

**A SURVEY OF COMPUTER SECURITY
VULNERABILITY IN THE BANKING INDUSTRY IN
KENYA.**

By

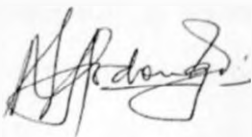
WASILWA O. MESHACK

**A MANAGEMENT RESEARCH PROJECT SUBMITTED IN PARTIAL
FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTERS OF BUSINESS AND ADMINISTRATION (MBA), FACULTY
OF COMMERCE, UNIVERSITY OF NAIROBI.**

Declaration

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

Name : Wasilwa Odongo Meshack



Signature:

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

SUPERVISOR

Name : KIPNGETICH J.K.

Lecturer, Department of Management
Science, Faculty of Commerce,
University of Nairobi.

Signature : 

CHAIRMAN OF DEPARTMENT

Name : KORUKU C.M.

Chairman, Department of Management
Science, Faculty of Commerce,
University of Nairobi.

Signature : 

Dedication

I dedicate this dissertation to my Wife Jane N. Wasilwa and Children Prudence Wasilwa & Mathew Wasilwa. Without their patience, understanding support, and most of all love, the completion of this work would not have been possible.

Acknowledgement

I would like to express the deepest appreciation to my supervisor Mr. Julius K. Kipng'etich who has the attitude and the substance of a genius. He continually and convincingly conveyed a spirit of adventure in regard to research and an excitement in regard to teaching. Without his guidance and persistent help this dissertation would not have been possible.

For everything from conception to finalisation of the project, and lots of stops along the way, thanks to all my friends who gave me the encouragement.

For their helpful suggestions throughout the project, special thanks to Julius Kipngetch and the Management Science team, University of Nairobi.

For their incisive review comments, thanks to Tom Kahigu and Francis Nyawade

For help with research, transcription, resource material and other forms of support, my gratitude to Mr. Julius Kipnegtich, Mr. Cyrus Sang, Mr. Francis Nyawade and the KCB Management Centre.

Abstract

In today's complex IT environments, managing security is made more challenging as businesses expand and extend to a broader consumer base. The enterprise security infrastructure has become populated with diverse technologies installed across heterogeneous systems. This has resulted in pressure on businesses to understand the need for information security, the choices that you have to implement and maintain the right information security strategy for the organisation. Quoting what Walter Wriston, the former chairman of Citicorp, said some years back: "Information about money is just as important as money itself." It underscores the importance of information and the need to guard this information from unauthorized access.

This study aims at determining the Security posture of the banks in Kenya that are in normal operations as per the Central Bank of Kenya regulations. Out of a total of 44 banks, only 30 responded to the questionnaires. This is due to the fact that the study is focused on Security, an area considered very sensitive in the Banking domain.

The study had two objectives namely:

1. To identify various approaches by the management towards security implementation in comparison to the Best practices of Computer security.
2. To establish the level of Computer Security Vulnerability in the Banking Sector in Kenya.

To satisfy the above objectives, data was collected using questionnaires and analysed using various statistical tools including descriptive statistics and factor analysis.

The findings of the study indicate that most of the Banks have made averagely Kshs.109.84 Million as investment in Information Technology. However, most of the Banks do not have an Information Technology professional at the executive Board level.

I am pleased to present to you the results of a Survey on Computer Security Vulnerability at 30 medium and large banks in Kenya. It is my hope that this survey will provide valuable insight on the extent of Security Vulnerability and the level of security awareness in the Kenyan banking institutions and assist the managements' in the betterment of implementing the Best practices of Computer Security.

List of Abbreviations

List of Tables

CoBiT Control Objectives for Information and related Technology.

BS7799 British Standard 7799

DDoS Distributed Denial-of-Service

IT Information Technology

List of Figures

List of Tables

Table Number	Page Number
4.1	37
4.2.1	38
4.2.2	40
4.2.3	42
4.2.4	42
4.2.5	43
4.2.6	44
4.2.7	45
4.2.9	46
4.2.10	47
4.2.11	48
4.2.12	49
4.2.13	50
4.2.14	50
4.2.14	51
4.2.15	51
4.2.16	52
4.2.17	53
4.3	55
4.4.1	57
4.4.2	58
4.5	83

List of Figures

Figure Number	Page Number
2.1	28
3.1	36

Table of contents

Declaration	i
Dedication	ii
Acknowledgement.....	iii
Abstract	iv
List of Abbreviations.....	vi
List of Tables.....	vii
List of Figures	vii
Table of contents	viii
Chapter 1.....	1
INTRODUCTION.....	1
1.1 Background of the Study	1
1.2 Statement of the Problem	4
1.3 Objectives of the Study	7
1.4 Importance of the Study	7
Chapter 2	8
LITERATURE REVIEW.....	8
2.1 Introduction	8
2.1.1 Critical Evaluation – The IT Security Challenge.....	11
2.1.2 The Real Threats	12
2.1.3 The Real Risks	13
2.1.4 The Real Solutions	16
2.2 Major Studies	18
2.2.1 Software Flaws:.....	23
2.2.2 Negligence and Recklessness	25
2.2.3 Failure to segregate duties and /or impose dual controls at the top management.....	26
2.2.4 Compromised password.....	27
2.2.5 Unsecured Audit Logs	27
2.2.6 A web spoofing example.....	28
2.2.7 An Electronic Cheque Handling Swindle.....	29
2.3 Summary	30
2.3.1 Seven Essential foundation elements.....	30
Chapter 3	39
METHODOLOGY/STUDY DESIGN	39
3.1 Population of Study:	39
3.2 Data Collection Method	40
3.3 Data Analysis techniques:	41
3.4 Measurement of Reliability:	43
3.5 Model	44

3.5.1	Introduction to Risk Analysis	44
3.5.2.1	Quantitative Risk Analysis	44
3.5.2.2	Qualitative Risk Analysis	45
Chapter 4	48
DATA ANALYSIS & FINDINGS		48
4.1	Summary of Responses.....	48
4.2	Analysis of IT Resources in the Organisation.....	49
4.2.1	First Computer Installations existence.....	49
4.2.2	Number of Computers.....	50
4.2.3	IT Director's Position.	52
4.2.4	Investments in Computer Systems.....	52
4.2.5	Previous Year IT Budget.	53
4.2.6	Internet and World Wide Web Access.	54
4.2.7	Computer Security Policy.....	55
4.2.8	Security Reviews.....	55
4.2.9	Security Budgets.....	56
4.2.10	Computer Literacy among Management staff.	57
4.2.11	Information Systems.	57
4.2.12	IT Strategic Plan.....	59
4.2.13	Ownership of Companies.....	59
4.2.14	Computer Security Training.....	60
4.2.15	Computer Security Threats.....	60
4.2.16	Knowledge of Passwords.	61
4.2.17	Computer Security Awareness	61
4.3	Risk Analysis.	62
4.3.1	Vulnerability Assessments.....	63
4.3.2	Vulnerability Assessments within Banks.	65
4.4.	Factor Analysis.	66
Chapter 5	94
CONCLUSION		94
5.1.	Conclusions on Status of IT Resources.....	94
5.2	Conclusion on Vulnerability assessment and Factor Analysis.....	97
5.3.	Conclusion on Perceived Security Risk.	105
5.4	Recommendations.....	106
5.5.	Limitations of the Study.....	109
5.6	Recommendations for Future Research	110
6.0	APPENDIX I.....	111
	APPENDIX II.....	113
7.0	Glossary	130
8.0	References and Bibliography.....	133

Chapter 1

INTRODUCTION

1.1 Background of the Study

Computers today are very important, and even integral to all aspects of the activities and operations of organisations and even individuals. As we become critically dependent upon computer information system, we recognize that computers and computer-related problems must be understood and managed, the same as any other resource.

This study will focus on implementation of security in the Kenyan Banking industry, as a reliable system is perceived to carry the elements of confidentiality, integrity and availability of information (CoBiT, 2000). The study tries to establish the level of awareness in terms of security with different players in the industry. As Banks continue investing more and more in the applications and architectures that suit their business /corporate strategies, the issue of security is downplayed by many as it is assumed that this is automatically addressed by the software and hardware vendors. This dates back to the days of Mainframe environments where threats /attacks were unheard off. The system users especially in the Banking sector perceived that a system once installed is immune to security threats that can compromise the vital information or make it malfunction.

Security protects an information system from unauthorized attempts to access information or interfere with its operation. According to a study conducted by the Systems security Study Committee (SSSC) in 1991,their findings show that organisations rate their security needs in terms of confidentiality, integrity and Availability. However, Accountability is another important factor to be incorporated. The definitions of the above terms in brief are as follows:

- Confidentiality : Information is disclosed only to users Authorised to access it
- Integrity : Information is modified only by users who have the right to do so, and only intended ways.
- Accountability : Users are accountable for their security relevant actions
- Availability : Use of the system cannot be maliciously denied to authorised users.

According to, Mwondi (2002), he underscores the importance of Security Awareness by suggesting that companies should create a culture that enables managements to constantly make employees aware of the risks facing the IT installations they work with. He concedes that a good security policy will form a good foundation for implementing the best practices of System Security. Orina (2002) highlights that electronic security is much like securing any business premises. There are locks on the doors to prevent unauthorized entry, checks to ensure that correspondence remains safely filed away from prying eyes, and systems to prevent goods or money from leaving without proper authorization. Just to emphasize on the importance of Computer security, the President of the United States Of America recognised the danger of “information warfare”-attacks against the basic information infrastructure of the country and he issued an executive order on July 15,1996 which stated in part:

“Certain infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services and continuity of government. Threats to these critical infrastructures fall into two categories: Physical threats to tangible property and threats called cyber threats of electronic, radio frequency, or computer-based

attacks on the information or communications components that control critical infrastructures”(Fighting Computer Crime, pg.2).

Thus it is an open secret that System Security is a concern to governments and any organisation that needs to embrace the new technology in terms of doing business that will propel it to market leadership.

1.2 Statement of the Problem

The Banking Industry has been at the forefront of change fueled by technology. It wasn't that long ago that we first experienced the convenience of drive-up teller windows, or first used an ATM, or signed up for electronic deposit of our paychecks. Certainly many banking customers in the developed world have enjoyed the convenience of supermarket banking, and many have enjoyed the convenience of phone banking and the more extensive home banking. Internet banking is a very natural "next" step for the banking industry to take along the e-commerce path, and the banks that are thinking and acting on today's reality will survive and prosper tomorrow (Stafford 2002).

Unlike the mainframe environment that was much a closed environment, the Internet was designed to be open and approachable, with control and trust resting with the users. With the digital nature of the Internet, there are no physical or geographic locations or boundaries. This means that traditional or time-honored physical security is no longer much relevant in an environment with no boundaries. 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, this is not the same in today's rapidly advancing technological world. We can no longer use technical complexity to shield organisations' computer systems from manipulation of unauthorized access. On the contrary, new technology enabled Automated teller Machines/Cash Dispensers and Electronic funds Transfer transactions 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 the Computer Systems, probing for soft spots, weaknesses and operational vulnerabilities, which they can convert into great opportunities. Considering Wilk's statement in 1983, the attacks then were far fetched/remote and thus the ball game has now changed over a period of time. With easily accessible tools and education material on the Internet, a casual guest has ability to launch a fairly sophisticated attack with minimum effort/skill on their part. In a recent security workshop in Nairobi [May, 2002], Patrick Evans of Symantec group talked widely of the new kinds of blended threats.

Fraud, theft, hacking and breaches of confidentiality and Data integrity are potential hazards that face Computer systems in the Banking environment. It is hard to believe that five years ago almost none of us were on the Internet, but today many of us would feel that our lives had been disrupted if our Internet Service provider went down, even a few hours. In most of the developed world like Europe and America, it is simply not an option for a business and especially financial services system, to go back to serving its customers the old fashioned way should their computers go out. Press reporting of security breaches over the net, such as hacking and theft details, has been widespread and many system flaws that result into fraud are never reported.

Our increased reliance on computers and other technology raise a new set of security needs. With the increased publicity of system flaws and other security breaches, it raises a question in our minds whether the assumption that the computer solutions in the Banking sector are security foolproof. 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.

As the technology continue shaping up business models and especially in Kenya where Technology has been utilized as a strategic tool in providing competitive edge to the rest of the competition, the Banks have not been left behind in embracing the new technology into their corporate network infrastructures. The study by Richu done over 10 years ago cut across the financial sector and a lot has changed in the world of Information Technology in terms of advancement, security threats, availability of free education material and tools from the Internet

The trend by banks in moving from predominantly Mainframe environments, which were closed systems towards Risk and Internet technologies such as Internet banking, Telephone Banking, Automated call centres and other delivery channels such as ATMs etc in order to satisfy customer expectations in terms of delivery of services means more exposure to risks. Considering the accelerated growth of Information Technology that has already been incorporated in the Banks Computer Systems, there has not been a commensurate or equivalent awareness and investment in Computer Security. Therefore, there exists a definite gap between the Information Technology solutions acquired and implemented in the Banks, and the level of Security put in place to secure or protect those systems. This study will mainly focus on the Computer security Vulnerability in the Banking sector in Kenya.

1.3 Objectives of the Study

The objectives of this study are: -

1. To identify various approaches by the management towards security implementation in comparison to the Best practices of Computer security.
2. To establish the level of vulnerability of the Computer Systems.

1.4 Importance of the Study

1. This study will assist in establishing the level of awareness in the Kenyan banking industry about computer security as articulated by the Best Practices.
2. The study will also provide an analysis of what the people in the banking industry perceive to be a threat to information and how they manage the risk.
3. The study will bring to the forefront the security loopholes that surround computer systems in the banking industry and enforce the need to implement the Best Practices of security as documented under BS 7799 or CoBiT security standards.
4. The study will provide the management of the Banks with an objective assessment of its information security posture.
5. The study will assist the government with formulating legislature that concerns Data Protection and computer security
6. The study is also expected to form a basis for further research in the area of Computer security in the banking sector.

Chapter 2

LITERATURE REVIEW

2.1 Introduction

As Computers become more pervasive in every field of human activity, the security of information stored on them becomes a societal concern. Increasingly, computers are used to store data that may be considered sensitive (e.g. Health Information, Customer Information etc). Unauthorized access to such data renders the individuals and firms about whom data is stored vulnerable to embarrassment, discrimination and even extortion. Likewise, the custodians of the private data are exposed to greater risk of legal suits and even fallout from the customers because of lack of confidence. Secondly, computers are often embedded in the operation of mechanical and electrical equipment (e.g. telephone switches, traffic control systems etc), whose malfunction due to hardware or Software failure poses serious threats to public safety. Finally the potential for abuse has multiplied significantly in a networked environment wherein physical proximity to a computer is no longer a requirement for operating the computer-all that is needed is a connection to the machine over some combination of public and private networks (Amit Das, 1997). 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. Evans (1994) notes that this may have been true of the past when 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 make this belief no longer true.

Form of the cutting edge of technology, innovations in communications, computers and software command the attention of leading financial institutions. Advanced technology provides a unique opportunity for Banks to leapfrog the competition by providing efficient ways for quality delivery, product differentiation and product costing.

However, the implementation of information technology in the banking industry is today uneven (Chorafas, 1998). Although most private financial networks share a common set of technical design characteristics such as transmission, signaling, synchronization, regulatory restrictions etc-each has its own competitive advantages or disadvantages that depend on the way it is:

- Designed
- Implemented
- Used and
- Maintained

A bank's private network exists for the benefit of a large class of customers, not to mention its own organisation for which timely, error free and leading edge information is vital. Customers with large and growing real-time information needs want to deal with a bank possessing a highly efficient banking network, able to ensure quality of service, security, timeliness, bandwidth as well as offering reliable networked financial services.

In this age of connectivity, customers are getting extremely tech-savvy and demanding. Every day they are exposed to a glut of information. In such scenarios, banks are forced to get more customer focused, improve customer service and offer innovative products to meet the requirement of their customers. Dr. Dimitris N. Chorafas (1998) explains that successful banks need applications that can address the key issues of this exciting e-age. For this

- One must invest in a platform that can offer innovative products to meet all the requirements of customers
- Enable the interface with multiple delivery channels in an integrated manner to ensure 24x7x365 service levels across channels
- Be agile enough to respond to any market requirement and competition quickly
- Inter-operate with other business applications on a real-time basis
- Embrace new generation architecture, safeguard IT investments and empower employees in becoming knowledge workers
- Allow banks to take full advantage of the e-commerce revolution
- Be complete in design and functionality rich
- Have sophisticated multi-level security to minimize the risks of unauthorized use of data and illegal access (Finacle Newsletter, 2002).

Unfortunately, application vendors develop their systems with the primary purpose of meeting the customers' requirements, security being considered the last area of concern/ priority. The users on the other hand measure the affectability of a system by establishing how easy it is to manipulate, user-friendly screen, and availability without assessing the security aspects of the system. Thus a good system to the vendor is what can satisfy the end user processing/transaction requirements while a good system to the end user is how user friendly it is and whether it can address their day-to- day operations. Banks that used to operate legacy systems were not prone to security threats as the new systems that have come in to replace which are very vulnerable to threats. This made most of the users within the Banking industry who still operate within the mainframe environments to assume the security aspect of systems and imagined that any system was above any kind of threat or attack. This is not anymore where computers operated in standalone environments. In 1950s, 1960s and 1970s the computer was the centre of the IT universe. Since the 1980s, however, the network has become a Christmas tree and computers hang on it

like ornaments. This has increased the probability of attacks/threats (Chorafas, 1998).

Considering the stages of evolution IT has undergone over the years, it is foolhardy to assume that the systems in operation are security proof and all the data is safe. According to Jenkins (1998), security measures cannot assure 100% protection against all threats. However, the process of evaluating system vulnerabilities and threats facing it coupled with the methods used to mitigate the risks provides a generalized conceptual understanding of how in-depth the management and the organisation at large is aware about Computer security.

2.1.1 Critical Evaluation - The IT Security Challenge

Much attention has been paid recently to companies and organizations under fire from external and internal hacks and plagued by new waves of viruses, e-mail worms and Distributed Denial-of-Service (DDoS) attacks. This focus is warranted as viruses like the much-discussed "I Love You" bug and worms such as "sadmind/IIS" have meant crashes, downtime and data leaks. But what can companies and their IT administrators do to truly shore up their systems' defenses and strengthen their networks' security? What steps should be taken to build a robust network, maintain an efficiently administered system and establish enforceable security policies for all users? The best steps can be identified and taken only when organizations acknowledge and understand the real threats, the real risks and the real solutions of IT security [Blake 2001].

2.1.2 The Real Threats

There are three real threats that every company should be aware of and address: “Hackers”, “Insiders” and “Spies” says [Scott Blake, 2001].

“Hackers”, although they receive the most attention and carry a rebel mystique, are the least of your worries when it comes to securing your network. Hackers can use their skills towards their ends, which may range from trivial to political in scope. By undermining the security of a web server, they may access any legitimate organisation’s web page and change its contents. Similar attacks are occurring with increasing regularity, and before and after versions of web pages, which have been attacked, are available for viewing online [2600,1997]. In some cases, the hackers have squandered their opportunity to effect change or promote any political view. One such case is that of the hacked CIA’s home page, which was modified to include a link to a “naked women”. In other cases, effective use has been made by the hacking of the Republic of Indonesia’s web page, which was modified on more than one occasion to include anti-Indonesian, Pro East Timor propaganda. Basic security measures such as vulnerability assessment software like Symantec Enterprise Security Manager (which will scan networks for possible security risks and alert IT administrators so that they can close up those holes) scanning tools and updated password programs will keep hackers out and your information safely in.

A much more tangible threat comes from company “Insiders”. Disgruntled current employees and former workers are often the most dangerous security threats and account for up to 75 percent of all security breaches, according to FBI statistics. The Computer Security Institute [iQ Magazine, 2002] estimates that between 60 percent and 80 percent of network misuse comes from within the enterprise. Even the normal employee who is adventurous or have curiosity, when presented with open systems can be tempted. Employees may already have access to a company’s

network and, most likely, know the network fairly well. This combination of access and knowledge can spell disaster when placed in the wrong hands. In order to diminish the threat of “Insiders”, organizations should establish strict security policies and develop internal processes to enforce those policies. Deployment of Security appliances like internal Firewalls (e.g. Velociraptor), firewall software like Cisco Pix, Intrusion Detection Systems & enterprise Security Managers will keep a check on security violations of the system, whether internal or external.

