EVALUATION OF SECURITY OF INFORMATION SYSTEMS IN THE KENYAN BANKING INDUSTRY

BY:

KIEMO, PETER MURAYA

D61/P/7709/05

A MANAGEMENT RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT OF THE DEGREE OF MASTERS OF BUSINESS ADMINISTRATION (MBA), SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI.

NOVEMBER, 2009
DECLARATION

STUDENT:
This research project is my original work and has not been submitted to any University for the award of a degree.

KIEMO, PETER MURAYA
D61/P/7709/05

SUPERVISOR:
This project has been submitted for examination with my approval as the University Supervisor

KATE LITONDO
Lecturer, Department of Management Science
School of Business
University of Nairobi
DEDICATION

I dedicate this publication to my family and friends for their inspiration during my studies.
ACKNOWLEDGEMENTS

I am very grateful to my Supervisor, Mrs. Litondo for the valued academic and professional guidance, not forgetting Mr. Lelei and Dr. Muganda for their valuable criticisms and suggestions and finally the entire University of Nairobi fraternity for according me a conducive learning environment.

May the Almighty God bless you all!
TABLE OF CONTENTS

DEDICATION .......................................................................................................................... ii

ACKNOWLEDGEMENTS .................................................................................................... iii

List of Abbreviations ................................................................................................................ vi

List of tables ............................................................................................................................. vii

List of figures .......................................................................................................................... viii

CHAPTER ONE: INTRODUCTION ...................................................................................... 1

1.1 Background ............................................................................................................... 1

1.2 Statement of the Research Problem ......................................................................... 5

1.3 Objectives of the Study ............................................................................................. 7

1.4 Importance of the Study ............................................................................................. 7

CHAPTER TWO: LITERATURE REVIEW ......................................................................... 8

2.1 The Value of Information Assets .............................................................................. 8

2.2 Information Security ................................................................................................. 8

2.3 Information Security Systems .................................................................................. 13

2.3.1 Information Security Policies, Standards, Procedures and Guidelines .... 13

2.3.2 Data Encryption............................................................................................... 13

2.3.3 Firewalls.......................................................................................................... 13

2.3.4 Virus Protection Software .............................................................................. 14

2.3.5 Intrusion Detection and Prevention Systems ................................................ 14

2.3.6 Security Awareness and Training Programs ................................................ 14

2.3.7 Access Control Systems................................................................................. 15

2.3.8 Incident Management Process........................................................................ 15

2.4 Elements of Security ............................................................................................... 15

2.4.1 Confidentiality................................................................................................. 16

2.4.2 Integrity ............................................................................................................ 17

2.4.3 Availability ...................................................................................................... 18

2.4.4 Identification, Authentication and Accountability ...................................... 19

2.4.5 Authorization, Privacy and Nonrepudiation ................................................ 19

2.5 Benefits of Information Security in the Kenyan Banking Sector ......................... 20

2.6 Challenges in Implementation of Information Security in the Banking Industry. ......................................................................................................................... 21
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.7 COBIT Framework</td>
<td>28</td>
</tr>
<tr>
<td>2.8 Summary of Literature Review</td>
<td>29</td>
</tr>
<tr>
<td>CHAPTER THREE: RESEARCH METHODOLOGY</td>
<td>31</td>
</tr>
<tr>
<td>3.1 Research Design</td>
<td>31</td>
</tr>
<tr>
<td>3.2 Population of Study</td>
<td>31</td>
</tr>
<tr>
<td>3.3 Data Collection</td>
<td>31</td>
</tr>
<tr>
<td>3.4 Data Analysis and Reporting</td>
<td>32</td>
</tr>
<tr>
<td>CHAPTER FOUR: RESULTS AND FINDINGS</td>
<td>33</td>
</tr>
<tr>
<td>4.0 Introduction</td>
<td>33</td>
</tr>
<tr>
<td>4.1 Demographic Analysis</td>
<td>33</td>
</tr>
<tr>
<td>4.2 Information security systems</td>
<td>38</td>
</tr>
<tr>
<td>4.3 Benefits of implementation of information security</td>
<td>39</td>
</tr>
<tr>
<td>4.4 Challenges in implementation of information system security</td>
<td>42</td>
</tr>
<tr>
<td>CHAPTER FIVE: SUMMARY OF FINDINGS, DISCUSSION, CONCLUSIONS AND RECOMMENDATION</td>
<td>45</td>
</tr>
<tr>
<td>5.1 Introduction</td>
<td>45</td>
</tr>
<tr>
<td>5.2 Summary and Discussions of the findings</td>
<td>45</td>
</tr>
<tr>
<td>5.3 Conclusion and Recommendations</td>
<td>47</td>
</tr>
<tr>
<td>5.4 Limitation of the Study</td>
<td>48</td>
</tr>
<tr>
<td>5.5 Suggestions of further Study</td>
<td>48</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>49</td>
</tr>
<tr>
<td>APPENDICES</td>
<td>53</td>
</tr>
<tr>
<td>Appendix 1</td>
<td>53</td>
</tr>
<tr>
<td>Appendix 2</td>
<td>54</td>
</tr>
<tr>
<td>Appendix 3</td>
<td>60</td>
</tr>
</tbody>
</table>
LIST OF ABBREVIATIONS

ATM- Automated Teller Machines  
CBK- Central Bank of Kenya  
CISO- Chief Information Security Officer  
COPPA- Children’s Online Privacy Protection Act  
DTI- Department of Trade and Industry  
EFT- Electronic Finance Transfer  
FAT- File Allocation Table  
GSM- Global System for Mobile  
HIPPA- Health Insurance Portability and Accountability Act  
IIS- Internet Information Services  
ICT- Information Communication Technology  
IT- Information Technology  
ITIL- Information Technology Infrastructure Library  
ITGI- Information Technology Governance Institute  
ISACA- Information Systems Audit and Control Association  
KBA- Kenya Bankers Association  
LAN- Local Area Network  
PC- Personal Computer  
PDA- Personal Digital Assistant  
SMS- Short Messaging Services  
SOX- Sarbanes Oxley  
SQL- Structured Query Language  
WAN- Wide Area Network  
VoIP- Voice over Internet Protocol
LIST OF TABLES

Table 4.1 Employees in the bank ................................................................. 35
Table 4.2 Spread of bank’s network............................................................. 36
Table 4.3 Bank dependence on IT............................................................... 36
Table 4.4 Current job profile....................................................................... 38
Table 4.5 Information security systems .................................................... 38
Table 4.6 Total variance explained ............................................................. 40
Table 4.7 Rotated Component Matrix......................................................... 41
Table 4.8 Total variance explained ............................................................. 42
Table 4.9 Rotated Component Matrix......................................................... 43
LIST OF FIGURES

Figure 4.1 Period of operation................................................................................................34
Figure 4.2 Ownership of bank................................................................................................34
Figure 4.3 Number of branches..............................................................................................35
Figure 4.4 Level of security measures ..................................................................................37
Figure 4.5 Presence of an overall security officer.................................................................37
ABSTRACT

This project evaluates the security of information systems in the Kenyan banking industry by examining the systems utilized by the Kenyan banks, challenges encountered in the implementation of information security and benefits accrued from such implementations. The advancement of global technological trends have made the issue of information security very complex with huge losses being experienced daily through web based fraud, denial of service attacks, computer viruses and hacking of corporate information. These losses can be minimized with the implementation of sound information security systems.

