systems (SIS) [ ]

15. Does your organization have a formal strategic plan for Information Technology?

Yes [ ]
No [ ]

Please explain

....
....
....
....

SECTION B

isted below are statements dealing with various issues in the security of computer systems. Please tick ( ) in the ppropriate box to indicate the extent to which you consider the following countermeasures to be important.

	Very Important	←→	Moderately Important	←→	Not Important
ountermeasures.					
Alternative system communication paths are available.	( )	( )	( )	( )	( )
A policy on the use of personal computers for Communication exists.	( )	( )	( )	( )	( )
There are dedicated phone lines for system communication.	( )	( )	( )	( )	( )
A documented network configuration control procedure exists.	( )	( )	( )	( )	( )
A documented procedure exists for adding and removing network users.	( )	( )	( )	( )	( )
The network provides an identification and authentication mechanism(e.g. User ID & password)	( )	( )	( )	( )	( )
A written hardware configuration control procedure is available.	( )	( )	( )	( )	( )
. System preventative maintenance is done on a regular basis.	( )	( )	( )	( )	( )
. Redundant or functionally equivalent system hardware is available.	( )	( )	( )	( )	( )
0. The computer room is kept clear of hazardous material.	( )	( )	( )	( )	( )
1. Changes to the computer room environment setting is controlled (e.g. heat and humidity).	( )	( )	( )	( )	( )
2. Protection against natural disaster (e.g. floods and earthquakes).	( )	( )	( )	( )	( )

	Very Important	←→	Moderately Important	←→	Not Important
ountermeasures.					
. The duties of individuals are separated by a procedure or software.	( )	( )	( )	( )	( )
. Pre-employment screening is done regarding the applicant's previous employment, formal education, criminal history, personal financial situation, drugs and alcohol abuse.	( )	( )	( )	( )	( )
. Technical Personnel are cross-trained in all aspects of managing and maintaining your computer resources.	( )	( )	( )	( )	( )
. A procedure for the management of magnetic media exists.	( )	( )	( )	( )	( )
. You store copies of back-up media separately for the computer.	( )	( )	( )	( )	( )
. You remove data storage media from the system when it is not in use.	( )	( )	( )	( )	( )
. Management is both informed about computer security and supportive.	( )	( )	( )	( )	( )
. A system computer security official is assigned in writing.	( )	( )	( )	( )	( )
1. You have had formal or informal computer security training and aware of information security rules and regulations.	( )	( )	( )	( )	( )
2. The room which houses the computers has restricted access.	( )	( )	( )	( )	( )
3. Communication access points (Closets, rooms, etc) are kept locked.	( )	( )	( )	( )	( )
4. Security monitors and alarm systems are installed in the computer room.	( )	( )	( )	( )	( )
5. Users have a pre-authorized set of system privileges and commands.	( )	( )	( )	( )	( )

	Very Important	⟷	Moderately Important	⟷	Not Important
ountermeasures.					
Log-in to software applications requires a unique identifier.	( )	( )	( )	( )	( )
Computer diagnostic programmes are run periodically.	( )	( )	( )	( )	( )
Partial backups are done at least once a day and full backups of network files are done at least once a week.	( )	( )	( )	( )	( )
Data that are critical to the mission is stored off site.	( )	( )	( )	( )	( )
You virus scan all software before loading into the system.	( )	( )	( )	( )	( )
Log-in attempts are limited to a specific number for the network users.	( )	( )	( )	( )	( )
Vendor (logon) identifications are removed from the network server.	( )	( )	( )	( )	( )
Computer screens are created away from passersby.	( )	( )	( )	( )	( )
A Uninterruptible Power Supply (UPS) is installed for your system.	( )	( )	( )	( )	( )
A backup power source e.g. battery or Generator, is installed.	( )	( )	( )	( )	( )
Access to the computer fuse or circuit breaker panel is controlled.	( )	( )	( )	( )	( )
Critical data is stored in fireproof safes.	( )	( )	( )	( )	( )
Fire detection equipment and extinguishing systems are installed in the computer room.	( )	( )	( )	( )	( )
Computer room is constructed using fireproof material.	( )	( )	( )	( )	( )

	Very Important	←→	Moderately Important	←→	Not Important
ountermeasures.					
0. Computer users have had training on system's hardware and software they use.	( )	( )	( )	( )	( )
1. Computer users have had formal or informal computer security training.	( )	( )	( )	( )	( )
2. Policy forbids using unauthorized or illegally obtained software.	( )	( )	( )	( )	( )
3. All software configuration changes follow a written procedure.	( )	( )	( )	( )	( )
4. A written procedure exists for acceptance testing of software.	( )	( )	( )	( )	( )
5. New software is validated in accordance with an established policy.	( )	( )	( )	( )	( )
6. Resigned or terminated employees are removed from premises.	( )	( )	( )	( )	( )
7. Locks are installed for doors to the computer/ terminal space and network controllers.	( )	( )	( )	( )	( )
8. An inventory of computer related hardware exists.	( )	( )	( )	( )	( )

SECTION C.

1. On a scale of 1-10 please rank the following security related problems in order of the degree of risk to your computer systems. (Ranking Scale : Least Risk=1 , Highest Risk=10).

a). Personnel and other people problems. [ ]

b). Hardware failure. [ ]

c). Software failure. [ ]

d). Communication systems failure. [ ]

e). Physical building facilities. [ ]

f). Practices and procedures. [ ]

g). Laws and Regulations. [ ]

2. Can you please list any serious computer security related problems your organization has experienced.

....
....
....
....