Finally, “Spies” pose a veritable threat to an organization’s IT infrastructure. Whether these often-paid sleuths looking for company secrets and information come from a competitor’s ranks or from elsewhere, they are often armed with plenty of time and resources to study your network. Again, established and enforced security policies can help to lessen this threat. Vulnerability assessment software and administration tools can help IT administrators to shore up a network’s defenses by alerting your IT department when there are potential holes and security risks present in your network and informing them about how to close these gaps. By knowing if these holes exist and where they are, IT administrators can prevent “Spies” from gaining access to the network.

2.1.3 The Real Risks

There are various real risks that IT administrators should be aware of when securing and administering their networks: “Passwords”, “Known Software Flaws”, “Inattention to Security”, “Content Management” and “Access Control”(Blake, 2001).

“Passwords” are, in many cases, the first and last line of defense. Often, passwords are not changed frequently, are shared between users on a common desktop computer or are displayed in easy-to-see places such as on the computer itself.

These habits, while perhaps more convenient on a day-to-day basis, create more security threats and attack risks for IT administrators. Network administration software and security management products are available (e.g. Lopht) that will scan all passwords for common words or easy-to-break codes, identify inactive log-on and alert IT administrators as to which passwords have not been updated. These software programs can act as another layer of password security insurance and can keep possible security holes closed.

“Known Software Flaws” are perhaps the most preventable security risks and those often overlooked by organizations in their quest to strengthen their networks. Each year security teams, security institutes and software companies issue hundreds of alerts and patches for these known flaws. According to St Bernard Software Inc. of San Diego, USA, Microsoft constantly releases patches for Microsoft Windows XP/NT/2000, Terminal Servers, IIS, SQL Server, Exchange, Internet Explorer, Media Player, Netmeeting, Office and Outlook. These patches primarily focus on Security Vulnerability & system Stability. If the patches are not implemented well, these could cause the system to suffer vulnerability and instability. Security holes in software have a negative impact on your business. With one breach of your systems, a malicious intruder can change your web site content, dump critical files, destroy and steal customer data etc. These events result in downtime and affect the bottom line.

While the alerts raise awareness for IT administrators, they also raise red flags for hackers and people who will then use the identified vulnerabilities to access networks. Consequently, patches must be applied to correct bugs, flaws and security holes. Additionally, patches must be updated and IT administrators should be constantly scanning their systems for unpatched flaws. Software programs are available that will continuously scan a network for these flaws, alert IT administrators if there are patches needed and actually direct them to the patch or

further information, for example UpdateEXPERT Software from St Bernard company in USA.

The third real risk as outlined by Scott Blake [2001] is a “General Inattention to Security”. While it's hard to imagine that any organization or IT administrator could ignore security, it's not hard to understand why security may not be the most pressing issue. In a time of e-age when continual “uptime” is essential and “downtime” can mean losses of millions of dollars, IT administrators are often focused on keeping systems running. IT administrators that focus on security can help to increase this “uptime” as a safer system will be more secure when up against hackers, viruses and bugs. Again, software programs that continuously scan systems or that automate queries and automatically generate reports can help IT administrators by cutting down on the time it takes to tend to system security.

The fourth risk is “Content Management”. Many system administrators pay attention to the security of the Core system giving little consideration about how the outputs of those systems are stored and managed. a typical example would be an output fro a banking system, which is ported into an excel spreadsheet ready to be transmitted as an Electronic File Transfer (EFT) file. There are no security measures incorporated in this kind of auxiliary applications that users sometimes use to make their work easy.

The fifth risk is “Access Control” to corporate data. A number of systems in the Banking industry are not certified CoBiT or BS 7799 systems and thus several system loopholes in terms of security are ignored. A user might have access to several different data views, of which some areas might not be relevant to their day-to-day operations. This is made possible from the system's poor or inefficient system security policy. An example is a Manager of a unit, who is given upper most rights almost comparable to the system administrator. Thus the managers can

be able to have a view of several screens without violating any security. This is dangerous for that manager who may want to be adventurous or a want to cause some damage to the organisation's data or may be sale it out to those interested in the information.

2.1.4 The Real Solutions

The real solutions for organizations and IT administrators that address the threats and risks outlined above are categorized into four [Blake, 2001]. Many of these solutions have been mentioned in the course of explaining these threats and risks. The four real solutions are: "Security Policy", "Firewalls", "Constant Assessment" and "Making System Administrators Responsible for Security". Also, according to an article on Network security in the IQ Cisco Magazine [2002], it identifies the following as solutions to threats and attacks. These are Access Control, Firewall, Encryption, Intrusion Detection and Network Scanning. Analyzing from the two sources of information on solutions to the threats and attacks, we can outline the following as the controls that will mitigate the threats and attacks of a system.

1. "Security Policy" is necessary and can aid in an organization's cost/benefit analysis. When security policies are set and enforced, a plan is created of which everyone is aware and to which everyone is expected to adhere. Effective security policies spell out requirements, policies and ramifications. Additionally, the strongest security policies are constantly re-evaluated and measured against in order to gauge their success.

2. Firewalls

The second real solution is "Firewalls". "Firewalls", while inefficient when used alone, are a very important first step to overall system security. When used wisely, firewalls systems are put in place in order to provide a barrier

between an organization's internal information and files and external Internet users. Firewalls help to keep company information protected internally and to block external data and materials that may be harmful to the IT infrastructure.

3. Constant assessment

“Constant Assessment” is the third of the real solutions and overlaps onto many of the other solutions. Only organizations that constantly assess, analyze and then administer their IT infrastructures can set benchmarks for security, monitor security progress and determine security success. For example, Network scanning conducts detailed analysis of network activities to identify potential vulnerabilities.

4. Access Control

Access Control validates the user's identity and determines entitlement to information and applications based on user profiles. Authorization and privilege management depend on directories that include user process, and object security attributes based on security policies and business rules. Authentication methods range from simple password systems to biometric devices that scan physical characteristics such as fingerprints.

5. Encryption

Encryption ensures that messages cannot be intercepted or read by anyone but the intended recipient. As more information travels over public networks, the need for encrypting the information becomes more important. Companies

can implement encryption at both the network and application-to-application layers.

6. Intrusion Detection

Intrusion Detection analyses network activity, detects security breaches, and sends alarms to administrators across the network. By monitoring network and transaction activity, companies can detect attacks at different levels.

7. Accountability

Finally, Making System Administrators Responsible for Security allows organizations to empower their IT professionals to protect the infrastructures they administer. These organizations should be certain to also provide the time, training and resources necessary to allow system administrators to be effective system security officers.

Major Studies

The nature of Threats and attacks are ever changing due to rapid technological changes, globalization and the relaxation of trade barriers, which are among the factors that give opportunities for new, and more sophisticated computer system threats and attacks. Some security threats include viruses, Trojan horse programs, vandalism, Data interception, social engineering etc. according to the iQ Magazine [2002], attacks come in three basic forms namely reconnaissance attacks, access attacks and denial of service attacks. According to a Fraud survey report by KPMG [2002], the following valuable points can be noted: -

68% of respondents indicated that employees were the major source of their frauds and accounted for the largest financial loss. This clearly supports the argument that most of the security breaches are done better by insiders.

70% of respondents indicated that they have written policy documents containing guidelines about acceptable ethical behaviour; however, only 18% of these respondents have an ethics officer or committee designated to deal with ethical issues in the company. This implies that no proper mechanisms are put in place to enforce enacted policies.

- Financial services had the highest cases of fraud. This implies that they are real targets.
- The report also indicates that out of the frauds discovered, only 3% were detected through IT system controls. This shows that very few security breaches are detected via the IT system controls, thus many go undetected.

A Little over a year ago, i.e. on October 1,2001, the SANS Institute and the National Infrastructure Protection Center (NIPC) released a document that summarized the Ten Most Critical Internet Security Vulnerabilities. The document mentions that the majority of successful attacks on computer systems via the Internet can be traced on exploitation of security flaws. It gives an example of the solar sunrise pentagon hacking incident and the easy and rapid spread of the code red and NIMDA worms as a result of unpatched software. An example of a vulnerability discovered by the institute is the default installs of operating systems and applications. Most software, including operating systems and applications, comes with installation scripts or installation programs. The goal of these installation programs is to get the systems installed as quickly as possible, with the most useful functions enabled, with the least amount of work being performed by

the administrator. To accomplish this goal, the scripts typically install more components than most users need. The vendor philosophy is that it is better to enable functions that are not needed, than to make the user install additional functions when they are needed. This approach, although convenient for the user, creates many of the most dangerous security vulnerabilities because users do not actively maintain and patch software components they don't use. Furthermore, many users realise what is actually installed, leaving dangerous samples on a system simply because users do not know they are there. Those unpatched services provide paths for attackers to take over computers.

According to SANS Institute resources, operating systems default installations nearly always include extraneous services and corresponding open ports. Attackers break into systems via these ports. In most cases the fewer ports you have open, the fewer the avenues an attacker can use to compromise your network. For applications, default installations usually include unneeded sample scripts .One of the most serious vulnerabilities with web servers is sample scripts. Attackers use these scripts to compromise the system or gain information about it. In most cases, the system administrator whose system is compromised did not realise that the sample scripts were installed. Sample scripts are a problem because they usually do not go through the same quality control process as other software. In fact they are shockingly poorly written in many cases. Error checking is often forgotten and the sample scripts offer a fertile ground for buffer overflow attacks. According to another example from the Computer Incident Advisory Capability described in their information bulletin, they indicate that some vulnerability in hardware firewalls may allow attacks to go undetected and thus unrecorded. These can only be sorted out by applying the required software patch. According to CIAC, circumvented Intrusion Detection Systems can impair virus infection investigations.

Wilk [1993] argues that the increasing use of computers by commercial, government and law enforcement organisations has resulted in large concentrations of data and assets in a system, which has become the favourite target of dissident groups. The computer has occasionally been a target for anti-establishment rebels & anti-war protesters and rampaging students. The height of this activity was felt during 1970 when the U.S Army Mathematics Research centre at the University of Wisconsin was bombed, resulting in massive destruction and loss of data estimated at 7.5 Million Dollar loss. Data that had been collected over a 20 year period and represented 1.3 million man hours of effort was also irretrievably lost [Wilk, 1993]. A similar terrorist attack happened in Kenya in August 1998 and severely damaged the Computer infrastructure of Cooperative Bank of Kenya.

Errors and Omissions are a 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. Users, data entry clerks, system operators, and programmers frequently make errors that contribute directly or indirectly to security problems. 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 sixty five percent of losses to organisations were the result of errors and omissions [Gaithersburg, 1992]. Errors attributed to installations and maintenance can cause security problems too. 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].

A 1993 Information Week/Ernest and Young study found that ninety percent of Chief Information Officers viewed employees “who do not need to know” information as threats [Violino, 1993]. Computer fraud and theft is largely the work of insiders. Since insiders have both access to and familiarity with the installed systems, including the overall design and architecture, authorised system users are in a better position to commit crimes. In the late eighties, a clerk in one of the large Kenyan Banks defrauded customers by debiting each client in the system with a 50-cent and crediting an anonymous account by the same every time when the end of day was being performed. Although the debits from the customer’s accounts looked negligible, the overall net effect was large in terms of money lost.

Employee sabotage is a great threat especially for those leaving an organisation due to downsizing or /and sacking. They might cause the most damage, mischief or sabotage. According to Sprouse [1992], the downsizing of organisations in both the public and private sectors has created a group of individuals with organizational knowledge, who may retain potential system access. Sprouse [1992], in sabotage in the American Workplace, reported that the motivation for sabotage could 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.

Malicious Code is another form of threat that has been studied and found harmful to Computer Systems. They include viruses, Worms, Trojan Horses, Logic Bombs and other uninvited software. Studies show that they can attack a wider range of different 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”. The rate of PC-DOS virus incidents in medium to large North American businesses appears to be approximately one percent per 1000 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].

In the book written by Parker [1998], *Fighting Computer Crime*, he narrates several occurrences where there have been computer abuse and misuse, impacting negatively to the security of the system. The following examples will constitute experiences due to system vulnerabilities.

2.2.1 Software Flaws:

I: A flawed System for Protecting the Transfer of Funds

In the 1980's, British Banks proposed a new Security measure for Electronic Funds Transfers. The measure, called the Standard Test Key (STK), treated monetary values only as series of three-digit groups-which resulted in major problems. The Banks planned to use the technique to check the authenticity and integrity of messages that authorised the transfer of money from one bank to another. In these messages, the sending bank would replace each unit of information, such as the name of a bank, the date, and the amount of money to be transferred, with a code number obtained from a codebook. The bank's computer would sum these numbers to yield a number-called the Test Key-that it placed at the end of the message. Any error in transmission or change in the message after it left the sending bank would produce a different The Key, which would

warn the receiving bank not to act until the discrepancy was resolved.

Designed to reduce the number of codes that the banks had to keep track of, the STK system used standardized (and easily obtainable) tables of four –digit code numbers for the words that were transmitted. Since monetary amounts usually exceeded four digits, they needed to be broken up into three –digit groups. For example, if Bank A had an account at Bank B and instructed Bank B to transfer sums totaling \$ 191,975 from that account to three other accounts in Bank B, the total would have been coded by checking the STK tables for the code for 191 (5580) and 975 (5359). Adding the two code numbers, would produce a sum of 10,939, which, with other code numbers, would yield the STK. Unfortunately, the same STK would result from transfer of \$975,191, an amount created by transposing the first and the last three digits. An enterprising criminal would tap into the transmission line and send an additional message to transfer the surplus \$783,216—the difference between \$975,191 and \$ 191,975—to an account that the thief had set up under a fictitious name at Bank B, the STK would be unchanged, and the bank would remain unsuspecting until it reconciled its account with the sending bank—but presumably long after the thief had emptied and closed her account. The thief would not need to know what amounts were being transferred. With the transmissions between the banks routed through her computer, she could simply program it to calculate whatever additional amounts would result in the same code numbers as those in the genuine messages. Fortunately, the

banks dropped the STK idea and introduced the encrypted message authentication codes (MAC).

II: The Millennium Bug/Problem

Before year 2000, the date fields representing years had a capacity of only two digits in most computer programs. In the year 2000, computers interpreted going from 99(1999) to 00 (2000) as going from 1999 to 1900. The program occurred in applications that relied heavily on dates such as amortization, planning and budget systems.

2.2.2 Negligence and Recklessness

The ethics, Crime and Loss considerations of a software theft.

A small software company fired a programmer but neglected to cancel her authorization to access files on the company's computers. Following her termination, the programmer spent many hours downloading proprietary software from the company's computers over telephone lines into a her home PC. Her intent, which she later admitted, was to use the software to start her own company. She had written and participated in developing much of the software and felt that she had some proprietary rights to it. To protect the software at the ethics level, the stakeholders needed to consider the various parties' understanding about the proprietary rights to the software produced by the employees and possessed by the company. These rights should have been documented in employee contracts with informed consent clearly spelt out in written policies. The company may have also been

negligent in tempting the perpetrator to act by failing to cancel her authority to use the computers.

2.2.3 Failure to segregate duties and /or impose dual controls at the top management

Collusion in a Big Bank Fraud.

On February 5,1995, Reuters News Service reported,” BANK WORKERS STEAL 1,630 MILLION YEN, CLEANUP ON A MAJOR BANK CRIME.” According to the story, three conspirators used personal computer money transfer system at a Tokyo bank to successfully transfer 140 Million yen to an account in another bank using a settlement system operated by personal computers, then withdraw the money on the same day. The following day, the thieves sent a total of 1,490 million yen in three unauthorized transfers from the accounts of various companies with the same intent. One of the people involved in the thefts was an employee of the Tokyo bank’s system department. Another was an employee of a software house who had worked for the bank under contract as an onsite system development engineer. The third was the president of the software house, allegedly associated with the Japanese organized crime activities. The SRI-Tokyo staff discovered that the thieves used a “one time” transfer application that was intended for occasional funds transfers. this type of funds transfer service requires four passwords; one for the company that wishes to transfer the money; one which is assigned by the bank for the intended recipient of the money; one for the fund’s transfer service; and one that is defined for each transfer transaction. According to newspaper accounts, the first three passwords are stored on the host computer in the bank in encrypted

form. The staff of the systems department is able to obtain those passwords, but only with the “top manager’s approval.” The bank confirms the transfer by letter to the customer who initiated it on the following day, whether the transfer occurred or not. This crime is probably attributable to a combination of security lapses including failure to segregate responsibilities, a failure to properly monitor contract employees and a failure to strictly maintain password security.

2.2.4 Compromised password

In a European company, a funds transfer clerk secretly observed his associate’s private password as he typed it on the keyboard. The clerk, using his own and his associate’s passwords, attempted to fraudulently transfer over \$ 50 million to his accomplice’s account in Lausanne. A bank clerk in Lausanne noticed the large transfer amount and called headquarters to confirm the transaction. He was arrested.

2.2.5 Unsecured Audit Logs

A small Business Crime.

Joe was the one and only computer programmer and operator in small savings bank in California. He came in to work early one morning, ran the computer for the equivalent of an entire banking day in about twenty minutes, and engaged in only one transaction, moving \$40,000 from a stranger’s account into his girlfriend’s account. He then removed the electronic and printed reports and audit log and turned the computer’s clock back to the correct day. Unfortunately for him, the stranger inquired about her account before the girlfriend could withdraw the money, and Joe was caught.

2.2.6 A web spoofing example

Spoofing is generally defined as any type of deceptive impersonation. Computer Internet spoofing consists of sending messages with disguised return addresses through networks to make it difficult, or impossible to trace the original source. IP spoofing changes the Internet Protocol source address to accomplish the same goal. Web spoofing is a relatively new crime method that is more dangerous, and more difficult to detect, than IP spoofing. Ric Steinberger offers the following description of a web spoofing attack, which involves establishing a malicious web server, then deceiving web users into entering a web site using the malicious web server as an intermediary. When Web browser users visit a web site, they usually type something similar to the following web site address: `www.company.com`. It is easy, however, to make a mistake and accidentally type `www.c0mpany.com`, using a zero instead of “o”.

If `c0mpany.com` actually exists, a perpetrator can set up his web site to mimic the real `www.company.com` site. And he can keep this bogus site inserted between unsuspecting browser users and the “genuine” sites that they visit. If a user requests a secure web connection, the perpetrator’s web site can set one up—but between the user site and the desired genuine site that the user wishes to visit. If web users have their browsers configured to trust certificate authorities (which is often the default state for browsers), establishing what they perceive as a “secure” web connection does not defeat the spoofing web server.

2.2.7 An Electronic Cheque Handling Swindle

In April 1980 a man calling himself Marvin Goldstein (not his real name) opened a cheque account with Maryland financial organisation with a cash deposit of \$15,000. One week later, Goldstein returned to the branch and withdrew \$14,000 from his account, reducing his balance to \$ 1,000. His account then remained dormant until May 6, when he deposited a cheque for \$ 880,000 at a second branch located a few blocks from the branch where he had opened the account. The cheque was then processed in the usual manner with no special safeguards. Banks are generally not notified when cheque deposited with them are paid by the payer bank. The large volume of cheque in the banking system would make such a notification system expensive and unwieldy. If payment is refused, however, the payer bank must notify the depository bank refusal promptly. In order to protect themselves against uncollectable cheques, banks commonly estimate the amount of time the cheque is likely to spend in the collection system before reaching the payer bank and place a hold on the deposited cheque for that length of time. After that time has passed, the depository bank assumes that the cheque had cleared.

In this case, however, Goldstein had printed a faulty Magnetic Ink Character Recognition number on the cheque, cleverly designed to slow down the processing time. As a result, the cheque did not reach the payer bank until eight days after its deposit at Union trust, well after automatic hold had been lifted. Meanwhile, Goldstein was allowed to transfer by wire \$ 660,9000 to the account of a Maryland coin dealer and had disappeared with \$ 660,000 worth of coins before the financial organisation was notified that the cheque was fraudulent. Goldstein was never caught.

The above studies indicate that installed systems are not perfect in themselves and security measures have to be undertaken when implementing the Banking systems. Thus a benchmark for minimum-security configuration depending with the complexity of the banking systems in respective institutions must be addressed and incorporated in the networks in order to protect information from threats and attacks.