The research uses COBIT framework that have been drawn from the literature especially on implementation of information security and a descriptive survey has been used in this study. Questionnaires were administered by a “drop and pick” method to all 46 banks in Kenya. The respondents were the ICT Managers, Information Security Managers or any other IT professionals with the knowledge of information security systems in the banks. The data collected has been analyzed using the descriptive statistics and presented in frequency tables, percentages and charts. In addition factor analysis was used to analyze the data.

The project finds that, for the banking industry in Kenya the issue of information security has been taken seriously and has deployed various systems and practices to enhance the security of information. The study revealed that the most widely deployed information security system in the banks is the firewall, followed by intrusion detection systems. The study further reveals that the challenges can be grouped in two categories namely information related challenges and financial related challenges. Majority of the respondents see lack of senior management commitments to security initiatives as the greatest challenge to implementation of information security due lack of understanding of information security issues. This has contributed to lack of budget for information security strategy and tactical plans. The study also found out that majority of the banks agreed that they benefited by having a firm foundation for efficient and effective risk management as a result of implementation of information security, a lesser number...
strongly agreed that information security leads to improved trust in customer relationship.

To overcome the challenges and maximize the benefits the banks need that to give information risks the same prominence given to financial risk. The senior management of the banks needs to be educated on the importance of information security so that they can give support to information security initiatives. Further the information security role must be elevated in the organization hierarchy preferably to the board level. The best example is of having a chief information security officer (CISO) sitting in the board who will ensure that information security matters are discussed at the highest level of the bank.
CHAPTER ONE: INTRODUCTION

1.1 Background

1.1.1 Overview of the banking industry in Kenya
The banking industry in Kenya has experienced rapid growth in the last five years in terms of numbers the banks and their branch networks with some spreading their reach regionally. Rao et al (2007) observes that banks store, process, and transact a variety of electronic information for various stakeholders, this information in particular need to be kept secure, confidential, and accurate.

Currently, there are forty-six commercial banks in Kenya (Central Bank of Kenya, 2009). Thirty-five of the banks, most of which are small to medium sized, are locally-owned. The industry is dominated by a few large banks most of which are foreign-owned, though some are partially locally-owned. The commercial banks offer corporate and retail banking services but a small number, mainly comprising the larger banks, offer other services including investment banking. Commercial banks in Kenya are governed by the Companies Act, the Banking Act, the Central Bank of Kenya Act and the various prudential guidelines issued by the Central Bank of Kenya (CBK).

The banking sector was liberalised in 1995 and exchange controls lifted. The CBK, which falls under the Minister for Finance’s docket, is responsible for formulating and implementing monetary policy and fostering the liquidity, solvency and proper functioning of the financial system. The Central Bank Kenya publishes information on Kenya’s commercial banks and non-banking financial institutions, interest rates and other publications and guidelines. The banks have come together under the Kenya Bankers Association (KBA), which serves as a lobby for the banks’ interests and also addresses issues affecting its members. The efficiency and the range of services provided by banks have tremendously increased. This is as a result of the banks having taken to large use of information systems which plays a very important role in banking.

1.1.2 Information Systems in the Banking Industry
McCumber (2005) defines information systems as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition...
of information. Drucker (1993) stated, "The diffusion of technology and the modification of
information transform the role of information into a resource equal in importance to important
resources of land, labour and capital". Use of information for decision making has become
paramount for the success of organizations. He further argues that knowledge is fast becoming
the sole factor of productivity, sidelining both capital and labour. According to Rao (2007),
banks have installed large and complex information systems that comprises core banking
systems, internet banking, automated clearing houses, electronic funds transfer, credit and debit
card networks and large local and wide area networks.

Osborne (2006) observes that traditionally banks stored information on paper, this paper
information was processed manually. By 1961, most banks had taken a significant step to
introduce computers into their operations. These early computer systems were programmed in
machine code and required information to be manually inputted via punched cards. These
systems were limited by the method of inputting information and the computer system's process
power. Today's computer systems are mostly networked and ON-LINE, that is, information is
automatically updated.

Leeladhar (2005) states that many banks would affirm that from playing a passive back-end role
in the business, ICT has gradually become acknowledged as one of the key drivers of business
success. Today's banks would confirm that the information systems is pivotal to the success of
every business and is a vital strategic asset. It is the platform on which banks communicate not
only internally but also externally, i.e., with other corporations. Ogeto (2004) asserts that with
increased reliance on computers and other technology there raises a new set of security needs. He
further asserts that Information Technology has improved the speed and efficiency of banking
operations particularly routine banking transactions and as a result has shaped the nature of the
services provided to customers. The flexibility provided by IT has helped banks develop new
products and improve the quality of current services offered to customers. Examples of these
transactions include deposits, withdrawal, and transfer of funds between banks or countries and
payment of bills. Banks are faced with a lot of challenges that requires only those with the best
mix of personnel and objectives to survive. One such challenge is security of information
systems.
1.1.3 Security of Information Issues in the Banking Industry

Calder et al (2005) states that security of information systems means different things to different people; to vendors of security products, it tends to be limited to the product(s) they sell. To many directors and managers, it tends to mean something they don't understand and that the IT manager has to deal with. To many users of IT equipment, it tends to mean unwanted restrictions on what they can do on their corporate PCs. These are all dangerously narrow views.

Ogeto (2004) observes that threats to information systems need to be contained. This containment is best done via an information security programme. An information security programme should support the mission of the organization. It is an integral element of sound management. It should be cost effective. The individual's responsibilities and accountability should be explicit. It requires a comprehensive and integrated approach; and finally, it should be periodically reassessed.

Security of information systems has also been defined by McCumber (2005) as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability. Kairab (2005) asserts that over the past few years, security of information systems has evolved from a technology issue to a boardroom issue. Companies are affected every day by security-related incidents such as network intrusions, viruses, or denial of service attacks. Some of these incidents are reported but many probably are not.