....
....
....
....

....
....
....
....

....
....
....
....

....
....
....
....

....
....
....
....

APPENDIX III

VULNERABILITIES.

1. Susceptibilities to communications activity technology.

2. Susceptibilities to inter/ intranetwork user activity.

3. Susceptibilities to hardware failure or configuration change.

4. Susceptibilities to environmental hazards.

5. Susceptibilities to key person dependency.

6. Susceptibilities to improper handling of storage media.

7. Susceptibilities to Lack of awareness by computer security issues.

8. Susceptibilities to unauthorized physical access.

9. Susceptibilities to unauthorized programmatic access.

10. Susceptibilities to loss of data or software files.

11. Susceptibilities to unauthorized information theft or disclosure.

12. Susceptibilities to failure and instability of electrical power sources.

13. Susceptibilities to fire.

14. Susceptibilities to user operator errors.

15. Susceptibilities to software flaws or inadequacies.

16. Susceptibilities to theft of system resources.

UNIVERSITY OF NAIROBI
FACULTY OF COMMERCE
MBA PROGRAM - LOWER KABETE CAMPUS

Telephone: 732160 Ext. 208
Telegrams: "Varsity", Nairobi
Telex: 22095 Varsity

P.O. Box 30197
Nairobi, Kenya

14th August, 2000

Dear Sir/Madam,

I am a postgraduate student in the Faculty of Commerce, University of Nairobi. In partial fulfillment of the requirements of the Masters of Business and Administration degree, I am collecting data with a view to writing a Management Research Project entitled "**A Computer Security Risk Analysis of Firms Quoted in The Nairobi Stock Exchange."**

The purpose of this letter, therefore, is to request you to assist me by completing the attached questionnaire. The information requested is purely for academic purposes and will be treated in strict confidence. However, the findings of this research can be availed to you upon request.

Enclosed please find a self-addressed and stamped envelope to be used for the return of the completed questionnaire.

If you have any queries or you would like further information about this project please call me on tel. No. 02-577351/2, or e-mail me at **sang@adwest.net**.

Your co-operation in completing the questionnaire is greatly appreciated.

Thank you in advance.

Yours sincerely,

CYRUS K. SANG
MBA STUDENT

Approved

[illegible]

8.0. REFERENCE AND BIBLIOGRAPHY.

Bellovin, S.M. : **"There Be Dragons,"** *Proceedings of the Third Usenix UNIX Security Symposium.* 1993.

Bem, D.J. : **"Self-perception: An alternative interpretation of cognitive dissonance phenomena."** *Psychological Review*, Vol 3, 1967, p. 183-200.

Charney S. : **"Letter from Scott Charney, Chief, Computer Crime Unit, U.S. Department of Justice, to Barbara Guttman,"** NIST. July 29, 1993.

Cooper,J et al : **"Arousal as a necessary condition for attitude change following induced compliance."** *Journal of Personality and Social Psychology*, Vol 45, 1978, p. 1101-1106.

Daily Nation : **"Shs 18 billion to be put in IT Projects,"** *The Daily Nation.*, 11 June 1998, p. 10.

Dizon, O. : **"Evaluation of feasibility of IT Projects by Publicly Quoted Companies in Kenya."** Unpublished MBA Thesis, University of Nairobi.,1999.

Evans R. : **"Security in the Computer Environment,"**IDPM.London, 1994.

Fazio, R.H. : **"Attitude accessibility following a self-perfection process."** *Journal of Personality and Social Psychology*, Vol 47, 1984, p. 277-286.

Festinger, L. : **A Theory of Cognitive Dissonance**. Stanford University Press, Stanford, 1957.

Gaithersburg J. : **"Computer System Security and Privacy Advisory Board,"** *1991 Annual Report.*, March 1992, p. 18.

Garry Dinnie : **"The Second Annual Global Information Security Survey."** *Information Management & Computer Security,Vol 07, Issue 3,1999.*

Infosecurity News : **"Theft, Power Surges Cause Most PC Losses."** *Infosecurity News*, September/October,1993, p. 13.

Jenkins B. D. : **Security Risk Analysis and Management**. Countermeasures, Inc. New York,1998.

Kephart J. O. et al: **"Measuring and Modeling Computer Virus Prevalence,"** *Proceedings, 1993 IEEE Computer Society Symposium on Research in Security and Privacy*, May 1993.

Kiesler, C.A. et al: **" On Inferring one's Beliefs from One's Behavior."** *Journal of Personality and Social Psychology*, Vol 4,1969, p. 321-327.

Nyambane, T. : **"An Evaluation of the Extent of and Factors Limiting Information Technology Usage in Publicly Quoted Companies in Kenya."** Unpublished MBA Thesis. University of Nairobi,1996.

Onunga J. : **The Internet**. Information Systems Academy. Nairobi, 1998.

Rembaum A. : **IPSec VPN Info Pack.** Radguard Ltd. Tel Aviv, Israel, 1999.

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

Sprouse M. : **Sabotage in the American Workplace: Anecdotes of Dissatisfaction, Mischief, and Revenge.** Pressure Drop Press. San Francisco, Carlifornia,1992.

Violino B. et al : **"Tempting Fate,"** *Information Week*, October 4,1993: p. 42.

White K. B. : **"National (UK) Computer Security Survey 1996".** *Information Management and Computer Security, Vol 4,No. 3,1996.*

Wilk R. J. : **Security and Control of Your PC Network.** International Association for Computer Systems Security, Inc. New York, 1993.