Summary

2.3.1 Seven Essential foundation elements.

The goal of information technology security is to enable an organisation to meet all of its mission/business objectives by implementing systems with due care consideration of IT-related risks to the organisation, its partners and customers. The proposed framework model of security is referred to as the “MOT” framework model. The “MOT “ which stands for Management, Operational & Technical security, provides a baseline that will be used to address the seven essential elements of security that are mentioned above. The “MOT” model proposed formulates the standard due care of security implementation in organisations with a purpose of satisfying the seven essential foundation elements of security.

If any of them is omitted, information security is deficient in protecting the business. I will demonstrate by use of examples on how the seven elements constitute the framework of Computer Security in the banking Industry.

1. Confidentiality (of data and system information)

Confidentiality is the requirement that private or confidential information not be disclosed to unauthorized individuals. Confidentiality protection applies to data in storage, during processing and while in transit. For many organisations, confidentiality is frequently behind availability and integrity in terms of importance. Yet for some systems and for specific types of data in most systems (e.g. authenticators), confidentiality is extremely important.

Example:

There exists an online Customer Database Management System that generates reports about the current status of the Customer Balances in their Accounts. These reports not only represent corporate information that must be protected from release outside the company, but also contain Customers valued information. In order to preserve Information privacy, it may be appropriate to restrict the access to such reports, even within the company, to those who have a legitimate reason to be looking at those reports.

2. Integrity

The information must be protected from unauthorized, unanticipated, or unintentional modification. Integrity has two facets:

- Data Integrity-the property that data has not been altered in an unauthorized manner while in storage, during processing or while in transit. This also covers authenticity of the information i.e. a third party must be able to verify that the content of a message has not been changed in transit & Non-repudiation-The origin or the receipt of a specific message must be verifiable by a third party

- **System Integrity**-the quality that a system has when performing the intended function in an unimpaired manner, free from unauthorized manipulation.

Example:

An intruder can prevent an authorized user from referring to or modifying information, even though the intruder may not be able to refer to or modify the information. Causing a system "crash," disrupting a scheduling algorithm, or firing a bullet into a computer are examples of denial of use. This is a form of sabotage.

3. Availability

The information technology resource (system or data) must be available on a timely basis to meet mission requirements or to avoid substantial losses. Availability also includes ensuring that resources are used only for intended purposes. Availability is a requirement intended to assure that the systems work promptly and service is not denied to authorised users. This objective protects against:

- Intentional or accidental attempts to either:
 - Perform unauthorized deletion of data
 - Otherwise cause a denial of service or data
- Attempts to use system or data for unauthorized purposes.

Availability is frequently an organisation's foremost security objective

Example:

A rejected contract programmer, intent on sabotage, removed the name of a data file from the file directories in a credit union's computer. Users of the Computer and the data file no longer had the file available to them because the computer operating system recognizes the existence of information available for users only if it is named in the file directories. The credit union was shut down for two weeks while another programmer was able. The perpetrator was eventually convicted of computer crime.

4. Utility

In this case, an employee routinely encrypted the only copy of valuable information stored in his organisation's computer, then accidentally erased the encryption key. The usefulness of the information was lost and could be restored only through successful cryptanalysis.

To preserve utility of information, the management require mandatory backup copies of all critical information, and control the use of powerful protective mechanisms such as cryptography. Management should require security walk-through tests during application development to limit unresponsive forms of information. It should minimize the adverse effects of security information use, and control the types of activities that enable unauthorized persons to reduce the usefulness of information.

The loss of utility can vary in severity. The worst-case scenario would be the total loss of usefulness of the information with no possibility of recovery. Less severe cases may range from a partially useful state with the potential for full restoration of usefulness at moderate cost.

5. **Accountability**

Information Security accountability and responsibility must be clearly defined and acknowledged. The roles and actions of everyone who has access to information must be clearly defined, identified and authenticated at a level commensurate with the sensitivity and criticality of the information they are accessing. The relationship between all parties, processes and information must be clearly defined, documented and acknowledged by all parties. All parties must have responsibilities for which they are held accountable.

Example:

Irregular Network Traffic

An institution's security officer was having difficulty in locating anomalous packet traffic on his network. When the systems administrator checked through an installed network management system, he determined that a client was running a modem. Seems the manager of that lone department wanted a "better" internet connection so he routed his employees through pop ISP, all without firewall protection, allowing external packets into the companies secure environment.

6. **Assurance (that the other five objectives have been adequately met)**

Assurance is the basis for confidence that the security measures, Managerial, operational and Technical, work as intended to protect the system and the information in process. The other five security objectives (Confidentiality, Integrity, Availability, Accountability & Utility) have been adequately met by a specific implementation when:

- Required functionality is present and correctly implemented
- There is sufficient protection against unintentional errors (by users or software), and

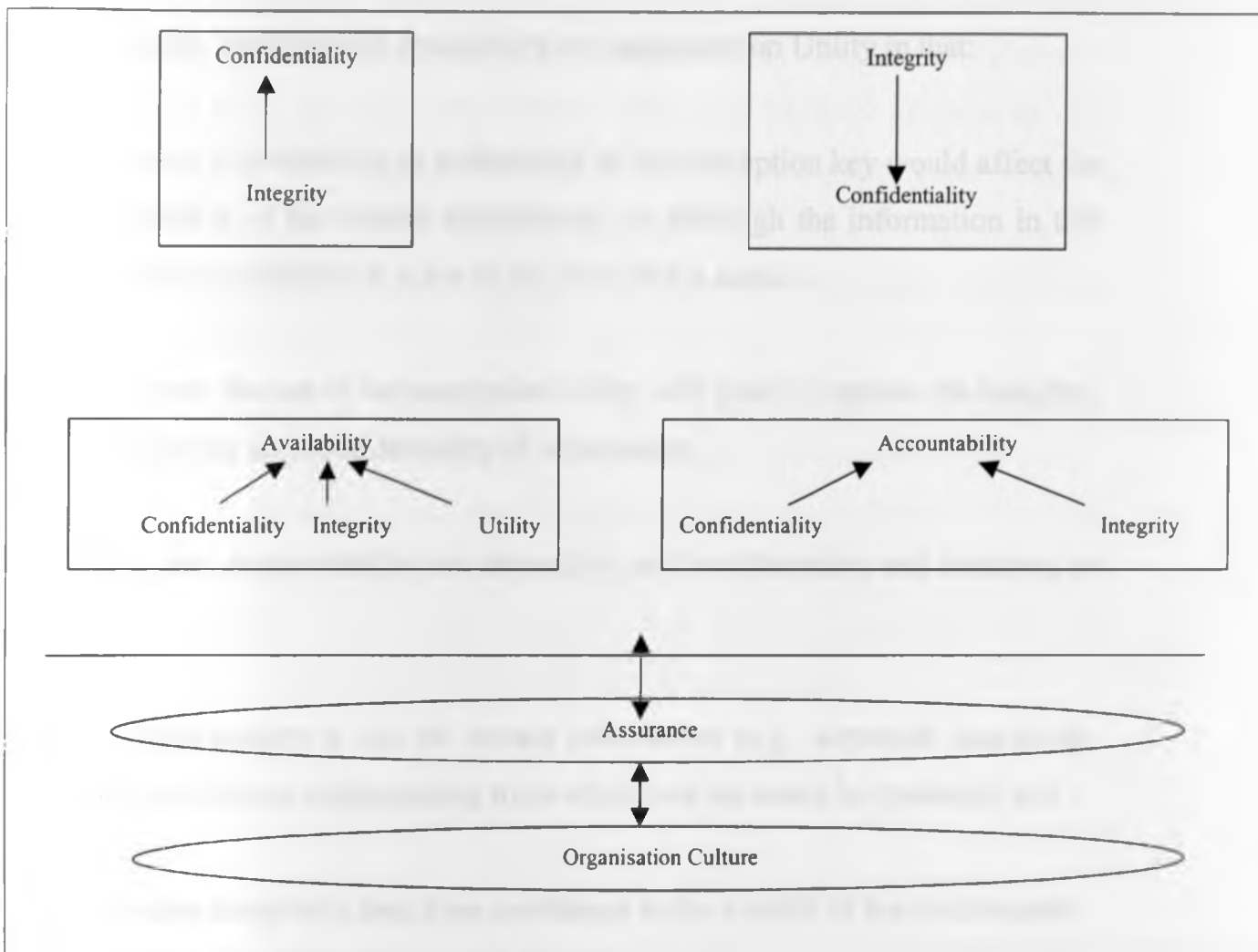
There is sufficient resistance to intentional penetration or by-pass.

7. **Culture of the Organisation**

It does not matter whether the organisation has put the best controls to mitigate any kind of threat or attack to the systems, whether intentional or unintentional, if not much has been done to cultivate proper organisation culture towards security. Recent leaking of vital organisation information to unauthorized persons/public by a staff member in a local Bank is a leaving case (Nation, 2001). This dwells much on culture of the staff. Thus there must exist a culture that supports security awareness, policies that people can refer to and understand, and specific procedures that people can follow.

In summary, unless an organisation has the overall infrastructure in place that satisfies the seven elements, then they cannot maintain any level of Computer Security.

The diagram below shows the interdependencies of the security elements. Achieving one objective without consideration of others is seldom possible.



The Figure 2.1 shows the following dependencies:

Confidentiality is dependent on Integrity, in that if the integrity of the system is lost, then there is no longer a reasonable expectation that the confidentiality mechanisms are still valid.

Integrity is dependent on Confidentiality, in that if the confidentiality of certain information is lost (e.g., the superuser password), then the integrity mechanisms are likely to be by-passed.

Confidentiality, Integrity and Availability are dependent on Utility in that:

- The loss of availability or authenticity of the encryption key would affect the availability of the owners information, i.e. although the information in this scenario is available, it is not in the form that is useful.
- However, the use of the encryption Utility will greatly improve the integrity, authenticity and confidentiality of information.

Availability and Accountability are dependent on Confidentiality and Integrity, in that:

- If confidentiality is lost for certain information (e.g., superuser password), the mechanisms implementing these objectives are easily by-passable; and
- If system integrity is lost, then confidence in the validity of the mechanisms implementing these objectives is also lost.

All of these objectives are interdependent with Assurance. However, the Security framework is perceived not to be complete until the human factor is incorporated in the whole model. This implies that Security Culture in organisations must be incorporated in the Security framework to underpin the other six elements of security that have been discussed above.

The "MOT" Security Model will form a base line for evaluating the security awareness & practices of the Banks under study. The model will use threats and vulnerabilities to assess the controls put in place by various Banks to mitigate the risk of attack(s) & threats. The table 1.0, Appendix III provides the Security area and Criteria that will assist in the assessment. The vulnerabilities that are related to the security areas outlined in the "MOT" table will be used to generate the countermeasures in those respective areas. Computer security awareness weights the organisation's preparedness towards computer crime from the viewpoint of mainframe computers to micros including the respective operational system and application software.

Only when these real threats, real risks and real solutions are acknowledged can an organization begin to effectively meet the today's IT security challenges. While no system, software or security policy is infallible, when combined to create an overall security management plan, these solutions can help organizations and IT administrators ensure that their systems and networks are secure.

Chapter 3

METHODOLOGY/STUDY DESIGN

The chapter describes the research design used for the study

3.1 Population of Study:

The population of the study comprised of all banks in Kenya that were operating normally as per the Central Bank of Kenya regulations and had implemented computer Systems to support their business.

The choice of these companies was based on the strength of their track record of conducting good Banking practices. This is supported by the Banking Survey report, 2002. It was also perceived that the chosen Banks had made substantial investments in Information Technology solutions. Note that the Banking sector in Kenya has few players and therefore do not provide a wider scope of choice/selection.

Since the population under study is small, it was decided upon that no sampling would be done and rather the entire population would be studied.

The table in Appendix I show a list of Banks that were under study.

3.2 Data Collection Method

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

The Questionnaire consists of four sections (see Appendix II)

Section A:

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

Section B:

Section B will be used to gather the information systems managers' responses towards various Computer Security countermeasures. The countermeasures are obtained from the literature review. The managers' responses will be used to determine the level of Security awareness within the organisations. The countermeasures are to be scaled on a likert -type scale.

Thus the researcher will be applying the Five Point Agreeable Scale .The scale will constitute the following different ratings:

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
5	4	3	2	1

Section C

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.

For all the respondents who are located in Nairobi, the “drop and pick later” method of administering the questionnaire was used. There was none distributed outside Nairobi.

Section D:

Section D will be used to gather information from the Information Technology /Information System Managers in relation to Computer System Security Awareness.

3.3 Data Analysis techniques:

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

Responses to section B were used to perform the risk assessment in order to determine the level of vulnerability. This analysis is based on the axiom: “As the level of in-place countermeasures increases, the level of vulnerability decreases.

Postulation:

The level of vulnerability to threats is reduced by the implementation of countermeasures. Some countermeasures have a greater propensity to offset vulnerability than others. The level of vulnerability and the relative value of each countermeasure said to reduce it can be expressed numerically.

Other axioms that will be important during this study are:

1. Axiom 2:

All countermeasures have vulnerabilities

Postulation:

A Vulnerability level of ZERO can never be obtained since all countermeasures have vulnerabilities themselves. One or more vulnerabilities can be identified for any given countermeasure.

2. Axiom 3:

An acceptable level of vulnerability can be obtained by the implementation of countermeasures.

Postulation:

There exists a mix of countermeasures that can achieve any arbitrary level of vulnerability. By adding countermeasures, the vulnerability level can be adjusted to a level commensurate with the importance, sensitivity or classification level of the information being processed.

A list of vulnerabilities that represent various security criteria is given in appendix III. These vulnerabilities are paired with specific countermeasures for the analysis process. Each countermeasure has a minimum weighting of 1 and a maximum weighting of 5. The total weight of the countermeasures determined the systems level of vulnerability.

The rating of countermeasures by the Information systems Managers determines 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 were further analysed using factor analysis to group together those vulnerabilities that are highly correlated. The results are presented through the use of descriptive statistics.

3.4 Measurement of Reliability:

Cronbach's alpha analysis was used to determine whether the variables used in the countermeasure and vulnerability analysis were reliable. Cronbach's alpha is not a statistical test-it is a coefficient of reliability (or consistency). If the average inter-item correlation is low, alpha will be low. As the average inter-item correlation increases, Cronbach's alpha increases as well. If the inter-item correlations are high, then there is evidence that the items are measuring the same underlying construct. This is really what is meant when someone says they have "high" or "good" reliability. Note that a reliability coefficient of **0.8** or higher is considered as "acceptable" in most social science applications.

Data collected in section C of the questionnaire was analysed through the use of descriptive statistics, such as mean and mode.

Data collected in Section D was analysed through Descriptive statistics such as mean and mode. An average score of 50% and above from the analysis of responses in this section is presumed acceptable in relation to the level of Computer Security Awareness achieved.

3.5 Model

There have been several models developed to address the issue of Information Security in the organisations. Parker (1998) talks of various models that he has encountered and suggests his model that he views to address the Security aspect comprehensively. Parker's model which he believes resolves the problems of existing models consists of six security elements: Availability & Utility, integrity & authenticity, and Confidentiality & possession. He bases his model on the *standards of due diligence/care*. Other models developed earlier by different Security Institutions included: -

1. CIA Model (Confidentiality, Integrity & Availability).
2. The Threat, Assets and Vulnerabilities Model
3. Clark-Wilson Integrity (CWI) Model
4. Baseline Approach (Parker)

3.5.1 Introduction to Risk Analysis

Security in any system should be commensurate with its risks. However, the process to determine which security controls are appropriate and cost effective, is quite often a complex and sometimes a subjective matter. One of the prime functions of security risk analysis is to put this process onto a more objective basis. There are a number of distinct approaches to risk analysis. However, these essentially break down into two types: quantitative and qualitative.

3.5.2.1 Quantitative Risk Analysis

This approach employs two fundamental elements; the probability of an event occurring and the likely loss should it occur.

Quantitative risk analysis makes use of a single figure produced from these elements. This is called the 'Annual Loss Expectancy (ALE)' or the 'Estimated

Annual Cost (EAC)'. This is calculated for an event by simply multiplying the potential loss by the probability.

It is thus theoretically possible to rank events in order of risk (ALE) and to make decisions based upon this.

The problems with this type of risk analysis are usually associated with the unreliability and inaccuracy of the data. Probability can rarely be precise and can, in some cases, promote complacency. In addition, controls and countermeasures often tackle a number of potential events and the events themselves are frequently interrelated.

Notwithstanding the drawbacks, a number of organisations have successfully adopted quantitative risk analysis. Some examples of the risk analysis methods that have been used before include:

1. Comprehensive Risk Analysis & Management method (CRAMM)
2. NIST annual Loss Expectancy
3. Riskpack
4. Bayesian Decision Support system(BDSS)

3.5.2.2 Qualitative Risk Analysis

This is by far the most widely used approach to risk analysis. Probability data is not required and only estimated potential loss is used[C & A Systems Security Limited, 2002].Most qualitative risk analysis methodologies make use of a number of interrelated elements:

THREATS

These are things that can go wrong or that can 'attack' the system. Examples might include fire or fraud. Threats are ever present for every system.

VULNERABILITIES

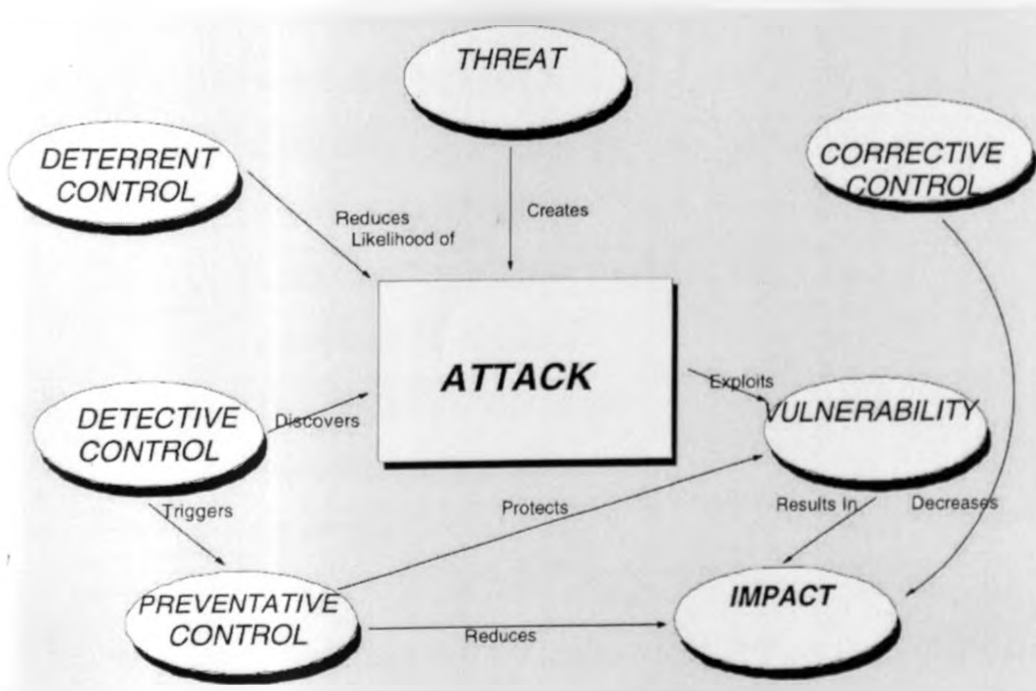
These make a system more prone to attack by a threat or make an attack more likely to have some success or impact. For example, for fire vulnerability would be the presence of inflammable materials (e.g. paper).

CONTROLS

These are the countermeasures for vulnerabilities. There are four types:

- Deterrent controls reduce the likelihood of a deliberate attack
- Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact
- Corrective controls reduce the effect of an attack
- Detective controls discover attacks and trigger preventative or corrective controls.

A simple relational model can illustrate these elements:



The knowledge base supplied with *COBRA Risk Consultant* employs this methodology and variations of it [C & A Systems Security Ltd, 2002]. [Figure 3.1]

Borrowing from the C & A Systems Security model [2002], TNC Engineering Security Standards [Murray, 1998], stoneburner [October, 2001], Swanson [Nov., 2001] and the Baseline Approach from Parker [1998], the researcher will be using a framework of Management security, operational security and Technical security (MOT) criteria to form a solid building block that will satisfy the suggested model to be used in these research. The model will constitute seven essential elements of security namely Confidentiality, Integrity, Availability, Utility, Accountability, Assurance & Culture.