Rao et al (2007) asserts that security of information systems has taken the defence in depth principle. The defense in depth is a methodology that originated from the military and refers to having multiple levels of defense in place to maximize the amount of time it takes for the attacking party to reach the most valuable assets. Defense in depth includes three levels: people, process, and technology. Controls need to be applied on all three levels for an effective defense in depth approach. He further asserts that banking is a highly regulated industry. Information security regulation requires banks to protect the confidentiality, integrity, and availability of customer information. There exist several of the important laws that require information security
According to Rao et al (2007) several security issues face the banking industry; this includes technology enabled cyber crimes where someone gains unauthorized access to the bank's networks. Identity fraud which occurs when a person uses another person's personal data in someway that involves fraud or deception, typically for economic gain. Identity theft is another process by which the person obtains the personal information about a victim. This does not have to done with a computer; however, computer technology has made it easier for criminals to obtain this information. The most common and oldest method of identity theft is dumpster diving where an individual searches for valuable information from papers thrown in the dustbin. Phishing is an online scheme where e-mails are sent by criminals who seek to steal your identity, rob your bank account or take over your computer. Skimming is used to describe a type of credit card fraud where the magnetic stripe on any type of card is cloned and used without the owner's knowledge stealing the information from a person's credit card can be done in many different fashions. The tangible and intangible benefits the implementing security of information systems generates to banks cannot be over emphasised.

1.1.4 Challenges and Benefits of Implementing Security of Information Systems in the Banking Industry

Olivia (2004) states that with constantly increasing technical complexity, legal barriers and privacy expectations, the challenges of information security have risen exponentially in the past five years. Information Systems Audit and Control Association (ISACA) (2005) has summarized several factors that pose as the greatest challenge in implementation of information security. Some of these are; lack of senior management commitment to information security initiatives, failure of management to understand the information security issues, lack of information security planning prior to implementation of new technologies and lack of Integration between business and information security.

Information Technology Governance Institute (ITGI) (2006) has outlined the various benefits of implementing information security systems in the banking industry. Firstly, banks are protected from increasing potential for civil or legal liability as a result of information inaccuracy or the
absence of due care. Secondly, there is increased predictability and reduced uncertainty of business operations by lowering information security-related risks to definable and acceptable levels. Thirdly, banks that practice good information security governance has increase of share value. Finally, implementation of information security ensures that there is firm foundation for efficient and effective risk management, process improvement, and rapid incident response related to securing information and a level of assurance that critical decision are not based on faulty information.

As Rao et al (2007) puts it, with implementation of information security, banks have improved trust in customer relationships as well as ensuring that organisation reputation is protected. There is decreasing likelihood of violation of privacy, greater confidence when interacting with trading partners. It also enables new and better ways to process electronic transactions thus reducing operational costs by providing predictable outcomes and mitigating risk factors that may interrupt the process. Other benefits include protection from loss of customers and business revenue through loss of employee productivity and inability to meet business requirements. Implementation of information security enables banks to have a competitive advantage over their competitors, however there various challenges in the implementation.

1.2 Statement of the Research Problem
Calder (2005) states that there are a number of trends that lie behind the increases in threats to information security, which, when taken together, suggest that things will continue to get worse, not better: The threats basically create major challenges for the banking industry. Better hacker tools are available every day, on hacker websites that, themselves, proliferate. These tools are improved regularly and, increasingly technologically proficient criminals and computer literate terrorists are thus enabled to cause more and more damage to target networks and systems. Olivia (2004) concludes that IT executive and senior management must retain a vigilant posture concerning information security, as the impact of a successful attack or theft can be devastating to customers and the organization in terms of loss of customer trust, unreliable information and corrective action expenses.

A survey by Ernst and Young (2002) that focused on corporation in US found that more than 75
percent of business had experienced some interruption of their critical business systems related to IT security. Garg et al (2003) cites a survey by CSI/FBI which revealed that companies in US had reported a total loss of US$ 456 Million for IT-security related incidents in 2002. However, given that only between 10 and 20 percent of detected incidents are actually reported, while informative, this estimate could likely be a significant understatement. The global economic impact of information security is high and this calls for extensive research in the field of information security especially in the Kenyan banking sector with a view of identifying the information security systems deployed, establishing the benefits derived from the implementation of information systems security and finally analyzing the challenges in encountered in such implementation.

Security of information is therefore of paramount importance especially to the banking sector and this forms the motivation behind the study to evaluate the security of information in the Kenyan banking industry. Further motivation emanates from the researcher having keen interest in the area of information security having pursued some certifications in this area of study.

There are previous studies done on the area of information security both in the local and international arena. Ogeto (2004) undertook a survey of computer-based information systems security implemented by large private manufacturing companies in Kenya. The study was done with a special focus on the manufacturing sector and concluded that though most of the Manufacturing firms have invested heavily in information technology, few of the firms allocate specific budget to the IS security team or function which means that this critical and crucial function has to compete with other IT/IS functions for resources. This has been seen to hamper growth development in information systems security leading to further exposure from the information systems security risk perspective.

A study done by Sookdawoor (2005) undertook an Investigation of Information Security Polices and Practices in Mauritius; this study focused on only a limited area of information security systems (policies and practices) and was a general study not limited to the banking industry. The study concludes that organization in Mauritius lacked properly defined and implemented security policies.
Another study done by Biri and Trenta (2004) on Corporate Information Security Governance in Swiss Private Banking looked into the governance aspect of information security in relation to private banking industry in Switzerland. The findings of this study indicates that information security in the form of reliable and efficient processing, though often overlooked, makes significant contribution to both internal company value creation chain and protection of good reputation and is tackily by clients and company management.

This study seeks to answer the following research questions: Given the vulnerabilities of information systems due to technological development, what challenges do banks face when implementing information security systems and what benefits have been derived from their implementation? This study also will seek to fill the knowledge gap in the area of information security, specifically in the Kenya banking industry.

1.3 Objectives of the Study

The general objective of the study is to undertake an evaluation of security of information systems in the Kenyan banking industry with the following specific objectives;

1. Identify information security systems and practices.
2. Establish the benefits of implementing information systems security.
3. Analyze challenges in implementation of information systems security in the banking industry in Kenya.

1.4 Importance of the Study

This study will be important to commercial banks will get a better understanding of the challenges they are likely to face when implementing security of information system and the benefits likely to accrue from the same. It will also add on to the existing body of knowledge in the area of information security. Thus, academics will use this study as a basis for further research on the area. The study will also be invaluable to information systems security consultants and information systems auditors as the study will pin point areas that need to be addressed in the implementation of information security in the banking sector.
CHAPTER TWO: LITERATURE REVIEW

2.1 The Value of Information Assets
Olivia (2004) states that information has value to its owners, users, automated systems that must use it and government agencies that regulate access to it. For example, Wal-Mart stores could not operate efficiently without over 30 terabyte data warehouse that tracks the cost, profit, shelf life, and other metrics associated with every product sold in every store. Major domestic and international airlines could not efficiently schedule and crew billions of dollars of equipment, nor operate their revenue capacity maximization models without the use of sophisticated databases and information systems valued over several billion dollars of replacement cost.

As Olivia (2004) further observes, the business model for Visa, MasterCard International and American Express is based around card use data collection, account tracking, fraud analysis, customer billing and receipt collection information for hundreds of millions of credit and charge cards. The collective value of their databases and information assets is in the hundreds of billions of dollars; more than the annual budgets of all nations of the world, except for the U.S. and Japan. Wall Street stock trading and financial institutions would not be able to open for business without having confidence in the accuracy of information used to conduct trades, base valuations on, or estimate earnings against. Accurate and trusted information is a core underpinning in market transparency and investor confidence.

2.2 Information Security
According to Calder (2005, the use of distributed computing is increasing. Computing power has migrated from centralized mainframe computers and data processing centers to a distributed network of desktops, laptops and micro-computers. There is a strong trend towards mobile computing. The use of laptop computers, Personal Digital Assistants (PDAs), mobile phones, digital cameras, portable projectors and MP3 players has made working from home or on the road relatively straightforward, with the result that network perimeters have become increasingly porous. There are many more remote access points to networks, and the number of easily accessible endpoint devices has increased dramatically, increasing the opportunities to break into networks and steal or corrupt information.
As Wylder (2004) observes, there has been a dramatic growth in the use of the internet for business communication, and the development of wireless, VoIP and broad-band technologies will drive this even further. He asserts that there is widespread computer literacy. While most people today have computer skills, the next generation is growing up with a level of familiarity with computers that will enable them to develop and deploy an entirely new range of threats.

Bosworth et al (2000) states that security can be defined as the state of being free from danger and not exposed to damage from accidents or attack, or it can be defined as the process for achieving that desirable state. The objective of information system security is to optimize the performance of an organization with respect to the risks to which it is exposed. Business is becoming increasingly dependent on technology and the internet to the point where some businesses would come to a screeching halt if they did not have it. This is particularly true in larger companies, where the ability to communicate and access information is the lifeblood of the business. The internet provides an effective, immediate and powerful method for organizations to communicate on all sorts of issues. This exposes all these organization to the security risks that go with connection to the internet.

According to Kairab (2005), the need to secure information is becoming greater all the time as we leverage technology to automate functions, as more data becomes electronic, and as companies become increasingly reliant on the internet as an integral part of their information technology (IT) infrastructure. Businesses are becoming increasingly connected because business to business relationships are helping companies drive efficiencies and shorten the supply chain. E-commerce is gaining acceptance as more people buy goods and services online, resulting in an increasing number of companies having a presence on the Web. With these relationships, a host of security issues must be addressed.

According to Peltier (2005), an effective information security program endeavors to ensure that the organization’s information and its processing resources are available when authorized users need them. It must take into account the business objectives and the mission of the organization and ensure that these goals are met safely and securely as possible. Understanding the customer’s
needs must be the first step in establishing an effective information security program. Information security is not only a technical issue, but a business and governance challenge that involves adequate risk management, reporting and accountability. As ITGI (2006) puts it, effective security requires the active involvement of executives to assess emerging threats and the organization's response to them.

According to McCumber (2005) the art and science of security requires a complete understanding of the value of the assets requiring protection. The asset under scrutiny is primarily the information transmitted, stored, and processed by the organization. Secondarily, the computer and telecommunications resources themselves require protection. The goals of Information security are to ensure the confidentiality, integrity and the availability of data within a system. The data should be accurate and available to the appropriate people, when they need it, and in the appropriate condition. Warkentin et al (2006) notes that perfect security is not feasible, instead IT security managers strive to provide a level of assurance consistent with the value of the data they are asked to protect.

ITGI (2006) argues that an enlightened approach to information security takes the larger view that an organization's information and the knowledge based on it must be adequately protected regardless how it is handled, processed, transported or stored. It addresses the universe of risks, benefits and processes involved with all information resources. The security of information, as with other critical organizational resources, must be addressed at the total enterprise level. It further argues that as banks strive to remain competitive in the global economy, they respond to constant pressures to cut costs through automation, which often requires deploying more information systems. Whilst managers become ever more dependent on these systems, the systems have become vulnerable to a widening array of risks that can threaten the existence of the enterprise. This combination is forcing management to face difficult decisions about how to effectively address information security. This is in addition to scores of new and existing laws and regulations that demand compliance and higher levels of accountability.

Calder et al (2005) assert that security of information system is necessary because the threats to the availability, integrity and confidentiality of the organization's information are great, and
always increasing. All organizations possess information, or data, that is either critical or sensitive. In the Information Security Breaches Survey 2004, the UK Department of Trade and Industry commented: ‘information is widely regarded as the lifeblood of modern businesses’.

According to a 2000 DTI survey, 49 per cent of organizations believe that information is critical or sensitive because it will be of benefit to competitors, while 49 per cent believe that it is critical to maintaining customer confidence. The 2004 survey identified the fact that, while 58 per cent of all businesses had highly confidential information stored on their computer systems, 77 per cent of large businesses were in this category. Two other findings of the 2004 survey indicate the extent to which UK businesses are dependent on electronic information: roughly nine-tenths of them now send e-mail across the internet, browse the web and have a website; and 87 per cent of businesses now identify themselves as ‘highly dependent’ on electronic information and the systems that process it, compared to 76 per cent in 2002.

Organizations are facing a flood of threats to this information. It is self-evident that organizations should, therefore, take appropriate steps to secure and protect their information assets. This is particularly so because, as Osborne (2006) asserts, a web of legislation and regulation makes firms criminally liable and, in some instances, makes directors personally accountable, for implementing and maintaining appropriate risk control and information security measures.

Olivia (2004) argues that information security is no longer an “event” or part-time assignment for corporate and government organizations rather it has become a continuous process every second of every day, from both the technology and management perspectives. Most executives of small companies are unaware that their corporate firewall is probed hundreds of times a day by automated attack tools. Financial services and government firewalls are often probed tens of thousands of times every day.

According to Garg et al (2003), without a doubt, information security is a pervasive concern for all companies and continues to rise in importance. It is now considered a mainstream operational concern as companies utilize the Internet as a key driver of E-business and greater collaboration. While the exigencies of E-commerce require that the internet be safe and secure, the reality is drastically different. As adoption and dependence on the internet grows, electronic collaboration
will accelerate rapidly as organizations see the impact on their bottom lines. However, concerns over security and associated issues continue to be listed as a top challenge, hindering the multibillion dollar potential of B2B (business-to-business) and B2C (business-to-consumer) opportunities.