Table 4.1: Summary of Programmes

Programme	Year	Author
COBRA Risk Consultant	2002	C & A Systems Security Ltd
TNC Engineering Security Standards	1998	Murray
stoneburner	October, 2001	stoneburner
Swanson	Nov., 2001	Swanson
Baseline Approach	1998	Parker
Confidentiality, Integrity, Availability, Utility, Accountability, Assurance & Culture	-	-

Chapter 4

DATA ANALYSIS & FINDINGS

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

4.1 Summary of Responses.

A total of 44 questionnaires were distributed to the respondents. Out of these, thirty questionnaires were successfully completed and returned, which represents a response rate of 68.18%. These were used as the basis for the data analysis and the findings of the study.

Table 4.1: Summary of Responses.

IT invest category	Frequency	%
Less than 50 Million	20	66.7
Less than 100 Million but more than 50 Million	3	10
Less than 150 Million but more than 100 Million	0	0
Less than 200 Million but more than 150 Million	1	3.3
Less than 250 Million but more than 200 Million	1	3.3
More than 250 Million	5	16.7

The table above indicates that the highest response rate was in the category of Kshs 0-50 Million investment with a response rate of 66.7%. The 100-150

Million category had the lowest rate of response at zero%. This shows that the majority of the Banks in Kenya have not invested immensely in IT owing to the fact that most of them are small size banks (Market Intelligence, 2002) and thus have lower volume of operations.

4.2 Analysis of IT Resources in the Organisation

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

4.2.1 First Computer Installations existence.

Most of the respondent's computer installations are more than five years old. The majority of them (36.7%) have had Computer installations for more than 5 years but less than 10 years as shown in table 4.2.1. This indicates that these Banks have been using computers for an average period of 10.8 Years and over 27 Banks rely on Computer systems for their day –to- day operations.

Table 4.2.1: Computer Installations

Category	Frequency	%
Less than 5 yrs ago	3	10
Between 5-10 Yrs	11	36.7
Between 10-15 Yrs	9	30
More than 15 Yrs	7	23.3

4.2.2 Number of Computers.

The findings indicate that there exists very low usage of mainframe computers as compared to the rest. This is shown in table 4.2.2.

Twenty-one companies (70%) indicated that they have between 1 and 10 minicomputers. However about four (13.3%) indicated that they have no minicomputers. Only 10% have more than 30 minicomputers. This can be explained from the fact that these banks require powerful computer systems to run their voluminous operations that covers a substantial branch network.

The entire respondents have desktop personal computers (PC's), with 83.3% indicating that they have more than 30 computers. This is a clear indication that Computing is taking root across the Banking spectrum, from small to large Banks in the Banking industry.

Table 4.2.2: Number of computers.

	Freq.	%
Number of computers		
a) Mainframes		
None	25	83.3
1 - 10	5	16.7
11 - 20	0	0.0
21 - 30	0	0.0
More than 30	0	0.0
b) Minicomputers		
None	4	13.3
1 - 10	23	76.7
11 - 20	0	0.0

	Freq.	%
21 – 30	0	0.0
more than 30	3	10.0
c) Desktop PC's		
None	0	0.0
0 – 10	0	25.0
11 - 20	0	0.0
21 – 30	5	16.7
More than 30	25	83.3
d) Laptop PC's		
None	15	50
0 – 10	10	33.3
11 - 20	3	10.0
21 – 30	1	3.3
More than 30	1	3.3
e) Notebooks		
None	28	93.3
0 – 10	2	6.7
11 - 20	0	0.0
21 – 30	0	0.0
More than 30	0	0.0

4.2.3 IT Director's Position.

Most of the respondent Banks (83.3%) indicated that they do not have the position of the IT Director as shown in Table 4.2.3. Most of the Banks have the position of IT/IS Manager as persons responsible for the running of the IT department.

Other titles for the person in charge of the IT department include Computer Manager, Head of IT, Shared Service Centre, Chief Manager Finance and Senior Manager IT. The information above indicates that majority of the Banks are not represented at the Board level in terms of IT.

Table 4.2.3: IT Director's Position.

	Freq.	%
IT Director position exists		
a) Yes	5	16.7
b) No	25	83.3

4.2.4 Investments in Computer Systems.

Most of the respondent banks (66.7%) have investments of less than Kshs 50 million, with 16.7% indicating that they have invested more than Kshs 250 million as shown in Table 4.2.4 below. This therefore indicates that these Banks have put a lot of resources in computer systems and hence the need to keep them secure. The average IT investment in the Kenyan Banks is Kshs 83.3 Million, a substantial investment that requires to be secured.

Table 4.2.4: Investments in Computer Systems.

IT invest category	Frequency	%
Less than 50 Million	20	66.7
Less than 100 Million but more than 50 Million	3	10
Less than 150 Million but more than 100 Million	0	0
Less than 200 Million but more than 150 Million	1	3.3
Less than 250 Million but more than 200 Million	1	3.3
More than 250 Million	5	16.7

4.2.5 Previous Year IT Budget.

The respondents IT budget for the previous year indicated that 26.7% allocated less than 1 Million, 33.3% allocated between 1 and 5 Million, 13.35% allocated between 5 and 10 Million, and 26.7% allocated more than 10 Million as shown in Table 4.2.5 below. 40% of the Banks allocated Kshs 5 Million and above. This indicates that there is continued heavy investment in computer systems by these companies.

Table 4.2.5: Previous Year IT Budget.

Category of Budget allocation	Freq.	%
Previous year IT Budget (in million Kshs)		
a) less than 1m	8	26.7
b) between 1 – 5m	10	33.3
c) between 5 – 10m	4	13.3
d) more than 10m	8	26.7

4.2.6 Internet and World Wide Web Access.

All the respondent companies indicated that they have access to the Internet as shown in Table 4.2.6 below. This is a good indication from the Banks in the sense that apart from providing the benefits of ICT (Information Communication & Technology) to their staff, they are preparing them and the infrastructure towards embracing the E-commerce and E-Banking technologies.

Table 4.2.6: Internet and World Wide Web Access.

	Freq.	%
Internet and www access exists.		
a) Yes	30	100.0
b) No	0	0.0

4.2.7 Computer Security Policy.

Most of the respondent Banks (83.3%) indicated that they have a written and formal computer security policy. The table 4.2.7 below indicates the results. This is a clear indication that the Banks are serious about informing the staff on issues related to computer Security.

Table: 4.2.7: Computer Security Policy.

	Freq	%
Written and formal computer security policy exists.		
a) Yes	25	83.3
b) No	5	16.7

4.2.8 Security Reviews.

The frequency of security reviews varies evenly with most of the Banks some preferring monthly reviews (40%), others quarterly & annually reviews (23.3%), and others bi-annually (10%) as shown in Table 4.2.8 below. However 3.3% of the respondents do not have a preferred frequency and perform reviews as and when need arises. Thus the review of Security aspects is a matter of internal policy, although it must be done at least once in a year as stipulated by the Central Bank of Kenya.

Table 4.2.8: Security Reviews.

	Freq.	%
Frequency of security reviews.		
a) Monthly	12	40
b) Quarterly	7	23.3
c) Bi-annually	3	10.0
d) Annually	7	23.3
e) Other	1	3.3

4.2.9 Security Budgets.

The responses from the Banks indicate that in average (53.3%) has annual security budget arrangements as shown in Table 4.2.9 below. However, if the investment in IT increases and we have more of the 66.7% of the Banks investing heavily in IT, i.e. over 100 Million, then the allocation of Security Budgets will also be in rise.

Table 4.2.9: Security Budgets.

	Freq.	%
Annual security budget exists.		
a) Yes	14	46.7
b) No	16	53.3

4.2.10 Computer Literacy among Management staff.

Most respondent indicated that most of their Management staff have good computer literacy levels. This is shown below in Table 4.2.10 where 66.7% of the management staff has good computer literacy levels. This is therefore an indicator of high usage rate among the Management staff.

Table 4.2.10: Computer Literacy among staff.

Category of Staff	Freq.	%
Computer literacy rating of Management Staff		
a) Management		
Excellent	4	13.3
Good	20	66.7
Fair	4	13.3
Poor	2	6.7

4.2.11 Information Systems.

Most of the respondents (76%) indicated that they have Transaction Processing Systems in use as shown in Table 4.2.11 below. A good number (70%) indicated that they have Management Information Systems in use. This is good indication in terms of usage rate by the management of the Banks. Few (6%) indicated they use Strategic Information Systems, an indication that the Chief executives in the Banks are yet to derive the full benefits of IT tools in strategic planning.

Table 4.2.11: Information Systems.

Category of different IS systems	Freq.	%
Information systems in use.		
a) Transaction Processing Systems	23	76
b) Management Information Systems	21	70
c) Decision Support Systems	9	30
d) Executive Information Systems	6	20
e) Expert Systems	0	0
f) Strategic Information Systems	2	6

4.2.12 IT Strategic Plan.

Most of the respondent (76.6%) indicates that they have a formal strategic plan for their information technology as shown in Table 4.2.12 below.

Table 4.2.12: IT Strategic Plan.

	Freq.	%
Formal strategic plan for IT exists.		
Yes	23	76.6
No	7	23.4

4.2.13 Ownership of Companies.

Most of the Banks (56.7) are locally owned, 26.7% are foreign owned and 16.6% are jointly owned as shown in Table 4.2.1 below.

Table 4.2.13: Ownership of Companies.

Category of ownership	Freq.	%
Ownership		
a) Foreign owned	8	26.7
b) Locally owned	17	56.7
c) Jointly owned	5	16.6

4.2.14 Computer Security Training.

All the respondent Banks (100%) indicated that their IT Heads have undergone Computer Security Training. See Table 4.2.14 below. This implies that the IT Heads rate the importance of IT Security highly in their priority lists/strategic plans.

Table 4.2.14: computer Security Training.

	Freq.	%
IT managers trained on computer security & are aware of information security rules & regulations		
a) Yes	30	100
b) No	0	0.00

4.2.15 Computer Security Threats.

Most of the respondent companies (96.7%) indicated that the staff is aware of security threats. This is a good indication in the sense that most of the staff in the Banking sector are in a position to recognize and report any kind of system malfunctioning. The statistics in the table 4.2.16 below show that very few (3.34%) staff in the banking sector are not aware of security threats.

Table 4.2.15: Aware of Security Threats.

	Freq.	%
Staff awareness on security threats		
a) Yes	29	96.7
b) No	1	3.3

4.2.16 Knowledge of Passwords.

All the Banks that responded to the questionnaire indicated that the staff (100%) is aware or have knowledge of passwords. See Table 4.2.17 below.

Table 4.2.16: Knowledge of Passwords.

	Freq.	%
Staff who have the knowledge of passwords		
a) Yes	30	100
b) No	0	0

4.2.17 Computer Security Awareness

Using a statistical analysis tool, the SPSS (Statistical Package for Social Sciences) for windows release 9.0, the following statistical results were derived at from the responses to questions in section D of the questionnaire that addressed the issue of Computer security Awareness in the Banking Sector. The Table 4.2.17 below shows the results.

Table 4.2.17 Computer Security Awareness.

Value (Scores)/12	Frequency	Percent	Valid Percent	Cum Percent
0.00	1	3.3	3.3	3.3
6.00	1	3.3	3.3	6.7
8.00	2	6.7	6.7	13.3
9.00	7	23.3	23.3	36.7
10.00	8	26.7	26.7	63.3
11.00	10	33.3	33.3	96.7
12.00	1	3.3	3.3	100.0
Total	30	100.0	100.0	

Mean	9.567	std err	0.400	Median	10.00
Mode	11.00	std dev	2.192	variance	4.806
Kurtosis	12.51	S E Kurt	0.833	Skewness	-3.105
S E Skew	0.427	Range	12.00	Minimum	0.00
Maximum	12.00				

From the results given above, the mean score is 9.567 indicating a 79.7% level of Computer security Awareness in the Banking Sector. Most of the respondent Banks returned a value of 11 out of 12 in terms of Security Awareness. This works out to 91.7% achievement in terms of Computer Security Awareness in the Banks. The negative Skewness (-3.105) indicates that the more extreme values are less than the mean score of 9.567. This implies that the extreme value exist within a maximum of 4 banks, which works out to 13.3% of the banks that responded.

In conclusion, the results show that most of the Banks in Kenya have achieved a high level of Computer Security Awareness.

4.3 Risk Analysis.

To perform the risk assessment, 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 9.5. Any score above this indicates that the vulnerability level is high and the system is susceptible to security violations.

4.3.1 Vulnerability Assessments.

Several countermeasures were grouped to address certain vulnerability. The scores from the respondent banks on the countermeasures indicate that the vulnerability levels range between 4.00 and 6.54, which is below the acceptable vulnerability level of 9.5. The implication, is that the respondent banks have addressed majority of the countermeasures effectively. This can be attributed to the fact that the Banking sector is a highly sensitive industry in that its trading commodity is money. The banks have to implement the best security practices to protect the computer systems in place.

All areas of vulnerability that were evaluated are shown in Table 4.3.1 below. The vulnerabilities fall within an acceptable level.

Susceptibility to loss of data or software files was ranked first with the lowest vulnerability level of 4.00 while susceptibility to unauthorized physical access was ranked the highest. The implication towards this results is that the Banks have done more investment towards ensuring that customer data is protected from loss and can be accessed whenever required. However, the least attention is given to unauthorized physical access infrastructure, at a vulnerability level of 6.54, which is above the average vulnerability of 5.268.

The Banks need to improve in this area since failure to invest properly in the physical access technologies like Electronic badge system, biometrics, CCTV, electric doors etc can lead to greater damage by unscrupulous persons towards the computer systems infrastructure.

Table 4.3: Vulnerability Levels.

Vulnerabilities	Level	Ranking
Susceptibility to authentication.	5.31	10
Susceptibility to authorisations	5.21	8
Susceptibility to Communication Technology.	5.83	14
Susceptibility to inter/intranetwork user activity.	4.72	5
Susceptibility to Hardware failure or Configuration Change	5.38	11
Susceptibility to environmental hazards	4.71	4
Susceptibility to key person dependency.	5.84	15
Susceptibility to improper handling of storage media.	4.83	6
Susceptibility to business continuity	6.34	17
Susceptibility to unauthorized physical access.	6.54	18
Susceptibility to unauthorized programmatic access.	4.84	7

Vulnerabilities	Level	Ranking
12) Susceptibility to loss of data or software files.	4	1
13) Susceptibility to unauthorized information theft or disclosure.	5.75	13
14) Susceptibility to failure and instability of electrical power sources	4.6	3
15) Susceptibility to fire	4.08	2
16) Susceptibility to user operator errors.	6.06	16
17) Susceptibility to software flaws or inadequacies.	5.5	12
18) Susceptibility to theft of system resources.	5.28	9

4.3.2 Vulnerability Assessments within Banks.

All the vulnerability levels are acceptable and range between 4.00 and 6.54. As indicated earlier, the calculated acceptable vulnerability level is 7.5. The implication of these results is that the Banks are above the danger zones in terms of Computer Security implementation, based on due diligence. This therefore means that computer systems in the Banking sector are less susceptible to security violation and other harmful activities.

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	Analysis N
a) Susceptibility to authentication.	1	4.13	0.2026	3
b) Susceptibility to authorization.	2	4.41	0.1825	3
c) Susceptibility to communication technology.	3	4.33	0.3150	3
d) Susceptibility to inter/intranetwork user activity.	4	4.51	0.2152	3
e) Susceptibility to hardware failure or configuration change.	5	4.36	0.3786	3
f) Susceptibility to environmental hazards.				
g) Susceptibility to key person dependency.	6	4.54	0.3092	3
h) Susceptibility to improper handling of storage media.	7	4.25	0.1079	3
i) Susceptibility to business continuity.	8	4.54	0.2501	3
j) Susceptibility to unauthorized physical access.	9	4.22	0.3958	3
k) Susceptibility to unauthorized programmatic access.	10	4.05	0.7814	3
l) Susceptibility to loss of data or software files.	11	4.56	0.2873	3
m) Susceptibility to unauthorized information theft or disclosure.	12	4.74	0.2730	3
	13	4.22	0.5888	3
n) Susceptibility to failure and instability of electrical power sources	14	4.80	0.1480	3
o) Susceptibility to fire				
p) Susceptibility to user operator errors.	15	4.71	0.2030	3
q) Susceptibility to software flaws or inadequacies.	16	4.13	0.4912	3
r) Susceptibility to theft of system resources.	17	4.24	0.6274	3
	18	4.34	0.4933	3

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

Table 4.4.2. Correlation Matrix.

Correlation Matrix																		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Correlati	1	.349	.732	-.951	-.928	-1.000	.791	-.384	.390	.509	-.997	-.936	.926	.767	-.902	-.727	-.434	.622
2		1.000	-.384	-.042	-.673	-.322	-.297	-.999	.999	-.629	-.418	-.656	-.031	-.333	.089	.390	.693	-.517
3			1.000	-.907	-.425	-.751	.996	.348	-.342	.959	-.679	-.445	.935	.999	-.954	-1.000	-.932	.989
4				1.000	.767	.960	-.941	.080	-.086	-.750	.925	.781	-.997	-.928	.991	.904	.691	-.834
5					1.000	.917	-.506	.701	-.705	-.152	.953	1.000	-.719	-.473	.677	.419	.067	-.286
6						1.000	-.808	.357	-.363	-.534	.995	.925	-.937	-.786	.914	.746	.460	-.645
7							1.000	.261	-.255	.929	-.743	-.525	.963	.999	-.977	-.995	-.894	.971
8								1.000	-1.000	.599	.452	.685	-.007	.297	-.051	-.355	-.665	.484
9									1.000	-.594	-.458	-.689	.014	-.291	.045	.349	.660	-.478
10										1.000	-.444	-.444	-.174	.796	.943	-.830	-.961	.991
11											1.000	.960	-.895	-.717	.868	.674	.365	-.562
12												1.000	-.734	-.493	.693	.439	.089	-.307
13													1.000	.953	-.998	-.932	-.742	.872
14														1.000	-.969	-.998	-.911	.979
15															1.000	.952	.780	-.899
16																1.000	.934	-.990
17																	1.000	-.975
18																		1.000
Sig. (1-te	1	.387	.239	.100	.122	.009	.210	.374	.372	.330	.024	.114	.123	.222	.142	.241	.357	.286
2		.387	.375	.487	.265	.396	.404	.012	.014	.283	.363	.272	.490	.392	.472	.372	.256	.327
3			.375	.139	.360	.230	.029	.387	.389	.091	.262	.353	.116	.017	.097	.002	.118	.047
4				.139	.222	.091	.109	.475	.472	.230	.124	.215	.023	.122	.042	.141	.257	.186
5					.131	.331	.253	.251	.452	.098	.007	.245	.343	.263	.363	.479	.408	
6						.200	.384	.382	.321	.033	.124	.114	.212	.133	.232	.348	.277	
7							.416	.418	.120	.233	.324	.086	.012	.068	.031	.148	.077	
8								.002	.296	.351	.260	.498	.404	.484	.385	.268	.339	
9									.298	.349	.258	.496	.406	.486	.387	.270	.341	
10										.354	.444	.207	.108	.188	.089	.027	.044	
11											.091	.147	.245	.166	.265	.381	.310	
12												.238	.336	.256	.355	.472	.401	
13													.238	.098	.019	.118	.234	.163
14														.098	.080	.019	.136	.065
15															.099	.215	.144	
16																.116	.045	
17																	.071	
18																		

The simple pair wise correlation matrix above reveals that: variable 1,2 and 9 are weakly correlated with the other variables; The following group of variables was found to be highly correlated positively;

- 1,3,7,10,13,14 and 18 were found to be highly correlated positively

- 4,5,6,11,12,15 and 16 were found to be highly correlated positively
- 9 and 17 were found to be highly correlated positively
- 16 and 17 were also found to be highly correlated positively

Communalities

	Initial	Extraction
1	1.000	1.000
2	1.000	1.000
3	1.000	1.000
4	1.000	1.000
5	1.000	1.000
6	1.000	1.000
7	1.000	1.000
8	1.000	1.000
9	1.000	1.000
10	1.000	1.000
11	1.000	1.000
12	1.000	1.000
13	1.000	1.000
14	1.000	1.000
15	1.000	1.000
16	1.000	1.000
17	1.000	1.000
18	1.000	1.000

Extraction Method: Principal Component Analysis.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	12.154	67.523	67.523	12.154	67.523	67.523	11.832	65.731	65.731
2	5.846	32.477	100.000	5.846	32.477	100.000	6.168	34.269	100.000
3	2.803E-15	1.557E-14	100.000						
4	2.189E-15	1.216E-14	100.000						
5	4.823E-16	2.679E-15	100.000						
6	3.362E-16	1.868E-15	100.000						
7	2.385E-16	1.325E-15	100.000						
8	2.140E-16	1.189E-15	100.000						
9	1.867E-16	1.037E-15	100.000						
10	1.122E-16	6.236E-16	100.000						
11	5.454E-17	3.030E-16	100.000						
12	-1.67E-17	-9.26E-17	100.000						
13	-4.11E-17	-2.28E-16	100.000						
14	-1.52E-16	-8.43E-16	100.000						
15	-2.35E-16	-1.30E-15	100.000						
16	-3.43E-16	-1.91E-15	100.000						
17	-4.20E-16	-2.34E-15	100.000						
18	-1.02E-15	-5.69E-15	100.000						

Extraction Method: Principal Component Analysis.