In addition to the growth of E-commerce, several significant changes driven by the forces of globalization and the regulatory environment make information security an even greater area of concern. Examples of such laws include the HIPAA (1996), COPPA (1998), and Gramm-Leach-Bliley Act (1999), SOX (2002), Other pieces of UK legislation that are relevant to information security include Copyright Designs and Patents Act (1988); the Computer Misuse Act (1990); the Data Protection Act (1998); the Human Rights Act (1998); the Electronic Communications Act (2000); the Freedom of Information Act (2000); Regulation of Investigatory Powers Act (2000); the Privacy and Electronic Communications Regulations (2003) that require thorough safeguards to protect the security and confidentiality of data, individual medical records, and the privacy of children on the Internet.

Sookdawoor (2005) argues that computer systems and the information processed on them must be considered critical assets that support the mission of an organization. Protecting them can be as important as protecting other organisation resources such as financial resources, physical assets, and employees. The costs and benefits of information protection should carefully be examined in both monetary and non monetary terms to ensure the cost of controls does not exceed expected benefits. Information protection controls should be appropriate and proportionate.

Today, as Bosworth et al (2002) puts it, information systems are much larger and more widely distributed, interconnected, and interdependent, and the risks are many times greater. So too are the potential costs of any IS disruption. Data processing, transmission, and storage now occur throughout the premises and far beyond. Many and diverse intra- and interoffice transmission media exist, and still more that may connect a vast number of remote sites. The infrastructure has become much harder to protect.
2.3 Information Security Systems

According to Pettersson (2008), banks have deployed various systems to secure their information. This includes but not limited to the following:

2.3.1 Information Security Policies, Standards, Procedures and Guidelines

ISACA (2007) defines policies as a formalization of information security practices as established and approved by the top management for implementation and compliance by all stakeholders in order to protect organisational information assets. Procedures and guidelines are derived from polices, industry standards and best practices to ensure that security of information is maintained. According to Miller et al (2007), policies, standards, guidelines, and procedures all work together as the blueprints for a successful information security program. They establish governance, provide valuable guidance and decision support and help establish legal authority.

2.3.2 Data Encryption

Osborne (2006), defined data encryption as the conversion of data in to a form, called a cipher text, that cannot be easily understood by unauthorized people. The science of writing secret code is referred to cryptography. Parker (1998) notes that cryptography is well suited for communicating and storing sensitive information that needs protection.

Banks have sensitive information, and we know from actual loss experiences that there are adversaries, including competitors, spies, and thieves, that want to take advantage of such information. Cryptography not only protects data from theft or alteration but can also be used for user authentication. According to Kessler (1998), there are two types of cryptographic schemes typically used, secret key (symmetric) cryptography and Public key (asymmetric) cryptography.

2.3.3 Firewalls

According to Pettersson (2008), the major activity deployed by businesses to protect computer systems and data from electronic intrusion is the utilization of firewalls. Firewalls are utilized to establish a barrier between the business computer systems and the outside world. Firewalls may be a combination of hardware and software or it may be software only. A firewall filters or restricts access externally to enter system and access internally to exit system. The usual
implementation of a firewall is to place a barrier between a computer system and the Internet (perimeter security). Firewalls must be set too restrict access both inbound and outbound.

### 2.3.4 Virus Protection Software

Charmayne (2001) states that viruses, worms, Trojan Horse, time bomb, logic bomb, and trapdoors may also harm information systems and supporting technology. Virus protection software must be deployed to protect bank’s information systems from damage by these activities. Virus protection software must be kept current as new viruses are developed on what seems like a daily basis. Some businesses have policies that limit acceptance of attachments to e-mails, prohibit the use of disks prepared on non-business systems, and restrict downloading files from the Internet to trusted sites only.

### 2.3.5 Intrusion Detection and Prevention Systems

According to Chesla (2004), these are network security devices that monitor network and/or system activities for malicious or unwanted behaviour. There are two kinds of intrusion detection systems which are normally deployed. These are host- and server-based intrusion detection systems. These systems must be able to detect the critical files being accessed and exploitation of system vulnerability. The systems need to be able to detect certain incidents through behavioural analysis and pattern recognition of known attack signatures. Intrusion prevention systems are an extension of intrusion detection systems but have further capability of reacting in real-time to block or prevent these activities. A network based IPS, for example, will operate in-line to monitor all network traffic for malicious codes or attacks. When attack is detected, it can drop the offending packets while still allowing all other traffic to pass.

### 2.3.6 Security Awareness and Training Programs

Peltier (2005) assert that an effective information security program can not be implemented without implementing employee awareness and training program to address policy, procedures and tools. Strong security architecture will be rendered less effective if there is no process in place to make certain that employees are made aware of their rights and responsibilities with regard to organization assets. Employees want to know what is expected of them and who to turn for assistance. An on going information security awareness will provide answer to the user
community. Employees need to understand that the security program is supported, approved and directed by the senior management.

2.3.7 Access Control Systems
According Calder (2005), authorized access to information processing facility, logical or physical, is proven to be a key element in security of these systems and applications. Banks have placed special emphasis on developing policies on many of these controls to set expectation and requirements of all the users both internal and external. Users of the organization’s processing facilities should be authenticated and authorized in accordance with a formal policy and method. The method should take the information classification guideline into consideration and take the least privilege when granting rights and permissions. User password management is an important component in controlling and managing access to information processing facilities. Access rights should be reviewed on regular basis by qualified staff not responsible for accounts creation to ensure that the rights are in alignment with roles and responsibilities.

2.3.8 Incident Management Process
ITIL defines an incident as any event which is not part of the standard operation of service and which causes, or may cause, an interruption to, or a reduction in the quality of that service. Calder et al (2005) asserts that the first goal of incident management process is to restore a normal service operation as quickly as possible and to minimize the impact on the business operations, thus ensuring that the best possible levels of service quality and availability are maintained. Incidents are as a result of failures or errors in the IT infrastructure. The incident management process consist of various sub processes; Incident detection and recording, classification and initial support, investigation and diagnosis, resolution and recovery, incident closure and finally incident ownership, monitoring, tracking and communication.

2.4 Elements of Security
There are many elements that form the foundation stone on which a successful information security program is built and for over twenty years, information security has held Confidentiality, Integrity and Availability (known as the CIA triad) as the core principles of
information security. Many information security professionals firmly believe that Accountability should be added as a core principle of information security.

2.4.1 Confidentiality

Osborne (2006) defines confidentiality is the requirement that particular information be restricted to the appropriate people. The concept of confidentiality attempts to prevent the intentional or unintentional unauthorized disclosure of a message's contents. Loss of confidentiality can occur in many ways, such as through the intentional or unintentional release of private company information or through a misapplication of network rights. According to McCumber (2005) confidentiality is perhaps the most widely recognized and most deeply studied security requirement. Confidentiality is the basis for the science of cryptography that has its documented beginnings in the Roman Empire. The primary consideration of confidentiality is not simply keeping information secret from everyone else; it is making it available only to those people who need it, when they need it, and under the appropriate circumstances. He further argues that perhaps the most significant imperative for confidentiality is not the element of secrecy, but the capability to ensure the appropriate subjects (both people and other processes or systems) have the requisite access when needed.

According to Parker (1998), to provide adequate security enforcement, it is always important to ensure you can develop and publish a comprehensive matrix that defines the nature of confidentiality for your environment. Identifying individuals in the organization may accomplish this, but the most common way is to define people by their job title or responsibilities. In this way, access requirements can be succinctly codified for the organization independent of the individuals in it. Depending on the size of the information systems environment, this policy process can be either relatively simple or amazingly complex. It begins with an inventory of individual roles and responsibilities throughout the organization that is supported by the IT system. Then a comprehensive list of all the available information resources needs to be developed. These lists are then mapped against each other as roles. This process is often lacking in even the most security-conscious environments. Alone, this exercise can be extremely beneficial for objectively determining who should have access to specific informational resources. When combined with the structured process, it becomes a powerful method to
strategically assess organization confidentiality policies and a key tool for tactically applying technology to support security requirements.

McCumber (2005) concludes that confidentiality is a relatively simple concept that, in practice, requires a broad spectrum of technology and procedural enforcement in IT systems. Once you have developed your confidentiality policies and have charted them in the methodology, you will have a basis for determining the requirements for cryptography and other confidentiality safeguards.

2.4.2 Integrity
Osborne (2006) defines integrity as the principle that requires information to maintain its precision. The concept of integrity ensures that: modifications are not made to data by unauthorized personnel or processes, unauthorized modifications are not made to data by authorized personnel or processes, and the data is internally and externally consistent; in other words, that the internal information is consistent among all sub entities and that the internal information is consistent with the real world (external situation).

According to McCumber (2005), the integrity element of security is foundational. Inaccurate information can be worse than worthless. It can provide a false understanding of the business environment or even a military battlefield and lead decision makers into taking self-destructive actions.

Parker (1998) state that integrity consists of ensuring the information is accurate, complete, and robust. As with the concept of security itself, integrity represents an ideal. Obviously, there are limits to the ability of security safeguards to provide for complete and robust information resources, but the integrity attribute is a central aspect to security enforcement. Integrity controls also include cryptographic solutions as well as authentication, non-repudiation, and comparative analysis. McCumber (2005) observes that many current definitions of integrity are woefully inadequate and many are notoriously incorrect. One widely cited definition defines data integrity as the assurance that data can only be accessed or modified by authorized users. Obviously, this definition is wildly deficient. This definition assumes that authorized users will always acquire,
maintain, and update information with 100 percent accuracy. It also presumes the user will not make any type of mistake nor undertake any malicious or non-malicious activity that could jeopardize the integrity of information resources for which they have authorized access. Because both of these scenarios are patently preposterous, we can safely assume we will not make the mistake of employing it as our understanding of information integrity.

Merkow et al (2000) concludes that information integrity is one of the most demanding and yet the subtlest and least defined of the information attributes to maintain. The great majority of investment in safeguards and protective techniques are targeted at maintaining information integrity. Yet, it is vital to ensure that integrity is assessed and enforced even at the acquisition of the data or the information's introduction into your systems.

2.4.3 Availability

Osborne (2006) defines availability as the principle to ensure that our data will be available in a timely manner. The concept of availability ensures the reliable and timely access to data or computing resources by the appropriate personnel. In other words, availability guarantees that the systems are up and running when needed. In addition, this concept guarantees that the security services that the security practitioner needs are in working order. According to McCumber (2005), if information is needed for a decision or for any other purpose and it is not there, it is simply not available. If integrity represents the accuracy and robustness of data, then availability is the timeliness factor. The availability element of security is often relegated as an afterthought, or at best, a control left for a simple demand for redundancy and uptime requirements. In practice, availability is often the single most critical assurance for critical IT systems. For example, the fact that a profit-making enterprise has a database of all its current customers makes the intrinsic value of the data important. If that information is deleted, the company may lose business from those customers as a result of its inability to meet the demand of access to its business information. Availability is the cornerstone security requirement and one that requires protection.

According to Merkow et al (2000), recovery systems work hand in hand with backup technology to ensure information can be restored to its primary function in the event it is required. A key
element of this process is once again a risk management decision. Solutions that provide near-
immediate fail over and recovery are, as a rule, significantly more expensive than solutions that
demand extensive manual recovery techniques. Availability also employs a variety of other
safeguards and countermeasures to ensure that information resources are available when they are
needed for the decision makers. Understanding the nature of security requires the practitioner to
ensure that security is applied to the information resources in the context of their environment.
Security is a moot concept unless it is fully analyzed with the elements of information valuation
threats as safeguards.

2.4.4 Identification, Authentication and Accountability
Identification is defined by Krutz et al (2007) as the means by which users claim their identities
to a system. Most commonly used for access control, identification is necessary for
authentication and authorization. Cole et al (2005) further defines identification as the act of a
user professing an identity to the system, such as logon ID. He also defines authentication as the
testing or reconciliation of evidence of a user's identity. It establishes the user's identity and
ensures that the users are who they say they are. He has also defined accountability as system's
capability to determine the actions and behaviours of a single individual within a system and to
identify that particular individual. Audit trails and logs support accountability.

2.4.5 Authorization, Privacy and Nonrepudiation
Krutz et al (2007) defines authorization as rights and permissions granted to an individual or
process that enable access to a computer resource. Once a user's identity and authentication are
established, authorization levels determine the extent of system rights that a user can hold.
Leeladhar (2005) argues that Authorization of users is an activity that needs to be closely
regulated and monitored. One of the basic requirements for implementation of security and
monitoring thereof at the various departments is the need for system administrators. Most of our
offices and departments have the system administration function clubbed to the normal
operational functions assigned to a particular officer. The proliferation of networks within an
office also acts as a negative factor in implementation of strict security features. Further, rights
assigned need to be changed upon change of functions assigned to the operative staff and that
updating, including those related to staff who retire have to be looked into.
Kruiz et al (2007) defines privacy as the level of confidentiality and privacy protection given to a user in a system. This is often an important component of security controls. Privacy not only guarantees the fundamental tenet of confidentiality of a company's data, but also guarantees the data's level of privacy, which is being used by the operator.

Stewart et al (2005) observes Nonrepudiation ensures that the subject of an activity or event cannot deny that the event occurred. Nonrepudiation prevents a subject from claiming not to have sent a message, not to have performed an action, or not to have been the cause of an event. It is made possible through identity, authentication, authorization, accountability, and auditing. Nonrepudiation can be established using digital certificates, session identifiers, transaction logs, and numerous other transactional and access control mechanisms.