Since the first two factors were the only ones that had eigenvalues > 1, the final factor solution will represent 100% of the variance in the data.

To extract the principal components the initial factor matrix was orthogonally rotated to maximize the variance using varimax rotation as shown in the table below

Rotated Component Matrix^a

	Component	
	1	2
1	.764	-.646
2	-.339	-.941
3	.999	4.825E-02
4	-.926	.378
5	-.468	.884
6	-.782	.623
7	.999	-4.36E-02
8	.303	.953
9	-.296	-.955
10	.944	.329
11	-.713	.701
12	-.488	.873
13	.951	-.310
14	1.000	-5.64E-03
15	-.967	.253
16	-.998	-5.51E-02
17	-.913	-.408
18	.981	.196

Extraction Method: Principal Component Analysis.
 Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 3 iterations.

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

- Variable 1,3,7,10,13,14 and 18 load heavily on factor 1(component 1)
- Variable 5,6,8,11 and 12 load heavily on factor 2

The factors and the vulnerabilities they represent are summarized in the table below

Factor (Component)	Vulnerability
1	<ul style="list-style-type: none"> ➤ Susceptibility to authentication ➤ Susceptibility to Communication technology ➤ Susceptibility to key person dependency ➤ Susceptibility to unauthorized physical access ➤ Susceptibility to unauthorized information theft or disclosure ➤ Susceptibility theft of system resources ➤ Susceptibility to failure and instability of electrical power sources
2	<ul style="list-style-type: none"> ➤ Susceptibility to hardware failure or configuration change ➤ Susceptibility to environmental hazards ➤ Susceptibility to improper handling of storage media ➤ Susceptibility to unauthorized programmatic access ➤ Susceptibility to loss of data or software files

The mean vulnerability for factor 1 is 4.30 while that for factor 2 is 4.55. Factor 2 has a higher vulnerability level as compared to the vulnerability level of factor 1. This is however below the maximum acceptable vulnerability level of 9.5.

4.4.3: Factor Analysis Output on the “MOT” variables.

The questionnaire design addressed the three fundamental areas of security regarded in this research as “MOT” security criteria. Various countermeasures were grouped together in accordance to the best practices of Security by COBIT and BS7799 security standards, notwithstanding the importance to consider benchmarking the countermeasures on the due diligent concept advocated by the C & A Systems Security model [2002], TNC Engineering Security Standards

[Murray, 1998], stoneburner [October, 2001], Swanson [Nov., 2001] and the Baseline Approach from Parker [1998]. The countermeasures developed addressed satisfactorily areas considered as a framework of Management security, Operational security and Technical security (MOT).

Factor analysis was performed on the results of the countermeasures that were related to Management Security, Operational Security and Technical Security. The countermeasures were split into three categories and treated as variables as shown in the Table 4.4.3. For the factor analysis the actual weight of the countermeasures was used.

Factor Analysis for Management Security Countermeasures

Descriptive Statistics

	Mean	Std. Deviation	Analysis N
cm 1	4.6897	.8064	29
cm2	4.5172	.7847	29
cm3	4.4828	1.1838	29
cm4	4.3448	.8567	29
cm5	4.4138	.9826	29
cm6	4.0000	1.1339	29
cm7	3.9310	1.2798	29
cm8	4.2414	1.2146	29
cm9	4.3103	1.2565	29
cm10	4.1724	1.2555	29
cm11	4.3448	1.1734	29
cm12	4.2414	1.2999	29
cm13	4.1379	1.1565	29
cm14	4.6897	.8064	29
cm15	4.2414	1.1230	29
cm16	3.7241	1.1618	29
cm17	3.7931	1.3727	29
cm18	4.3448	1.0098	29
cm19	4.3793	1.0493	29
cm20	3.9310	1.1628	29
cm21	3.8276	1.1042	29
cm22	4.6897	.8495	29

The average mean score on the countermeasure ratings in the category of Management Security is 4.2461 rounded off to 4. This is a high indication of Management Security practice implementation and can easily be attributed to the sensitivity of data that is handled in this sector.

Component Matrix^a

	Component						
	1	2	3	4	5	6	7
cm 1	.257	.637	-.343	7.982E-02	.367	-1.67E-02	.258
cm2	.433	.726	-.121	.207	-.180	8.238E-03	-.116
cm3	.474	.162	-.167	-.557	-.327	.150	-.184
cm4	.587	-.228	-8.36E-02	.395	-.296	-.117	.145
cm5	.632	.115	.448	.396	-.220	-.334	-5.77E-02
cm6	.613	-.136	-.230	.145	-.522	.251	-.115
cm7	.258	.628	.213	-7.51E-02	-.283	.512	-.213
cm8	.526	.428	-.207	.380	.348	-1.86E-02	-8.90E-02
cm9	.288	.113	.698	.226	.312	.224	-.333
cm10	.512	-.104	.388	-.380	8.000E-02	-2.17E-02	.239
cm11	.572	-.399	-.156	-.435	.319	3.994E-02	-.107
cm12	.704	-.308	-.313	7.171E-02	.210	.110	-1.62E-02
cm13	.765	-8.49E-02	-.161	-.344	.271	5.464E-02	-7.44E-02
cm14	.486	-.507	-.347	.374	2.024E-03	.383	.104
cm15	.837	-.215	.195	8.958E-02	9.023E-02	-.151	4.487E-02
cm16	.608	.201	.153	-.235	.366	-.281	-.250
cm17	.841	-2.14E-02	-.363	-3.11E-02	8.224E-02	.141	-2.41E-02
cm18	.533	.583	-.139	4.129E-02	-1.69E-03	-.112	.456
cm19	.650	-5.72E-02	.182	-.309	-.370	-.208	.339
cm20	.541	-.371	.285	.543	7.359E-02	-9.94E-03	-3.19E-02
cm21	.715	-2.83E-02	.179	-.265	-.277	-.215	-.196
cm22	.165	7.442E-03	.634	-.120	.155	.515	.458

Extraction Method: Principal Component Analysis.

a. 7 components extracted.

Correlation Matrix

	cm 1	cm 2	cm 3	cm 4	cm 5	cm 6	cm 7	cm 8	cm 9	cm 10	cm 11	cm 12	cm 13	cm 14	cm 15	cm 16	cm 17	cm 18	cm 19	cm 20	cm 21	cm 22
Correl. cm	.000	.545	.050	.046	.033	.039	.186	.553	.007	.055	.079	.142	.162	.011	.086	.248	.263	.619	.025	.138	.018	.041
cm .545	.000	.221	.150	.407	.361	.570	.501	.157	.051	.084	.083	.194	.019	.218	.240	.335	.623	.144	.040	.313	.126	
cm .050	.221	.000	.147	.068	.372	.400	.115	.056	.254	.339	.177	.471	.050	.258	.334	.503	.244	.509	.131	.394	.023	
cm .046	.150	.147	.000	.588	.515	.010	.329	.003	.208	.162	.468	.239	.471	.467	.171	.518	.229	.366	.455	.292	.005	
cm .033	.407	.068	.588	.000	.385	.194	.452	.471	.345	.027	.199	.231	.078	.618	.354	.278	.319	.500	.588	.529	.117	
cm .039	.361	.372	.515	.385	.000	.246	.156	.000	.201	.295	.460	.300	.586	.365	.054	.551	.187	.390	.325	.513	.074	
cm .186	.570	.400	.010	.194	.246	.000	.264	.303	.097	.150	.054	.103	.125	.012	.155	.175	.323	.100	.075	.269	.308	
cm .553	.501	.115	.329	.452	.156	.264	.000	.230	.065	.090	.437	.408	.189	.322	.378	.502	.454	.038	.240	.085	.063	
cm .007	.157	.056	.003	.471	.000	.303	.230	.000	.214	.046	.062	.142	.007	.350	.379	.039	.031	.016	.431	.169	.461	
cm .055	.051	.254	.208	.345	.201	.097	.065	.214	.000	.516	.280	.377	.055	.425	.377	.208	.177	.437	.180	.486	.420	
cm .079	.084	.339	.162	.027	.295	.150	.090	.046	.516	.000	.505	.753	.381	.504	.387	.512	.017	.267	.227	.461	.040	
cm .142	.083	.177	.468	.199	.460	.054	.437	.062	.280	.505	.000	.619	.619	.570	.353	.730	.179	.323	.366	.428	.006	
cm .162	.194	.471	.239	.231	.300	.103	.408	.142	.377	.753	.619	.000	.316	.578	.508	.761	.355	.485	.246	.523	.118	
cm .011	.019	.050	.471	.078	.586	.125	.189	.007	.055	.381	.619	.316	.000	.480	.057	.553	.048	.144	.586	.098	.011	
cm .086	.218	.258	.467	.618	.365	.012	.322	.350	.425	.504	.570	.578	.480	.000	.518	.613	.333	.617	.670	.611	.194	
cm .248	.240	.334	.171	.354	.054	.155	.378	.379	.377	.387	.353	.508	.057	.518	.000	.545	.358	.323	.197	.463	.055	
cm .263	.335	.503	.518	.278	.551	.175	.502	.039	.208	.512	.730	.761	.553	.613	.545	.000	.491	.428	.349	.447	.035	
cm .619	.623	.244	.229	.319	.187	.323	.454	.031	.177	.017	.179	.355	.048	.333	.358	.491	.000	.445	.143	.279	.129	
cm .025	.144	.509	.366	.500	.390	.100	.038	.016	.437	.267	.323	.485	.144	.617	.323	.428	.445	.000	.198	.613	.257	
cm .138	.040	.131	.455	.588	.325	.075	.240	.431	.180	.227	.366	.246	.586	.670	.197	.349	.143	.198	.000	.324	.158	
cm .018	.313	.394	.292	.529	.513	.269	.085	.169	.486	.461	.428	.523	.098	.611	.463	.447	.279	.613	.324	.000	.017	
cm .041	.126	.023	.005	.117	.074	.308	.063	.461	.420	.040	.006	.118	.011	.194	.055	.035	.129	.257	.158	.017	.000	
Sig. (1 cm	.001	.398	.406	.433	.420	.167	.001	.485	.389	.341	.231	.200	.477	.329	.097	.084	.000	.449	.238	.463	.416	
cm .001		.124	.218	.014	.027	.001	.003	.207	.396	.332	.334	.157	.460	.128	.104	.038	.000	.229	.417	.049	.258	
cm .398	.124		.223	.363	.023	.016	.277	.386	.091	.036	.179	.005	.398	.088	.038	.003	.101	.002	.250	.017	.452	
cm .406	.218	.223		.000	.002	.479	.041	.493	.139	.201	.005	.106	.005	.005	.188	.002	.116	.026	.007	.062	.490	
cm .433	.014	.363	.000		.020	.157	.007	.005	.033	.445	.151	.114	.344	.000	.030	.072	.046	.003	.000	.002	.274	
cm .420	.027	.023	.002	.020		.099	.210	.500	.148	.060	.006	.057	.000	.026	.390	.001	.165	.018	.043	.002	.351	
cm .167	.001	.016	.479	.157	.099		.083	.055	.309	.219	.390	.297	.259	.475	.211	.183	.044	.303	.349	.079	.052	
cm .001	.003	.277	.041	.007	.210	.083		.115	.368	.321	.009	.014	.164	.044	.022	.003	.007	.423	.105	.330	.372	
cm .485	.207	.386	.493	.005	.500	.055	.115		.133	.406	.375	.232	.485	.031	.021	.421	.436	.467	.010	.191	.006	
cm .389	.396	.091	.139	.033	.148	.309	.368	.133		.002	.071	.022	.389	.011	.022	.140	.179	.009	.176	.004	.012	
cm .341	.332	.036	.201	.445	.060	.219	.321	.406	.002		.003	.000	.021	.003	.019	.002	.466	.081	.118	.006	.419	
cm .231	.334	.179	.005	.151	.006	.390	.009	.375	.071	.003		.000	.000	.001	.030	.000	.176	.044	.025	.010	.489	
cm .200	.157	.005	.106	.114	.057	.297	.014	.232	.022	.000	.000		.048	.001	.002	.000	.029	.004	.099	.002	.271	
cm .477	.460	.398	.005	.344	.000	.259	.164	.485	.389	.021	.000	.048		.004	.385	.001	.402	.228	.000	.306	.478	
cm .329	.128	.088	.005	.000	.026	.475	.044	.031	.011	.003	.001	.001	.004		.002	.000	.039	.000	.000	.000	.157	
cm .097	.104	.038	.188	.030	.390	.211	.022	.021	.022	.019	.030	.002	.385	.002		.001	.028	.044	.153	.006	.389	
cm .084	.038	.003	.002	.072	.001	.183	.003	.421	.140	.002	.000	.000	.001	.000	.001		.003	.010	.032	.008	.429	
cm .000	.000	.101	.116	.046	.165	.044	.007	.436	.179	.466	.176	.029	.402	.039	.028	.003		.008	.230	.071	.252	
cm .449	.229	.002	.026	.003	.018	.303	.423	.467	.009	.081	.044	.004	.228	.000	.044	.010	.008		.152	.000	.089	
cm .238	.417	.250	.007	.000	.043	.349	.105	.010	.176	.118	.025	.099	.000	.000	.153	.032	.230	.152		.043	.206	
cm .463	.049	.017	.062	.002	.002	.079	.330	.191	.004	.006	.010	.002	.306	.000	.006	.008	.071	.000	.043		.465	
cm .416	.258	.452	.490	.274	.351	.052	.372	.006	.012	.419	.489	.271	.478	.157	.389	.429	.252	.089	.206	.465		

Communalities

	Initial	Extraction
cm 1	1.000	.798
cm2	1.000	.819
cm3	1.000	.752
cm4	1.000	.682
cm5	1.000	.934
cm6	1.000	.818
cm7	1.000	.899
cm8	1.000	.777
cm9	1.000	.892
cm10	1.000	.632
cm11	1.000	.814
cm12	1.000	.750
cm13	1.000	.818
cm14	1.000	.910
cm15	1.000	.825
cm16	1.000	.763
cm17	1.000	.868
cm18	1.000	.864
cm19	1.000	.850
cm20	1.000	.813
cm21	1.000	.776
cm22	1.000	.943

Extraction Method: Principal Component Analysis.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	7.244	32.926	32.926	7.244	32.926	32.926	3.628	16.491	16.491
2	2.732	12.416	45.342	2.732	12.416	45.342	3.221	14.639	31.130
3	2.177	9.897	55.239	2.177	9.897	55.239	2.854	12.973	44.103
4	2.033	9.239	64.479	2.033	9.239	64.479	2.839	12.904	57.007
5	1.598	7.265	71.744	1.598	7.265	71.744	2.105	9.566	66.573
6	1.176	5.347	77.090	1.176	5.347	77.090	1.892	8.601	75.174
7	1.038	4.718	81.809	1.038	4.718	81.809	1.460	6.634	81.809
8	.796	3.618	85.426						
9	.681	3.097	88.523						
10	.465	2.112	90.635						
11	.443	2.015	92.650						
12	.379	1.723	94.373						
13	.306	1.390	95.763						
14	.235	1.068	96.831						
15	.228	1.036	97.867						
16	.155	.705	98.572						
17	.118	.538	99.110						
18	6.659E-02	.303	99.412						
19	5.291E-02	.241	99.653						
20	4.354E-02	.198	99.851						
21	2.595E-02	.118	99.969						
22	6.882E-03	3.128E-02	100.000						

Extraction Method: Principal Component Analysis.

Performing a principal components analysis generates the result shown in the tables above, which shows the communalities and the eigenvalues. The communalities for each variable indicates the proportion of the variance of the variable that is due to the factors, for example 94.3% of the variance on variable 14 is due to the factors. The eigenvalues express the variances extracted by the factors, for example factor 1 explains 32.93% of the total variance. Since the first seven factors were the only ones that had eigenvalues > 1, the final factor solution will represent 81.8% of the variance in the data.

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 the table below.

Rotated Component Matrix

	Component						
	1	2	3	4	5	6	7
cm 1	.122	-6.08E-02	.870	-.121	-8.12E-02	1.191E-02	2.836E-02
cm2	-7.33E-02	5.212E-02	.672	.195	.168	.508	-.186
cm3	.478	-4.71E-03	1.647E-02	.266	-.250	.623	-3.63E-02
cm4	9.076E-03	.656	.118	.470	8.236E-02	-3.74E-02	-9.01E-02
cm5	-5.95E-02	.237	.206	.701	.577	5.895E-02	-5.68E-02
cm6	.127	.680	-9.59E-03	.301	-5.92E-02	.480	-.120
cm7	-7.73E-02	-6.67E-02	.261	2.455E-03	.213	.853	.218
cm8	.196	.244	.726	-5.05E-02	.351	5.153E-02	-.153
cm9	9.319E-02	-4.13E-02	-5.53E-03	-1.25E-02	.878	.151	.297
cm10	.447	-4.15E-02	-1.56E-02	.457	9.736E-02	8.163E-03	.461
cm11	.865	.203	-.103	6.467E-02	-3.12E-02	-6.05E-02	6.984E-02
cm12	.584	.608	.169	5.874E-02	5.507E-02	-5.69E-02	-2.38E-02
cm13	.822	.222	.210	.167	4.243E-02	.118	7.576E-02
cm14	.213	.918	-1.65E-02	-.105	-2.33E-02	-5.98E-02	7.552E-02
cm15	.471	.413	.141	.517	.355	-8.32E-02	.114
cm16	.633	-.178	.306	.279	.390	3.554E-02	-7.87E-02
cm17	.609	.537	.370	.161	-7.94E-03	.209	-3.69E-02
cm18	6.797E-02	6.757E-02	.809	.378	-.123	.122	.169
cm19	.289	.143	5.586E-02	.802	-.157	.137	.236
cm20	6.835E-02	.605	-2.99E-02	.268	.565	-.208	8.050E-02
cm21	.457	.106	-2.68E-02	.649	.168	.312	-8.87E-02
cm22	6.461E-03	-3.31E-04	-2.03E-02	6.035E-02	.208	8.089E-02	.943

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

^a Rotation converged in 12 iterations.

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

- Variable 11,12,13,16,and 17 load heavily on Factor 1
- Variable 12,14 and 20 load heavily on Factor 2
- Variable 1,8 and 18 load heavily on Factor 3
- Variable 5,15,19 and 21 load heavily on Factor 4
- Variable 5,9 and 20 load heavily on Factor 5
- Variable 2,3 and 7 load heavily on Factor 6
- Variable 22 loads heavily on Factor 7

The above 7 Factors/Components extracted from Management Security criteria explain most of the variance observed in the 22 components that were used to address these category.