### 2.5 Benefits of Information Security in the Kenyan Banking Sector

For reasons of efficiency, as well as the complexity of modern financial instruments, banking information is predominantly processed in the form of electronic data in computer systems within the framework of planning, decision, execution and control of transactions of all types (Biri et al, 2004). This is the reason why IT security is often referred to, where information security is actually meant. The limitation of information security to the specific aspect of the design and implementation of the protection of electronic data (IT Security) would be an undue simplification because other types of important data sources are therefore ignored. In addition, such as limited approach may hardly take the strategic objectives of the particular bank into consideration. When banks exchange information to help facilitate business processes, the importance of privacy is fairly well established and has become customary.

Cisco (2001) argues that banks want their information kept confidential to prevent damage that may occur if the information is obtained by third parties that could use the information to negatively impact the customers' trust resulting in legal suits and losing competitive position of the bank. In the case of publicly held banks, improper dissemination of proprietary information could negatively impact stock value. The common thread between the privacy of proprietary corporate information and personal data provided by individuals is that the improper
dissemination and use of the information can cause damage. Such damage could be financial, or it could damage reputations. In situations where HIPAA rules are involved, for example, the fines can be up to $250,000.

### 2.6 Challenges in Implementation of Information Security in the Banking Industry

To remain competitive banks have adopted technology to offer innovative services to their ever demanding customers. These technological trends lie behind the increases in threats to information security in the banking industry. The threats basically create major challenges for the banking industry. Calder (2005) indicates that there is a strong trend towards mobile computing. The use of laptop computers, Personal Digital Assistants (PDAs) and mobile phones has made access to banking services from office, home or on the road relatively straightforward. There has been a dramatic growth in the use of internet banking, electronic funds transfer (EFT), ATM services, SMS banking, and mobile phone banking (e.g. M-Pesa and Zap). This exposes banks to security risks that go with wide area networks (WANs) and connection to the internet.

According to Leeladhar (2005), banking as a business involves the management of risks. While much has been said about the financial risks, the risks arising out of the large scale implementation of technology is of recent origin, with banks having taken to large scale use of technology for their normal day-to-day business. Security in banks has thus assumed significant proportions, comprising both physical aspects in addition to those relating to Information, Information Systems and Information Technology, all of which have an impact on the reputational risk of a financial organisation. In a world where geographical barriers are losing significance and the death of distances is already a reality, it is but essential that security be given prime importance in a transnational scenario where large sums of money are at stake. While the challenges related to physical security are those which can be confronted with relative ease, the position is much more complicated in respect of information security.

Calder (2005) argues that security is as effective as the weakest link in a chain. And, in the case of banking, the weakest link, does not relate to the components of technology (which do have an implication although), but on the person who is part of the information supply chain, and is typically the insider in the bank itself. Studies have indicated that a substantial portion of the
breach of security in financial institutions have occurred on account of, or have been triggered with the aid of internal exposures or internal controls being compromised. Leeladhar (2005) asserts that indeed the growing reality of today's world is that with a few key strokes, an organization's entire arsenal of information could be wiped-out, completely destroyed. Banks are in this kind of vulnerable position. While providing an on-demand real time service to their clients, they must necessarily put in place the appropriate processes to help safeguard the sanctity and security of customer information and other critical data. Against this backdrop, the security requirements of the banking sector need to be assigned high levels of priority.

McCumber (2005) argues that information Security is something which is best experienced than explained. All of us have at some point of time experienced the flow of information to persons others than to the intended users - even in a non-electronic traditional environment. With networking and access to information being available at rates much larger than before, Information Security is an activity which provides some comfort to both the policy makers and the users of data. The largest set of functions in the banking sector which has benefited from the advances in IT relate to payment systems since quick, safe and efficient transfer of funds across the length and breadth of the country is the requirement of the day. Security in Payment Systems cannot be addressed in isolation. It requires the integration of work processes, communication linkages and integrated delivery systems and should focus on stability, efficiency and risk control. Yet another prime aspect of concern in a good security policy is the role that the human beings have in a secure computerised environment.

ISACA (2005) has outlined thirteen factors that are critical in success of information security programme. The factors create major challenges if they are lacking in implementation of information security programme. These factors are;

2.6.1 Lack of Senior Management Commitment to Information Security Initiatives

One of the factors considered as a major challenge in successful implementation of information systems security is lack of senior management’s commitment to information security initiatives. Senior management should require that all requests for technology expenditures include technology risk identification and risk mitigation requirements as part of the cost-benefit analysis, project objectives, deliverables and funding request. Senior management should
communicate consistently that every employee is accountable for information security by ensuring that expectations are clearly communicated in the company’s information security policies and standards, and consistently demonstrate that violations will not be tolerated. Every employee, including management, should be required to attend an information security awareness update annually and new employees should be appropriately informed of the company’s information security concepts and practices.

Miller et al (2007), supports by observing that senior-level management is often responsible for information security at several levels, including the role as an information owner. Management has a responsibility to demonstrate a strong commitment to an organization’s information security program. This commitment can be achieved through corporate information security policy and this policy should include a statement of support from management and should also be signed by the CEO or COO. The management should show leadership by example, a CEO who refuses to carry a mandatory identification badge or who bypasses system access controls sets a poor example. The management should put in place a compensation scheme for employees where proper security behavior is rewarded accordingly.

2.6.2 Failure of Management to Understand the Information Security Issues

Failure of management to understand information security issues as another major challenge. Information security managers must increase their understanding of the business and their skills in communication through industry-specific education and executive-level continuing education programs. Information security awareness sessions should start at the executive level and hierarchically proceed to the inclusion of all levels of management and employees. Information security managers should seek industry and other publications that target executive and senior management and ensure that those publications are made available to the management team. Senior Management will be in a better position to support security initiatives if they are educated on how critical IT systems are to the continued operation of the enterprise.

2.6.3 Lack of Information Security Planning Prior to Implementation of New Technologies

Lack of information security planning prior to implementation of new technologies has also been identified as a major challenge. The company’s policies and standards must require review and
formal authorization of changes to the technology environment prior to implementation. The designation of authority to provide such authorization should be a management position, without separation of duties conflicts, and include responsibility for reporting the status of information security to the board. Exceptions to the company’s policies and standards with regard to change management should be formally requested and approved by the company’s policy oversight committee or equivalent. The information security manager and the audit manager should work closely to monitor the environment for technology implementations that do not meet the requirements of the company’s policies and standards. The information security manager should identify all change management processes used by the organization to tap into them for notification that changes are taking place that may impact security. There is a need to implement processes whereby security implications are considered in each change management process that the organization may implement.