The factors and the countermeasures they represent are summarized below:

Factor	Countermeasures
1	<ul style="list-style-type: none"> ➤ 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 ➤ All software configuration changes follow a written procedure ➤ Has a mission or business impact analysis been conducted? ➤ Tests and examinations of key controls routinely made e.g. network scans, analysis of router & switch settings etc
2	<ul style="list-style-type: none"> ➤ A documented network configuration control procedure exists ➤ A written hardware configuration control procedure is available ➤ Resigned or terminated employees are removed from premises ➤ Computer users have had training on systems hardware and software they use
3	<ul style="list-style-type: none"> ➤ Security responsibility assigned to ensure that adequate security is provided for the mission-critical IT systems ➤ A policy on the use of personal computers or communication exists ➤ Protection against natural disaster ➤ Security alerts & security incidents are analysed & remedial actions taken
4	<ul style="list-style-type: none"> ➤ A documented procedure exists for adding & removing network users ➤ Risk assessments are performed & documented on a regular basis whenever the system, facilities, or other conditions change ➤ Management ensures that corrective actions are effectively implemented ➤ Computer users have had formal or informal computer security training
5	<ul style="list-style-type: none"> ➤ The duties of individuals are separated by a procedure or software ➤ Computer users have had training on systems hardware and software they use
6	<ul style="list-style-type: none"> ➤ There are dedicated leased lines for system communication ➤ There exists redundant communication links
7	<ul style="list-style-type: none"> ➤ Policy forbids using unauthorized or illegally obtained software

Factor Analysis for Operation Security Countermeasures

Descriptive Statistics

	Mean	Std. Deviation	Analysis N
cm23	4.6207	.6769	29
C24	4.1034	1.0805	29
C25	4.6207	.6769	29
C26	4.2759	1.2217	29
C27	4.7586	.5766	29
C28	4.6552	.8567	29
C29	3.2759	1.6013	29
C30	2.3103	1.4664	29
C31	3.9655	1.4011	29
C32	4.0345	1.3491	29
C33	4.5517	1.0885	29
C34	4.9310	.3714	29
C35	4.8276	.4682	29
C36	4.4138	1.1501	29
C37	4.2069	1.1458	29
C38	4.8966	.3099	29
C39	4.8621	.3509	29
C40	4.6207	.7752	29
C41	4.5172	1.0896	29
C42	4.6552	.8567	29
C43	4.9310	.2579	29
C44	4.0690	1.3345	29
C45	4.0000	1.4639	29
C46	3.6897	1.4418	29
C47	4.7931	.4123	29
C48	4.2414	1.1543	29
C49	4.8276	.3844	29
C50	4.4138	.8667	29
C51	4.4828	1.1838	29
C52	4.2069	1.2643	29
C53	4.4483	.9851	29
C54	4.6552	.7209	29
C55	4.7241	.6490	29

The average mean score on the countermeasure ratings in the category of Operational Security is 4.3814 rounded off to 4. This is a high indication of Operational Security practice implementation and can easily be attributed to the procedures that have been established and regulated over time by the Central Bank

of Kenya, which acts as the “eye “for the depositors funds and ensures prudent Banking practices which are supposed to secure c customer funds.

Correlation Matrix

	C23	C24	C25	C26	C27	C28	C29	C30	C31	C32	C33	C34	C35	C36	C37	C38	C39	C40	C41	C42	C43	C44	C45	C46	C47	C48
C23	1.000	0.300	0.065	0.304	0.123	0.382	0.364	0.159	0.014	0.132	0.045	0.461	0.124	0.025	0.151	0.658	0.524	0.329	0.421	0.013	0.459	0.425	0.216	0.095	0.093	0.187
C24	0.300	1.000	0.202	0.492	0.443	0.464	0.561	0.407	0.120	0.267	0.132	0.374	0.460	0.166	0.386	0.353	0.227	0.347	0.529	0.271	0.539	0.292	0.587	0.251	0.051	0.466
C25	0.065	0.202	1.000	0.433	0.306	0.444	0.430	0.159	0.325	0.102	0.197	0.108	0.124	0.066	0.033	0.317	0.373	0.533	0.276	0.049	0.459	0.267	0.324	0.204	0.603	0.213
C26	0.304	0.492	0.433	1.000	0.351	0.674	0.453	0.409	0.340	0.232	0.231	0.358	0.086	0.272	0.111	0.267	0.175	0.567	0.613	0.008	0.403	0.492	0.659	0.213	0.111	0.483
C27	0.123	0.443	0.306	0.351	1.000	0.621	0.191	0.261	0.343	0.011	0.618	0.253	0.634	0.425	0.457	0.055	0.006	0.507	0.547	0.187	0.124	0.301	0.592	0.164	0.061	0.252
C28	0.382	0.464	0.444	0.674	0.621	1.000	0.488	0.259	0.287	0.011	0.403	0.372	0.025	0.005	0.148	0.264	0.193	0.818	0.848	0.070	0.212	0.428	0.541	0.113	0.001	0.304
C29	0.364	0.561	0.430	0.453	0.191	0.488	1.000	0.419	0.091	0.276	0.053	0.273	0.018	0.045	0.221	0.491	0.451	0.490	0.591	0.202	0.394	0.342	0.198	0.038	0.252	0.484
C30	0.159	0.407	0.159	0.409	0.261	0.259	0.419	1.000	0.301	0.247	0.135	0.172	0.185	0.281	0.109	0.309	0.225	0.202	0.343	0.054	0.248	0.262	0.316	0.199	0.061	0.081
C31	0.014	0.120	0.325	0.340	0.343	0.287	0.091	0.301	1.000	0.056	0.200	0.142	0.154	0.231	0.018	0.009	0.063	0.251	0.129	0.100	0.092	0.135	0.435	0.242	0.013	0.083
C32	0.132	0.267	0.102	0.232	0.011	0.011	0.276	0.247	0.056	1.000	0.086	0.433	0.103	0.382	0.342	0.077	0.140	0.047	0.206	0.103	0.007	0.078	0.145	0.068	0.173	0.109
C33	0.045	0.132	0.197	0.231	0.618	0.403	0.053	0.135	0.200	0.086	1.000	0.079	0.404	0.410	0.507	0.037	0.074	0.215	0.202	0.172	0.114	0.145	0.336	0.409	0.211	0.089
C34	0.461	0.374	0.108	0.358	0.253	0.372	0.273	0.172	0.142	0.433	0.079	1.000	0.071	0.236	0.203	0.064	0.076	0.402	0.621	0.077	0.051	0.298	0.394	0.092	0.091	0.040
C35	0.124	0.460	0.124	0.086	0.634	0.025	0.018	0.185	0.154	0.103	0.404	0.071	1.000	0.535	0.468	0.365	0.285	0.010	0.029	0.381	0.490	0.306	0.417	0.341	0.173	0.344
C36	0.025	0.166	0.066	0.272	0.425	0.005	0.045	0.281	0.231	0.382	0.410	0.236	0.535	1.000	0.475	0.024	0.031	0.018	0.051	0.005	0.100	0.423	0.509	0.403	0.033	0.110
C37	0.151	0.386	0.033	0.111	0.457	0.148	0.221	0.109	0.018	0.342	0.507	0.203	0.468	0.475	1.000	0.062	0.074	0.092	0.111	0.003	0.050	0.154	0.298	0.192	0.013	0.177
C38	0.658	0.353	0.317	0.267	0.055	0.264	0.491	0.309	0.009	0.077	0.037	0.064	0.365	0.024	0.062	1.000	0.849	0.277	0.164	0.130	0.801	0.536	0.157	0.245	0.383	0.372
C39	0.524	0.227	0.373	0.175	0.006	0.193	0.451	0.225	0.063	0.140	0.074	0.076	0.285	0.031	0.074	0.849	1.000	0.326	0.100	0.074	0.680	0.402	0.070	0.124	0.533	0.261
C40	0.329	0.347	0.533	0.567	0.507	0.818	0.490	0.202	0.251	0.047	0.215	0.402	0.010	0.018	0.092	0.277	0.326	1.000	0.748	0.096	0.222	0.579	0.566	0.178	0.301	0.306
C41	0.421	0.529	0.276	0.613	0.547	0.848	0.591	0.343	0.129	0.206	0.202	0.621	0.029	0.051	0.111	0.164	0.100	0.748	1.000	0.045	0.131	0.417	0.537	0.038	0.071	0.323
C42	0.013	0.271	0.049	0.008	0.187	0.070	0.202	0.054	0.100	0.103	0.172	0.077	0.381	0.005	0.003	0.130	0.074	0.096	0.045	1.000	0.212	0.010	0.085	0.148	0.001	0.737
C43	0.459	0.539	0.459	0.403	0.124	0.212	0.394	0.248	0.092	0.007	0.114	0.051	0.490	0.100	0.050	0.801	0.680	0.222	0.131	0.212	1.000	0.326	0.284	0.132	0.533	0.418
C44	0.425	0.292	0.267	0.492	0.301	0.428	0.342	0.262	0.135	0.078	0.145	0.298	0.306	0.423	0.154	0.536	0.402	0.579	0.417	0.010	0.326	1.000	0.658	0.568	0.351	0.360
C45	0.216	0.587	0.324	0.659	0.592	0.541	0.198	0.316	0.435	0.145	0.336	0.394	0.417	0.509	0.298	0.157	0.070	0.566	0.537	0.085	0.284	0.658	1.000	0.541	0.113	0.275
C46	0.095	0.251	0.204	0.213	0.164	0.113	0.038	0.199	0.242	0.068	0.409	0.092	0.341	0.403	0.192	0.245	0.124	0.178	0.038	0.148	0.132	0.568	0.541	1.000	0.123	0.175
C47	0.093	0.050	0.605	0.117	0.067	0.007	0.252	0.067	0.013	0.179	0.214	0.097	0.179	0.036	0.018	0.386	0.536	0.304	0.071	0.007	0.533	0.351	0.118	0.128	0.001	0.184
C48	0.187	0.466	0.213	0.483	0.252	0.304	0.484	0.081	0.083	0.109	0.089	0.040	0.344	0.110	0.177	0.372	0.261	0.306	0.323	0.737	0.418	0.360	0.275	0.175	0.181	0.000
C49	0.426	0.302	0.426	0.409	0.289	0.572	0.544	0.288	0.121	0.195	0.150	0.086	0.226	0.086	0.165	0.744	0.612	0.492	0.391	0.030	0.596	0.511	0.254	0.158	0.443	0.419
C50	0.149	0.085	0.277	0.044	0.222	0.186	0.146	0.148	0.164	0.104	0.288	0.130	0.082	0.214	0.305	0.032	0.077	0.136	0.083	0.103	0.132	0.098	0.113	0.065	0.543	0.075
C51	0.281	0.323	0.148	0.226	0.124	0.135	0.248	0.028	0.054	0.033	0.131	0.078	0.413	0.058	0.029	0.530	0.424	0.362	0.104	0.557	0.464	0.611	0.247	0.363	0.353	0.722
C52	0.137	0.428	0.178	0.378	0.071	0.068	0.182	0.080	0.206	0.163	0.268	0.336	0.243	0.111	0.117	0.148	0.147	0.229	0.127	0.398	0.264	0.436	0.347	0.311	0.291	0.478
C53	0.057	0.156	0.218	0.047	0.009	0.107	0.190	0.321	0.063	0.337	0.094	0.108	0.174	0.303	0.548	0.157	0.185	0.097	0.157	0.107	0.015	0.220	0.050	0.101	0.021	0.099
C54	0.308	0.506	0.454	0.680	0.566	0.841	0.426	0.274	0.235	0.160	0.206	0.442	0.029	0.006	0.176	0.154	0.229	0.780	0.781	0.026	0.252	0.285	0.575	0.004	0.112	0.318
C55	0.322	0.450	0.648	0.685	0.484	0.722	0.488	0.243	0.107	0.093	0.122	0.511	0.073	0.063	0.079	0.208	0.141	0.636	0.714	0.049	0.309	0.476	0.564	0.134	0.313	0.235

a) Determinant = .000

b) This matrix is not positive definite.

Covariance Matrix^a

a. This matrix is not positive definite.

Communalities

	Initial	Extraction
cm23	1.000	.823
C24	1.000	.722
C25	1.000	.828
C26	1.000	.737
C27	1.000	.870
C28	1.000	.950
C29	1.000	.827
C30	1.000	.708
C31	1.000	.771
C32	1.000	.723
C33	1.000	.848
C34	1.000	.908
C35	1.000	.920
C36	1.000	.732
C37	1.000	.821
C38	1.000	.968
C39	1.000	.824
C40	1.000	.846
C41	1.000	.905
C42	1.000	.902
C43	1.000	.905
C44	1.000	.901
C45	1.000	.857
C46	1.000	.729
C47	1.000	.927
C48	1.000	.893
C49	1.000	.822
C50	1.000	.699
C51	1.000	.940
C52	1.000	.797
C53	1.000	.786
C54	1.000	.835
C55	1.000	.841

Extraction Method: Principal Component Analysis.

The communalities for each variable indicates the proportion of the variance of the variable that is due to the factors, for example 82.3% of the variance in variable 23 is due to the factors.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	9.642	29.218	29.218	9.642	29.218	29.218	6.715	20.349	20.349
2	4.048	12.268	41.486	4.048	12.268	41.486	4.207	12.747	33.096
3	3.324	10.074	51.560	3.324	10.074	51.560	3.157	9.568	42.664
4	2.532	7.672	59.232	2.532	7.672	59.232	3.005	9.106	51.770
5	2.182	6.613	65.845	2.182	6.613	65.845	2.443	7.404	59.174
6	1.895	5.742	71.587	1.895	5.742	71.587	2.308	6.994	66.168
7	1.552	4.702	76.288	1.552	4.702	76.288	2.023	6.130	72.298
8	1.278	3.873	80.162	1.278	3.873	80.162	1.984	6.014	78.312
9	1.111	3.366	83.528	1.111	3.366	83.528	1.721	5.215	83.527
10	.925	2.804	86.332						
11	.813	2.463	88.795						
12	.774	2.346	91.141						
13	.567	1.718	92.859						
14	.461	1.396	94.255						
15	.389	1.180	95.435						
16	.358	1.086	96.521						
17	.325	.985	97.507						
18	.246	.747	98.253						
19	.210	.638	98.891						
20	.140	.424	99.315						
21	8.259E-02	.250	99.565						
22	5.743E-02	.174	99.739						
23	3.703E-02	.112	99.851						
24	2.579E-02	7.816E-02	99.930						
25	1.765E-02	5.348E-02	99.983						
26	5.600E-03	1.697E-02	100.000						
27	6.186E-16	1.875E-15	100.000						
28	4.951E-16	1.500E-15	100.000						
29	3.435E-16	1.041E-15	100.000						
30	1.589E-16	4.814E-16	100.000						
31	4.752E-17	1.440E-16	100.000						
32	-1.54E-16	-4.66E-16	100.000						
33	-4.88E-16	-1.48E-15	100.000						

Extraction Method: Principal Component Analysis.

Performing a principal components analysis generates the result shown in the tables above, which shows the communalities and the eigenvalues. The communalities for each variable indicate the proportion of the variance of the variable that is due to

the factors. The eigenvalues express the variances extracted by the factors, for example factor 1 explains 29.218% of the total variance

Since the first nine factors were the only ones that had eigenvalues > 1 , the final factor solution will represent 83.5% of the variance in the data.

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 the table below.

	1	2	3	4	5	6	7	8	9
1	0.85	0.12	0.05	0.02	0.01	0.01	0.01	0.01	0.01
2	0.15	0.78	0.08	0.03	0.02	0.01	0.01	0.01	0.01
3	0.05	0.10	0.82	0.05	0.03	0.02	0.01	0.01	0.01
4	0.02	0.03	0.05	0.85	0.05	0.03	0.02	0.01	0.01
5	0.01	0.02	0.03	0.05	0.82	0.05	0.03	0.02	0.01
6	0.01	0.01	0.02	0.03	0.05	0.85	0.05	0.03	0.02
7	0.01	0.01	0.01	0.02	0.03	0.05	0.82	0.05	0.03
8	0.01	0.01	0.01	0.01	0.02	0.03	0.05	0.85	0.05
9	0.01	0.01	0.01	0.01	0.01	0.02	0.03	0.05	0.82

Rotated Component Matrix

	Component								
	1	2	3	4	5	6	7	8	9
cm23	.313	.700	-2.40E-02	-3.92E-02	.122	-.271	-6.13E-02	.346	-.145
C24	.437	.268	.325	.396	-4.27E-02	-2.94E-02	.237	.305	.211
C25	.482	.226	9.500E-02	-1.94E-02	-6.55E-03	.643	-.130	-.188	.264
C26	.691	.135	4.124E-02	.158	.199	5.372E-02	.142	.162	.355
C27	.561	-4.13E-02	.695	.142	1.508E-02	-9.03E-02	-7.91E-02	-.103	.160
C28	.931	.164	8.565E-02	4.519E-03	7.800E-02	-.131	-1.68E-02	-.140	7.312E-02
C29	.559	.374	-5.55E-02	.257	-9.74E-02	.183	.488	-3.23E-03	-.156
C30	.263	.194	2.830E-02	-1.56E-02	2.439E-02	-4.44E-03	.609	4.132E-02	.476
C31	.172	-2.16E-02	9.979E-02	-9.07E-02	.174	-3.97E-02	-1.09E-02	-.125	.822
C32	.116	-.147	8.710E-02	7.941E-02	-8.19E-02	-8.43E-02	.580	.567	-4.86E-02
C33	.297	-.138	.660	-.149	.171	-.191	5.616E-02	-.463	2.124E-02
C34	.509	-7.01E-02	3.400E-02	-5.02E-02	.164	-.175	2.786E-02	.731	-.217
C35	-.111	.301	.794	.354	.127	5.100E-02	-8.00E-02	-7.57E-03	.189
C36	-4.62E-02	-4.38E-02	.658	-3.88E-02	.372	-5.53E-02	.251	.238	.181
C37	9.493E-02	4.523E-02	.757	4.906E-03	5.075E-02	-7.82E-02	.395	9.308E-02	-.251
C38	.102	.938	3.758E-03	.161	.175	4.224E-02	.113	-7.59E-02	1.633E-02
C39	7.585E-02	.867	-6.08E-03	5.995E-02	9.234E-02	.195	8.954E-02	-9.19E-02	-2.80E-03
C40	.837	.149	-1.61E-02	2.822E-02	.285	.191	-1.45E-02	-5.91E-02	-3.25E-02
C41	.918	6.686E-02	6.796E-04	8.881E-02	2.303E-02	-.150	8.110E-02	.142	-1.97E-02
C42	-7.42E-02	2.840E-02	7.610E-02	.923	-.185	-2.58E-02	-3.93E-02	1.619E-02	-3.69E-02
C43	.104	.793	.160	.259	-6.38E-02	.288	-3.67E-02	.145	.253
C44	.359	.335	.102	.115	.771	.123	.136	8.513E-02	-2.23E-02
C45	.534	2.546E-02	.401	4.144E-02	.472	3.513E-02	5.839E-03	.226	.365
C46	2.997E-02	7.654E-02	.258	1.071E-02	.784	1.791E-02	2.530E-02	-5.71E-02	.191
C47	2.544E-02	.399	5.023E-02	1.172E-02	.158	.847	-.113	3.142E-02	-8.66E-02
C48	.298	.187	9.837E-02	.851	.127	5.028E-02	6.412E-02	-9.00E-02	-7.67E-02
C49	.421	.684	8.221E-02	7.320E-02	.123	.115	.126	-.348	-1.53E-02
C50	-4.95E-02	-5.53E-02	-.295	.128	2.274E-02	.756	.108	-4.46E-02	-6.53E-02
C51	4.978E-02	.349	-1.70E-02	.718	.507	.137	-9.71E-02	4.512E-02	-.110
C52	8.450E-02	2.335E-02	-3.47E-02	.572	.419	.226	6.810E-04	.448	.182
C53	-.220	.103	.239	-9.21E-02	.163	-2.63E-02	.794	-4.03E-02	-3.99E-02
C54	.884	.114	.110	2.706E-02	-8.61E-02	2.517E-02	-1.16E-02	8.440E-02	.116
C55	.802	.106	9.692E-02	-4.10E-03	7.375E-02	.308	-9.63E-02	.252	7.017E-02

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 10 iterations.

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

- Variable 26,27,28,29,34,40,40,41,54 and 55 load heavily on Factor 1 (cm23)
- Variable 23,38,39,43 and 49 load heavily on factor 2 (cm24)
- Variable 27,33,35,36 and 37 load heavily on factor 3 (cm25)
- Variable 42,48,51 and 52 load heavily on factor 4 (cm26)
- Variable 44 and 46 load heavily on factor 5 (cm27)

- Variable 26 and 50 load heavily on factor 6 (cm28)
- Variable 30,32 and 53 load heavily on factor 7 (cm29)
- Variable 34 load heavily on factor 8 (cm30)

The factors and the countermeasures they represent are summarized below:

Factor	Countermeasures
1	<ul style="list-style-type: none"> ➤ There exist documented job descriptions that accurately reflect assigned duties & responsibilities & that segregate duties ➤ The room which houses the computers has restricted access ➤ Communication access points are kept locked ➤ Log-in attempts are limited to a specific number for the network users ➤ Critical data is stored in fireproof safes ➤ Fire detection equipment are installed in the computer room ➤ Locks are installed for doors to the computer terminal space and network controllers ➤ Access to tables defining network options, resources and operator profiles is restricted
2	<ul style="list-style-type: none"> ➤ System preventative maintenance is done on a regular basis ➤ A backup power source e.g. battery or generator, is installed ➤ Access to the computer fuse or circuit breaker panel is controlled ➤ There is a disaster recovery site ➤ You store copies of back-up media for the computer.
3	<ul style="list-style-type: none"> ➤ Data that are critical to the mission is stored off site ➤ Vendor (logon) identification are removed from the network server ➤ Computer screens are created away from passersby ➤ A uninterruptible Power Supply (UPS) is installed for your system
4	<ul style="list-style-type: none"> ➤ Fire extinguishing systems are installed in the computer room ➤ A procedure for the management of magnetic media exists ➤ Access scripts with embedded passwords are prohibited ➤ All software configuration changes follow a written procedure
5	<ul style="list-style-type: none"> ➤ Individuals who are authorised to bypass significant technical & operational controls are screened prior to access & periodically after ➤ The Duties of individuals are separated by a procedure or software
6	<ul style="list-style-type: none"> ➤ You remove data storage media from the system when not in use
7	<ul style="list-style-type: none"> ➤ Safeguard computing facility ➤ Partial backups are done at least once a day and full backups of network files are done at least once a week ➤ Is information or media purged, overwritten or destroyed when disposed or used elsewhere?
8	<ul style="list-style-type: none"> ➤ Log -in attempts are limited to a specific number for the network users

Factor Analysis for Technical security Countermeasures

Descriptive Statistics

	Mean	Std. Deviation	Analysis N
CM56	4.7241	.6490	29
CM57	4.6552	.8140	29
CM58	4.7586	.7863	29
CM59	4.8621	.3509	29
CM60	4.3448	1.0446	29
CM61	4.3793	1.0493	29
CM62	4.6897	.5414	29
CM63	4.7931	.4913	29
CM64	4.9310	.2579	29
CM65	4.5862	.8667	29
CM66	3.7931	1.2923	29
CM67	4.5517	.8696	29
CM68	4.0690	1.3074	29
CM69	4.5862	.8667	29
CM70	4.5172	.8710	29

The average mean score on the countermeasure ratings in the category of Operational Security is 4.2205 rounded off to 4. This is a high indication of Technical Security practice implementation and can easily be attributed to the sensitive data that is handled in this sector.

Correlation Matrix

	CM56	CM57	CM58	CM59	CM60	CM61	CM62	CM63	CM64	CM65	CM66	CM67	CM68	CM69	CM70
Correla CM	.000	.625	.705	.141	.093	.107	.561	.039	.309	.044	.228	.153	.107	.298	.009
CM	.625	1.000	.926	.203	.187	.159	.154	.172	.223	-.007	-.002	.177	-.044	-.007	-.042
CM	.705	.926	1.000	.134	.061	.072	.069	.051	.267	.005	-.016	.202	-.087	.005	-.020
CM	.141	.203	.134	1.000	.329	.244	.331	.450	.680	.510	.250	.609	.177	.510	.475
CM	.093	.187	.061	.329	1.000	.756	.259	.353	.489	.045	.240	.019	.087	.045	.072
CM	.107	.159	.072	.244	.756	1.000	.277	.158	.496	-.018	.376	-.042	.293	-.018	-.027
CM	.561	.154	.069	.331	.259	.277	1.000	.153	.353	.325	.569	.225	.385	.706	.277
CM	.039	.172	.051	.450	.353	.158	.153	1.000	.447	.379	-.014	.360	-.088	.043	.009
CM	.309	.223	.267	.680	.489	.496	.353	.447	1.000	.187	.277	.176	.015	.187	.164
CM	.044	-.007	.005	.510	.045	-.018	.325	.379	.187	1.000	.399	.882	.499	.762	.719
CM	.228	-.002	-.016	.250	.240	.376	.569	-.014	.277	.399	1.000	.264	.685	.590	.352
CM	.153	.177	.202	.609	.019	-.042	.225	.360	.176	.882	.264	1.000	.405	.693	.694
CM	.107	-.044	-.087	.177	.087	.293	.385	-.088	.015	.499	.685	.405	1.000	.593	.438
CM	.298	-.007	.005	.510	.045	-.018	.706	.043	.187	.762	.590	.693	.593	1.000	.719
CM	.009	-.042	-.020	.475	.072	-.027	.277	.009	.164	.719	.352	.694	.438	.719	1.000
Sig. (1- CM		.000	.000	.233	.316	.291	.001	.421	.051	.411	.118	.214	.290	.058	.482
CM	.000		.000	.146	.166	.206	.213	.186	.123	.486	.495	.179	.410	.486	.415
CM	.000	.000		.244	.376	.356	.360	.396	.081	.489	.468	.147	.326	.489	.459
CM	.233	.146	.244		.041	.101	.040	.007	.000	.002	.096	.000	.179	.002	.005
CM	.316	.166	.376	.041		.000	.087	.030	.004	.409	.105	.461	.328	.409	.356
CM	.291	.206	.356	.101	.000		.073	.207	.003	.464	.022	.415	.062	.464	.445
CM	.001	.213	.360	.040	.087	.073		.214	.030	.042	.001	.120	.020	.000	.073
CM	.421	.186	.396	.007	.030	.207	.214		.008	.021	.472	.027	.325	.412	.482
CM	.051	.123	.081	.000	.004	.003	.030	.008		.165	.073	.181	.470	.165	.197
CM	.411	.486	.489	.002	.409	.464	.042	.021	.165		.016	.000	.003	.000	.000
CM	.118	.495	.468	.096	.105	.022	.001	.472	.073	.016		.083	.000	.000	.030
CM	.214	.179	.147	.000	.461	.415	.120	.027	.181	.000	.083		.015	.000	.000
CM	.290	.410	.326	.179	.328	.062	.020	.325	.470	.003	.000	.015		.000	.009
CM	.058	.486	.489	.002	.409	.464	.000	.412	.165	.000	.000	.000	.000		.000
CM	.482	.415	.459	.005	.356	.445	.073	.482	.197	.000	.030	.000	.009	.000	

Communalities

	Initial	Extraction
CM56	1.000	.827
CM57	1.000	.857
CM58	1.000	.918
CM59	1.000	.752
CM60	1.000	.749
CM61	1.000	.803
CM62	1.000	.646
CM63	1.000	.645
CM64	1.000	.709
CM65	1.000	.880
CM66	1.000	.764
CM67	1.000	.884
CM68	1.000	.701
CM69	1.000	.906
CM70	1.000	.697

Extraction Method: Principal Component Analysis.

The communalities for each variable indicates the proportion of the variance of the variable that is due to the factors, for example 82.7% of the variance in variable 56 is due to the factors.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	5.112	34.080	34.080	5.112	34.080	34.080	3.616	24.105	24.105
2	2.824	18.824	52.903	2.824	18.824	52.903	2.779	18.527	42.632
3	2.049	13.659	66.562	2.049	13.659	66.562	2.702	18.013	60.645
4	1.755	11.699	78.261	1.755	11.699	78.261	2.642	17.615	78.260
5	.909	6.060	84.321						
6	.693	4.617	88.938						
7	.511	3.409	92.347						
8	.300	2.001	94.348						
9	.268	1.784	96.133						
10	.202	1.346	97.479						
11	.176	1.171	98.649						
12	.123	.817	99.466						
13	5.024E-02	.335	99.801						
14	2.646E-02	.176	99.978						
15	3.368E-03	2.245E-02	100.000						

Extraction Method: Principal Component Analysis.

Since the first four factors were the only ones that had eigenvalues > 1 , the final factor solution will only represent 78.2% of the variance in the data.

Rotated Component Matrix^a

	Component			
	1	2	3	4
CM56	6.738E-03	.320	5.813E-02	.849
CM57	3.434E-02	-7.71E-02	.154	.909
CM58	4.419E-02	-8.61E-02	4.176E-02	.952
CM59	.673	3.017E-02	.532	.123
CM60	-6.82E-02	.165	.846	1.480E-02
CM61	-.221	.362	.789	1.287E-02
CM62	.202	.687	.251	.265
CM63	.435	-.339	.582	5.023E-02
CM64	.228	4.912E-02	.773	.240
CM65	.898	.265	4.189E-02	-4.54E-02
CM66	.175	.830	.212	-1.88E-04
CM67	.921	.124	1.960E-02	.143
CM68	.287	.780	-8.13E-03	-9.50E-02
CM69	.697	.642	-4.64E-02	7.420E-02
CM70	.756	.344	-4.35E-02	-7.54E-02

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 9 iterations.

To extract the principal components the initial factor matrix was orthogonally rotated to maximize the variance using varimax rotation as shown in the table above.

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

- Variable 59,65,67,69 & 70 load heavily on factor 1(cm56)
- Variable 62,66 and 68 load heavily on factor2 (cm57)
- Variable 60,61,63 and 64 load heavily on factor 3(cm58)
- Variable 56,57 and 58 load heavily on factor 4(cm59)

The factors and countermeasures they represent are summarized in the table below

Factor	Countermeasures
1	<ul style="list-style-type: none"> ➤ A written procedure exists for acceptance testing of software ➤ Access to files is restricted to logical view ➤ You have deployed firewall & IDS ➤ Alternative system communication paths are available ➤ Sensitive data is encrypted before transmission
2	<ul style="list-style-type: none"> ➤ Vendors do not retain their account on the system ➤ Access to tables defining network options, resources and operator profiles is restricted ➤ Access to online audit logs is strictly controlled
3	<ul style="list-style-type: none"> ➤ New software is validated in accordance with an established policy ➤ Sensitive data is encrypted before transmission ➤ Are passwords unique & difficult to guess ➤ Are inactive user identifications disabled after a specified period of time
4	<ul style="list-style-type: none"> ➤ Users have a pre-authorized set of system privileges and commands ➤ Log –in to software applications requires a unique identifier ➤ You virus scan all software before loading into the system

Management, Operational and Technical security analysis in terms of the actual score against the expected score.

Having performed factor analysis on the countermeasures in the three categories, there seems to be a clear indication that all the respondents scored an acceptable mean score of 4 out of the expected 5 for each variable, which is a high score. However, a general analysis in terms of actual versus expected scores reveal otherwise as outlined further.

Considering the three categories outlined earlier and the scores from the respondents to the respective questions, the Management Security area had a score of 84.42%, the Operational Security area had a score of 87.341% while the Technical Security area had a score of 90.67%. This has an overall indication score of 87% of the expected score.

We can deduce that the area of Management security receives less emphasis as compared to the other two areas. There is greater emphasis on both the area of operational security and Technical security. This is a clear indication of the inheritance of the tight operational procedures in terms of operations within the Bank that have been developed over a period of time. The Technical Security has the highest attention and this can be attributed to the fact that the Banking sector trades in a commodity that is highly sensitive and thus requires complete safeguards from any kind of risk. This has been enhanced by the regulatory/supervisory Bank, the Central Bank of Kenya which ensures among other things that Information systems audit is carried out at least once in a year by external auditors. The Management Security area has a high score in terms of achievement and this is as a result of technology setting pace in most of the businesses today, hence the need to understand the technology in use, the risks involved and how to mitigate those risks.

Area	Score	Weight
Operational Security	4.8	33
Technical Security	5.2	33
Management Security	4.5	34

4.5. Perceived Security Risk Related Problems.

Table 4.5: Perceived Security Risk Related Problems

Sector	Industrial & Allied	
	Ranking	
Security Problem	Mean	Mode
a) Personnel and other people problems	5.3	6
b) Hardware failure.	4.6	5
c) Software failure.	5.5	8
d) Communication systems failure.	6.0	10
e) Physical building facilities.	3.1	1
f) Practices and procedures.	3.9	1
g) Laws and regulations.	3.1	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 5.1 and 6.00 for the security related problems as shown in Table 4.6.1 above.

However communication systems failure have a modal score of 10 indicating that many of the respondents consider these problem to pose the highest risk to their computer systems. Across the Banks, the problem of laws and regulations, practices & procedures and physical building facilities are considered to be of least risk with a modal Score of 1.

Chapter 5

CONCLUSION

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 Banks have been using Computers for an average period of 11 years in this country. Seven Banks among the respondents (23.3 %) have had their computer installations for well over 15 years.

The study shows that there exists very low usage of mainframe computers as compared to the rest. A figure of 16.7%, which represents five Banks, is quite low. This can be attributed to the fact that these Banks had their first installations over 15 years ago. Nevertheless, this is an indication that most of the Banks are installing the Risk based computing technology, which is the state of art technology, to run their business. Twenty-one Banks (70%) indicated that they have between 1 and 10 minicomputers. This shows that minicomputers have replaced the mainframes in terms of major back office operations in these institutions. Only 10% of the Banks, which formulate the major Banks in Kenya, have more than 30 minicomputers. This can be attributed to the fact that these banks handle voluminous transactions over a wide branch network.

The entire respondents have desktop personal computers (PCs), with 83.3% indicating that they have more than 30 computers. This signals that computing or

process automation is taking root across the Banking spectrum, from small to large Banks in the Banking Industry.

In terms of investments in computer systems 66.7% of the Banks have investments of less than Kshs 50 Million, with 16.7% indicating that they have invested more than Kshs. 250 Million. The average IT investment in the Kenyan Banks is Kshs. 83.3 Million. 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 33.3% of the Banks have made heavy investments ranging from Kshs 50 Million to over Kshs. 250 Million in information technology, it is surprising that they do not have an information technology professional at the executive board level since 83.3% of the respondent companies indicated that they do not have the post of IT Director.

All the respondent Banks have access to the Internet. This implies that there is already in place technology to enrich them with knowledge on different issues in general and issues pertaining their work. It also indicates a positive move within the Banking sector towards reading itself for e-commerce and e-banking. However, to the contrary, the Banks's corporate networks are now more exposed to computer viruses and other malicious codes that are spread through the Internet especially through electronic mail.

In terms of policy formulation most of the respondents (83.3%) indicated that they had a written and formal computer security policy. This adequately did also address hardware and software acquisition (88.2%).

The frequency of security reviews varies evenly with most of the Banks some preferring monthly reviews (40%), others quarterly reviews and others annually (23.3) and others bi-annually(10%).However,3.3% of the respondents do not have a preferred frequency and perform reviews as and when need arises.. This means that 96.7% have a defined frequency for reviewing the security posture of their organizations.

Slightly over half (53.3%) of the Banks indicated that they do not have annual security budgets, this is close to the percentage (60%) of those companies that have IT budgets of KShs 5 million and below. In similar relative observation, it is shown that those Banks that have annual security budget (46.7%) have an IT budget of 10 Million and above (40%). 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 and vice-versa.

Most of the information systems are used mainly for Transaction Process Systems (76%) and for Management Information Systems (70%). The use of Decision Support Systems (30%), Executive Information Systems (20%), Expert Systems (0%), and Strategic Information Systems (6%) is very low, an indication of limited use of specialist information systems is by the management in these institutions.

Most respondent indicated that most of the management staff has good computer literacy levels (66.7%). This is an indicator of high usage rate among the management staff.

Most of the respondent (76.6%)indicate that they have a formal strategic plan for their information technology.56.7% of the banks are locally owned, 26.7% foreign while 16.6% are jointly owned.

All the respondent Banks indicated that the IT heads have undergone Computer Security Training. This implies that the IT heads rate the importance of IT Security highly in their priority lists/strategic plans.

Most of the information systems are used mainly for Transaction Process Systems (76%) and for Management Information Systems (70%). The use of Decision Support Systems (30%), Executive Information Systems (20%), Expert Systems (0%), and Strategic Information Systems (6%) is very low, an indication of limited use of specialist information systems is by the management in these institutions.

Most of the respondent companies (96.7%) indicated that the staff is aware of computer security threats. This is a good indication in the sense that most of the staff in the Banking sector are in a position to recognize and report any kind of system malfunctioning.

The results derived at from the responses to questions in section D of the questionnaire that addressed the issue of Computer security Awareness in the Banking Sector indicate that an average of 79.7% mark has been realized within the Banks in terms of Security Awareness

In conclusion, the results show that most of the Banks in Kenya have achieved a high level of Computer Security Awareness.

5.2 Conclusion on Vulnerability assessment and Factor Analysis.

The findings of this study indicates that the Banking sector on average have secure systems since the vulnerability levels to the susceptibilities considered in this study are all acceptable.

Considering the vulnerability levels, the highest susceptibility area is unauthorized physical access to computer systems, which implies that very few of the information systems/technology managers place little emphasis on securing computer rooms and communication access points such as the use of closed Circuit Television Monitoring, Sensors and Alarms, Biometrics access control and Electronic Badge System. This is a loophole that can lead to thefts of computers and computer parts, thus hampering the operations of the banks and by extension affecting the confidentiality, Integrity, Availability, Utility and assurance of the customer Data. .

The other high vulnerability areas include: susceptibility to authentications; susceptibility to authorisations; susceptibility to communication technology; susceptibility to hardware failure or configuration change; susceptibility to key person dependency; susceptibility to business continuity; susceptibility to unauthorized physical access; susceptibility to unauthorized information theft or disclosure; susceptibility to user operator errors; susceptibility to software flaws or inadequacies; and susceptibility to theft of system resources.

This explains why some of the problems experienced by the Banks in Kenya include:

- Fraudulent manipulation of financial transactions.
- Accidental misrouting of postings to client's accounts.
- Network and communication failure.
- High rate of system downtimes
- Limited incidences of hacking.
- Software and database corruption.
- Password violations due to users sharing the passwords with colleagues.

Therefore, the Banks need to address the mentioned areas of susceptibility, which have high vulnerability with a view of reducing the vulnerability levels substantively in order to minimize the repeated occurrence of the incidences reported.

The factor analysis was performed across the three categories that represented the security framework namely Management, Operational and Technical Security.

The factor analysis performed on the area of Management Security extracted seven factors to represent the 22 variables.

The average mark on the countermeasure ratings in this category is 4.2461 rounded off to 4. This is above average score in terms of the expected score of 5 per countermeasure. Weighting. This is a good indication of management security practice and implementation within the Banking sector. This can be attributed to the fact that Information Technology has become central in the business operations thus inevitable for the managers to understand the technology that is running the business. Since the data dealt with in this sector is of high sensitivity, the managers have taken it upon themselves to ensure proper security policy and procedures are put in place.

Deducing from the factors that were extracted in this category: -

The first factor (Factor 1) is security responsibility assigned to ensure that adequate security is provided for the mission-critical IT systems. This factor is concerned with Accountability, Availability, Integrity and Utility of the system.

The second factor (Factor 2) concerns the policy on the use of personal computers or communication. This factor is concerned with loss of confidentiality and to a greater extent addresses the security Culture.

The third factor (Factor 3) is concerned with reliable communication links. This factor is concerned with loss of availability and reliability.

The fourth factor (Factor 4) is a documented network configuration control procedure exists. This factor is concerned with loss of accuracy, assurance, culture and integrity.

The fifth factor (Factor 5) is a documented procedure exists for adding and removing network users. This factor is concerned with loss of accountability and security culture.

The sixth factor (Factor 6) is a written hardware configuration control procedure is available. This factor is concerned with Availability, Integrity and Utility of the system.

The seventh factor (Factor 7) addresses redundant communication links. This factor is concerned with the loss of communication thus affecting Availability of the system.

The factor analysis performed on the area of Operational Security extracted nine factors to represent the 33 variables.

The average mark on the countermeasure ratings in this category is 4.3814 rounded off to 4. This is the highest mean score in the three categories and is above the average score in terms of the expected score of 5 per countermeasure Weighting.

This is a good indication of operational security practice and implementation within the Banking sector. This can be attributed to the fact that Banks have existed for a long period of time over which strict procedures and rules have been developed and implemented to counter fraudulent practices. This in Kenyan context has a regulatory body, the Central Bank of Kenya that acts as the “dog watch” to the Banks and ensures that the operational manuals are followed to the letter. This has resulted to Banks practicing prudent banking continue to operate while those that overlooked or ignored this laid down procedures have fallen victims to fraudulent practices, which has led them to statutory management or closure.

Deducing from the factors that were extracted in this category: -

The first factor (Factor 1) is system preventative maintenance is done on regular basis. This factor is concerned with loss of Availability of the system.

The second factor (Factor 2) is all positions are reviewed for sensitivity level. This factor is concerned with loss of confidentiality and accountability.

The third factor (Factor 3) is changes to the computer room environment setting are controlled. This factor is concerned with loss of availability.

The fourth factor (Factor 4) is there exist a documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties. This factor is concerned with loss of accountability, assurance, culture and integrity.

The fifth factor (Factor 5) is the room that houses the computers has restricted access. This factor is concerned with loss of accountability, availability and integrity.

The sixth factor (Factor 6) is concerned with access to communication access points. This factor is concerned with Availability and Accountability of the system.

The seventh factor (Factor 7) is safeguard-computing facility using electronic badge systems etc. This factor is concerned with the loss of availability, accountability and integrity of the system.

The eighth factor (Factor 8) is security monitors and alarm systems. This factor is concerned with the loss of availability, accountability and integrity of the system

The ninth factor (Factor 9) is partial backups are done at least once a day and full backups of network files are done at least once a week. This factor is concerned with the loss of availability, utility, accountability and integrity of the system

The factor analysis performed on the area of Technical Security extracted four factors to represent the 14 variables.

The average mark on the countermeasure ratings in this category is 4.2205 rounded off to 4. This is a good indication of technical security practice and implementation within the Banking sector bearing in mind that computing is not that old in this country. This can be attributed to the fact that Banks handle highly sensitive data thus the need to put in place adequate technical security measures.

Deducing from the factors that were extracted in this category: -

The first factor (Factor 1) is users have a pre-authorised set of system privileges and commands. This factor is concerned with the loss of Accountability, Integrity and Utility of the system.

The second factor (Factor 2) is log –in to software applications require a unique identifier. This factor is concerned with loss of confidentiality, accountability and integrity of the system.

The third factor (Factor 3) is you virus scan all software before loading into the system. This factor is concerned with loss of accuracy, availability, utility, assurance, culture and reliability of the system.

The fourth factor (Factor 4) is a written procedure exists for acceptance testing of software. This factor is concerned with loss of accuracy, assurance, culture and integrity.

From the analysis all the factors that represented the Management Security area, factor 6 had the highest vulnerability within the Banking sector at a score of 7 out of the acceptable 9.25. Factors 1 and 2 had the least vulnerability.

In the area of Operational Security, Factor 7 had the highest vulnerability at a score of 9.25 while in the area of Technical security; Factor 4 had the highest vulnerability at a score of 5.375.

The countermeasure (factor 7 in operational security) is concerned with safeguarding of computing facilities via Electronic Badge systems, Biometrics and Closed circuit Television. This has received less attention and the banks need to

strengthen their effort towards improving the countermeasure rating thus lowering the vulnerability level. The area of Technical security has the lowest vulnerability scores when benchmarked on security practices based on due diligence. In general, for an organisation to meet its mission/business objectives, it needs to implement its systems with due care consideration of IT-related risks to the organisation, its partners and customers. Thus the Banks through its response to the countermeasures have addressed the seven elements of security namely availability, accountability, integrity, confidentiality, assurance and security culture.

Confidentiality, Integrity and Assurance

Confidentiality is dependent on Integrity, in that if the integrity of the system is lost, then there is no longer a reasonable expectation that the confidentiality mechanisms are still valid. Integrity is dependent on confidentiality, in that if the confidentiality of certain information is lost, then the integrity mechanisms are likely to be by-passed. Availability and accountability are dependent on confidentiality and integrity in that if confidentiality is lost for certain information, the mechanisms implementing these objectives are by passable while if system integrity is lost, then confidence in the validity of the mechanisms implementing these objectives is also lost. All these objectives are interdependent with assurance. Security culture enables management to constantly make employees aware of the risks facing the IT installations they work with. According to Mwondi [2002], a true foundation of security is good policy. Without a policy, there is no clear-cut way of controlling the way procedures or devices are implemented or how to manage them. In controlling the security risks, the respondents considered a combination of the Management, Operational and Technical security controls in order to maximize the effectiveness. In this study, the outcome of the analysis portrays a contrast position to the statement of the problem earlier stated. It shows otherwise in that banks have managed to incorporate security controls that are commensurate with the new technology acquired or enhanced. This assessment is based on the fact that

the analysis was benchmarked on due care approach to Computer security Practices.

Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior Management and functional and business managers to use the least-cost approach and implement the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the organisation's resources and mission.

5.3. Conclusion on Perceived Security Risk.

The perceived security risks were ranked on a scale of 1 to 10 and the analysis done based on mean and modal rank.

On average, the majority of the respondents indicated moderate risks ranked from 3.1 to 6.00 for the security related problems. However, communication systems failure received a high modal score of 10 indicating that majority of the respondents consider these problem to pose the highest risk to their computer systems.

In conclusion, there is no simple answer to the problem of achieving overall information system security. Issuing a policy is the first line of defense in a company's strategy to ensure that its network and information is safeguarded. The policy should be designed around the customs of a business, failing which its implementation would be difficult. Representatives of all cadres within the business should have a role to play in policy formulation one needs to keep the reader in mind by for example, including more technical detail for IT system personnel or using plain language for the average user. The policy should cover everything that cuts across the Management, Operational and technical security

controls. 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 of the organizations on computer-based systems means that the data they hold and the ability to process the same constitutes a major corporate asset. Data has no value until it is transformed by the application of intellectual process into information. Because information is company's most valuable asset, it must be the primary focus of corporate security. Therefore anything that denies the continued access to these assets jeopardizes their ability to conduct business in a timely and profitable manner. The protection of information requires the corporation to identify information assets, classify them, define access, establish ownership, determine vulnerabilities and the consequences of compromise. These requirements can be managed through the development of corporate security policies. Information assets are both tangible (marketing plans, customer lists, strategic plans, servers, network components) and intangible (company reputation, goodwill, databases). For each of these business assets, vulnerability assessment helps to develop strategies for safeguarding and protecting them.

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 procurement 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.

- In recommending controls and alternative solutions to minimize or eliminate identified risks, the following factors should be addressed:
 - Effectiveness of recommended options (e.g. system compatibility)
 - Legislation and regulation
 - Organizational policy
 - Operational impact
 - Safety and reliability.

- The government must provide proper security policy legislation and regulation in order to leverage IT investment in this sector (e.g. a common ATM switch to serve the Banks in Kenya).

- Proper contingency planning measures should be put in place and always tested and reviewed.

- Constant review of management, operational and technical security controls.

Corporate security is a continuous, on-going process involving business threat and risk assessment, review of technical, operational and management vulnerabilities and security policy refinement. 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:

1. 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.
2. The study did not incorporate the views of the end-users of the computer systems.
3. 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.
4. The sample collected is not a random sample
5. The researcher is in the Banking Industry. The respondents might not have been willing to give a lot of information as they may think that the same could be used against the competition.

5.6 Recommendations for Future Research

1. To carry out a cross sectional analysis of the security awareness in the Kenyan banking Sector. Hypothesis: Larger banks are more computer security Aware as compared to the smaller banks.
2. A detailed survey on the Computer Security Policies implemented by different Banks as compared to the CoBiT and BS 7799 Standards.
3. The Risk Analysis done in relationship to the implementation of Internet Banking in Kenyan Banks
4. The use of Smart Card Technology and its impact to Security in Kenyan Banks
5. The use of Confidentiality, Integrity and Availability factors as articulated by the CoBiT standards in predicting Security practices in Kenyan Banks.
6. Computer Security levels are set based on an organisation's willingness to "invest" in sound business processes rather than as an "insurance" to contain losses.
7. The impact of Computer Crime to the growth of Information Technology in the Banking Industry in Kenya.
8. How well are the Banks in Kenya prepared to handle E-Banking?

6.0 APPENDIX I

The table below shows a list of Banks in Kenya under study.

Barclays Bank of Kenya
Kenya Commercial Bank
Standard Chartered Bank
National Bank of Kenya
NIC Bank
Citibank
CFC Bank
Commercial Bank of Kenya
Co-operative Bank of Kenya
Diamond Trust
Development Bank of Kenya
First American
I & M
First American
Southern Credit Bank
Housing Finance
Consolidated Bank
Stanbic Bank
Credit Agricole Indosuez
Middle East Bank
Trans-National Bank
K-Rep Bank
Guardian Bank
Akiba Bank
Imperial Bank

The table below shows a list of Banks under study.

Industrial Development Bank
Fina Bank
Prime Bank
Victoria Commercial Bank
Prime Bank
Biashara Bank
City Finance Bank
Bank of Baroda
Bank of India
Giro Commercial Bank
Equatorial Commercial Bank
Habib A.G. Zurich
ABC Bank
Credit Bank
Chase Bank
Charterhouse Bank Ltd
Habib Bank Ltd
Dubai Bank (Formerly Mashreq Bank)
Paramount Universal Bank
Fidelity Commercial Bank
Central Bank of Kenya

APPENDIX II

QUESTIONNAIRE

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 []
- Palms : 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 []

1. 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) Unionisable Staff: 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)

Transaction Processing Systems (TPS) []

Management Information Systems (MIS) []

Decision Support Systems (DSS) []

Executive Information System (EIS) []

Expert Systems (ES) []

Strategic Information Systems (SIS) []

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

Yes []

No []

Please explain

.....

.....

SECTION B

Listed below are statements dealing with various issues in the security of computer systems. Please tick () in the appropriate box to indicate in terms of expectations, the extent to which you consider the following countermeasures to be applicable in your organisation.

	Strongly Agree		Neutral		Strongly Disagree
Countermeasures.					
MS					
1. Security responsibility assigned to ensure that adequate security is provided for the mission –critical IT systems	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. A policy on the use of personal computers or Communication exists	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. There are dedicated leased lines for system communication.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. A documented network configuration control procedure exists.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. A documented procedure exists for adding & removing network users.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. A written hardware configuration control procedure is available.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7. There exists redundant communication links	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Countermeasures.

8. Protection against natural disaster (e.g. floods and earthquakes).

9. The duties of individuals are separated by a procedure or software.

10. Vendors do not retain their accounts on the system

11. Pre-employment screening is done regarding the applicant's previous employment, formal education, criminal history, personal financial situation, drugs and alcohol abuse.

12. Technical Personnel are cross-trained in all aspects of managing and maintaining your computer resources.

13. All software configuration changes follow a written procedure.

14. Resigned or terminated employees are removed from premises.

15. Risk assessments are performed & documented on a regular basis whenever the system, facilities, or other conditions change.

16. Has a mission/Business impact analysis been conducted?

Countermeasures.

17. Tests and examinations of key controls routinely made e.g. network scans, analyses of router & Switch settings, penetration testing[]

18. Security alerts & security incidents are analysed & remedial actions taken.

19. Management ensures that corrective actions are effectively implemented.

20. Computer users have had training on systems hardware and software they use

21. Computer users have had formal or informal computer security training

22. Policy Forbids using unauthorized or illegally obtained software

OS

Countermeasures.

23. System preventative maintenance is done on a regular basis.

24. All positions are reviewed for sensitivity level.

25. Changes to the computer room environment setting is controlled (e.g. heat and humidity).

Countermeasures.

- | | | | | | |
|---|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| 26. A procedure for the management of magnetic media exists. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 27. There exist documented job descriptions that accurately reflect assigned duties & responsibilities & that segregate duties. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 28. The room which houses the computers has restricted access. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 29. Communication access points

(Closets, rooms, etc) are kept locked. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 30. Safeguard computing facility using | | | | | |
| Electronic badge system | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Biometrics Access Control | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Closed-Circuit Television
Monitoring ,Sensors & Alarms | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 31. Security monitors and alarm systems are installed in the computer room. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 32. Partial backups are done at least once a day and full backups of network files are done at least once a week. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 33. Data that are critical to the mission is stored off site. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Countermeasures.

- | | | | | | |
|--|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| 34. Log-in attempts are limited to a specific number for the network users. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 35. Vendor (logon) identifications are removed from the network server. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 36. Computer screens are created away from passersby. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 37. A Uninterruptible Power Supply (UPS) is installed for your system. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 38. A backup power source e.g. battery or Generator, is installed. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 39. Access to the computer fuse or circuit breaker panel is controlled. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 40. Critical data is stored in fireproof safes. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 41. Fire detection equipment are installed in the computer room. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 42. Fire extinguishing systems are installed in the computer room | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 43. There is a Disaster Recovery Site | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 44. Individuals who are authorised to bypass significant technical & operational controls are Screened prior to access & periodically after. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Countermeasures.

- | | | | | | |
|---|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| 45. Output to third party applications like Excel, Word Outlook is discouraged | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 46. The duties of individuals are separated by a procedure or software | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 47. The Computer room is kept clear of hazardous material | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 48. A procedure for the management of magnetic media exists | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 49. You store copies of back-up media for the computer | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 50. You remove data storage media from the system when its not in use | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 51. Access scripts with embedded passwords are Prohibited | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 52. All software configuration changes follow a written procedure | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 53. Is information or media purged, overwritten or destroyed when disposed or used elsewhere? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 54. Locks are installed for doors to the Computer terminal space and network controllers | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Countermeasures.

55. Access to tables defining network options, resources, and operator profiles is restricted

TS

56. Users have a pre-authorized set of system privileges and commands.

57. Log-in to software applications requires a unique identifier.

58. You virus scan all software before loading into the system.

59. A written procedure exists for acceptance testing of software.

60. New software is validated in accordance with an established policy.

61. Sensitive data is encrypted before transmission

62. Vendors do not retain their account on the system

63. Are passwords unique & difficult to guess (e.g. do passwords require alpha numeric, upper/lower case, & special characters)?

Countermeasures.

64. Are inactive user identifications disabled after a specified period of time?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
65. Access to files is restricted to logical view	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
66. Access to tables defining network options, resources, and operator profiles is restricted.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
67. You have deployed Firewalls & Intrusion Detection Systems	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
68. Access to online audit logs is strictly controlled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
69. Alternative system communication paths are available	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
70. Sensitive data is encrypted before transmission	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
71. Redundant or functionally equivalent hardware is available	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

SECTION C.

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. []

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

.....

.....

.....

.....

.....

.....

.....

.....

.....

SECTION D

Listed below are statements dealing with various issues of Computer Security Awareness. Please tick () in the appropriate box to indicate whether YES/NO to the statements provided.

1. Are policy documents on computer Security circulated to all staff in the organisation?

YES []

NO []

2. Are the IT staff informed of the critical assets of the organisation as relates to Computers?

YES []

NO []

3. You have had formal or informal computer security training and aware of information security rules and regulations?

YES []

NO []

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

YES []

NO []

5. Is important information on security threats such as viruses circulated to all staff on the network?

YES []

NO []

6. Does the organisation send IT staff to seminars on Computer Security?

YES []

NO []

7. Is the IT Manager aware of Security Standards? If yes, please name some.

YES []

NO []

8. Is the IT/IS Manager aware of the different types of threats?

YES []

NO []

9. Is the IT/IS Manager aware of legal liability incase of disclosure of customer information?

YES []

NO []

10. Does the IS/IT Manager alert user on the network of any new threat such as viruses from e-mails or from malicious/fraudulent codes?

YES []

NO []

11. Does everyone in the organisation know what to do in the event of an attack?

YES []

NO []

12. Does each employee know the importance of a password?

YES []

NO []

APPENDIX III

Table 1.0 The MOT table

Security Area	Security Criteria
Management Security	<ul style="list-style-type: none"> ➤ Assignment of Responsibilities ➤ Continuity of Business/Support ➤ Incident Response Capability ➤ Periodic Review of security Controls ➤ Personnel clearance and background investigations ➤ Security and Technical Training ➤ Separation of Duties ➤ System Authorization and Reauthorization ➤ System or Application security plan
Operational Security	<ul style="list-style-type: none"> ➤ Control of air-borne contaminants (smoke, dust, chemicals) ➤ Controls to ensure the quality of the electrical power supply ➤ Data Media access and disposal ➤ External Data distribution and labeling ➤ Facility protection (e.g. Computer room, Data centre, Office) ➤ Humidity Control ➤ Temperature control ➤ Workstations, laptops and standalone personnel computers
Technical Security	<ul style="list-style-type: none"> ➤ Communications (e.g. dial in, system interconnection, routers) ➤ Cryptography ➤ Discretionary access control ➤ Identification and Authentication ➤ Intrusion Detection ➤ System audit ➤ Application Software Maintenance Controls ➤ Data Integrity/Validation Controls

✓ VULNERABILITIES.

1. Susceptibility to Authentication
2. Susceptibility to Authorisations
3. Susceptibility to Communication Technology
4. Susceptibility to inter/ intranetwork user activity.
5. Susceptibility to hardware failure or configuration change.
6. Susceptibility to environmental hazards.
7. Susceptibility to key person dependency.
8. Susceptibility to improper handling of storage media.
9. Susceptibility to Business Continuity
10. Susceptibility to unauthorized physical access.
11. Susceptibility to unauthorized programmatic access.
12. Susceptibility to loss of data or software files.
13. Susceptibility to unauthorized information theft or disclosure.
14. Susceptibility to failure and instability of electrical power sources.
15. Susceptibility to fire.
16. Susceptibility to User operator errors
17. Susceptibility to software flaws or inadequacies
18. Susceptibility to theft of system resources

7.0 Glossary

1. Confidentiality is the security objective that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing and while in transit.
2. Integrity is the security objective that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).
3. Accountability is the security objective that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
4. Availability is the security objective that generates the requirement for protection against intentional or accidental attempts to perform unauthorized deletion of data or otherwise cause a denial of service or data.
5. Supermarket Banking refers to a one stop shopping for Banking services and Products.
6. E-commerce refers to trading or transacting over the Internet.

7. Fraud is commonly understood today to mean dishonesty in the form of an intentional deception or a willful misrepresentation of a material fact.
8. 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
9. Threat is the potential for a “threat source” to exploit (intentional) or trigger (accidental) a specific vulnerability. A threat source is either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) the situation and method that may accidentally trigger a vulnerability
10. Denial of Service attacks send large numbers of requests to a server, essentially creating a traffic jam and rendering the server inaccessible by legitimate users.
11. Hackers, sometimes called crackers, refer to those who break into computers without authorization. They can include both insiders and outsiders.
12. 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.
13. Patches are programs that correct a problem or software bug with or add additional features to a particular software title.
14. Social Engineering is a non-technical method of obtaining confidential network security information, such as people posing as technical support

representatives & making direct calls to employees to gather password information.

15. Reconnaissance attacks are essentially information-gathering activities in which hackers collect data to later compromise a network.
16. Access attacks exploit weaknesses in network access points such as authentication services or file-transfer protocol servers

11. Gaithersburg J. "Computer System Security and Privacy Advisory Board," 1991 Annual Report, March 1992, p.18.
12. Infosys India (2002) Finacle Newsletter on e-platform for tomorrow's Bank.
13. IQ Business Foundations Building the Network Infrastructure for Internet Success January/February 2002 Cisco Magazine
14. James Essinger (1990) Computer Security in Financial Organisations
15. 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.
16. KPMG East Africa Fraud Survey Report 2002
17. Marianne Swanson (Nov, 2001) Security Self-Assessment Guide for Information Technology Systems. COMPUTER SECURITY (National Institute of Standards and Technology).
18. Murray Kevin TNC Engineering Security Standards Whitepaper December 18,1998.
19. Ochieng Oloo et al: Market Intelligence; The Business & Finance Journal Banking survey 2002
20. 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.
21. SANS Institute resources www.sans.org
22. Scott Blake, Today's IT Security Challenge Date published in TECS: November, 2001 by: Security Program Manager, BindView
23. Security Patch Management by StBernard www.stbernard.com

24. Sprouse M. "Sabotage in the American Workplace: Anecdotes of Dissatisfaction, Mischief and Revenge. Pressure Drop Press, San Francisco, California, 1992
25. SSSC Systems security Study Committee (1991)
26. Symantec Antivirus Research Centre (SARC)
27. U.S. Department of Energy Computer Incident Advisory Capability (CIAC) Information Bulletin
28. Violino B. et al: "Tempting Fate," Information Week, October 4,1993: p.42
29. Wilk R. J. "Security and Control of Your PC Network". International Association for Computer Systems Security, Inc. New York, 1993.
30. 2600 (1997), 2600: The hacker Quarterly Web Page, http://www.2600.com/hacked_pages