2.6.4 Lack of Integration between Business and Information Security

Lack of integration between business and information security is also a major challenge that should be considered in successful implementation of information systems security. Senior management should ensure that business liaisons are held accountable for interacting with the information security manager to achieve mutually agreeable risk management objectives. Senior management should ensure that the business strategy is shared with information technology and appropriate risk management groups, such as information security. This will help ensure that necessary adjustments to the information security strategy and technology infrastructure capability can be proactively planned to help manage cost and risk. The information security status associated with high-risk legal and regulatory compliance should be monitored at the executive level to ensure that appropriate priority is given to risk management initiatives.

2.6.5 Lack of Alignment of Information Security with the Organization’s Objectives

Lack alignment of information security with the organization’s objectives is another critical factor in implementation of information security system. An information security strategy that is aligned with the company’s risk management and corporate governance requirements should be developed and implemented. Each line of business that “owns” information requiring specific levels of confidentiality, integrity and availability should designate a liaison to work with the
information security manager to ensure that requirements are properly reflected and prioritized in the information security strategy. Measurements of control effectiveness should include alignment with regulations and laws and those measurements should be reported to the board on a quarterly and annual basis through, or with, the chief legal counsel, chief compliance officer, and chief auditor or their equivalents. Information security must support business activities to be of value to the organization. Strategic alignment of information security in support of organizational objectives is a highly desirable goal often difficult to achieve. It should be clear that the cost effectiveness of the security program is inevitably tied to how well it supports the objectives of the organization and at what cost.

2.6.6 Lack of Executive and Line Management Ownership and Accountability for Implementing, Monitoring and Reporting on Information Security

Lack of executive and line management ownership and accountability for implementing, monitoring and reporting on information security is also a major challenge. Information security should have an independent reporting structure to ensure that concerns, accomplishments and views on governance are properly represented to those ultimately responsible to the stakeholders. Pertinent key control objectives should be incorporated into the performance measurement process for all employees. Appropriate levels of management should have responsibility for ensuring that information security violation, authorization exceptions and other pertinent security measurements associated with their line of business processes are researched and acted upon on their behalf.

2.6.7 Lack of Appropriate Employee Education and Awareness on Information Asset Protection

Every employee should be required to attend an information security awareness update annually and new employees should be appropriately informed of the company’s information security concepts and practices. Senior management should communicate consistently that every employee is accountable for information security by ensuring that expectations are clearly communicated in company information security policies and standards, and consistently demonstrate that violations will not be tolerated. Senior management should ensure that business liaisons are held accountable for interacting with the information security manager to achieve
mutually agreeable risk management objectives.

Peltier (2005) supports by observing that an effective information security program can not be implemented without implementing employee awareness and training program to address policies, procedures, and tools. This school of thought is also supported by Krutz et al (2003) who state that employees must understand how their actions, even seemingly insignificant actions, can greatly affect the overall security position of an organization. Roper et al (2006) supports and concludes that increasing awareness involves promoting the probability that people will consider security as they go about their work and personal lives by building recognition of the reality and presence of the threat so that countermeasures are recognized as necessary.

2.6.8 Lack of Consistent Enforcement of Information Security Policies and Standards

The company's policies and standards must require review and formal authorization of changes to the technology environment prior to implementation. The designation of authority to provide such authorization should be of management position, without separation of duties conflicts, and responsible for reporting the status of information security to the board. Exceptions to the company's policies and standards with regard to change management should be formally requested and approved by the company's policy oversight committee or equivalent. Measurements of control effectiveness should include alignment with regulation and law and those measurements should be reported to the board on a quarterly and annual basis through, or with, the chief legal counsel, chief compliance officer, and chief auditor or their equivalents. Schifreen (2006) supports by noting that every company needs a formal written document which spells out to staff precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. This document is known as an information security policy.

Ross (2007) supports by arguing that the ideal situation is for the security of the system to be self enforcing. To some extent, this is currently a reality. Firewalls, intrusion detection systems and virus filters do monitor there respective domains and take action when a deviation from the rules is detected. But then, who makes the rules? And even more particularly, how can it be demonstrated that rules implemented in a particular security measure equate to policies and
standards that were enunciated for human beings, not machines? Therefore people must undertake the role of security enforcement. Ogeto (2004) notes that the primary goal of an information security program is to manage risks to information systems. The programs plan is to develop ways to lower current risk through administrative, environmental/physical and technical measures.

2.6.9 Low Placement of Information Security within the Organization Hierarchy
Information security managers must increase their understanding of the business and their skills in communication through industry specific education and executive-level continuing education programs. The information security status associated with high-risk legal and regulatory compliance should be monitored at the executive level to ensure that appropriate priority is given to risk management initiatives. Information security should have an independent reporting structure to ensure that concerns, accomplishments and views on governance are properly represented to those ultimately responsible to the stakeholders.

2.6.10 Lack of Budget for Information Security Strategy and Tactical Plan
Senior management should require that all requests for technology solution expenditures include technology risk identification and risk mitigation requirements as part of the cost-benefit analysis, project objectives, deliverables and funding request. An information security strategy that is aligned with the company's risk management and corporate governance requirements should be developed and implemented. Each line of business that "owns" information requiring specific levels of confidentiality, integrity and availability should designate a liaison to work with the information security manager to ensure that requirements are properly reflected and prioritized in the information security strategy. Pattinson (2007) supports by noting that insufficient resources results in information security management systems suffering due to management failure to conduct an adequate risk assessment.

2.6.11 Lack of Consistent Board/Executive Management Message with Regard to Information Security Priorities
Communicate consistently that every employee is accountable for information security by ensuring that expectations are clearly communicated in company information security policies
and standards and consistently demonstrate that violations will not be tolerated. Senior management should ensure that business liaisons are held accountable for interacting with the information security manager to achieve mutually agreeable risk management objectives. Information security status associated with high-risk legal and regulatory compliance should be monitored at the executive level to ensure that appropriate priority is given to risk management initiatives.

2.6.12 Inability to Cost-Justify Information Security
Senior management should require that all requests for technology solution expenditures include technology risk identification and risk mitigation requirements as part of the cost-benefit analysis, project objectives, deliverables and funding request. An information security strategy that is aligned with the company’s risk management and corporate governance requirements should be developed and implemented. Each line of business that “owns” information requiring specific levels of confidentiality, integrity and availability should designate a liaison to work with the information security manager to ensure that requirements are properly reflected and prioritized in the information security strategy.

2.6.13 Failure of Applying Generally Accepted Information Security Best Practices/Metrics
The information security manager should participate in industry organizations that are actively working on developing metrics and practices that effectively balance business product development needs and risk management. The information security manager should seek training in process management, such as ITIL. The information security manager should work closely with line-of-business managers to ensure that measurements associated with information security tie to real business risks. Security metrics should tell us about the state or degree of safety relative to a reference point.

2.7 COBIT Framework
ITGI (2007) observes that, to achieve effective governance, executives require that controls be implemented by operational managers within a defined control framework for all IT processes. The Control Objective for Information and related Technology (COBIT) is a set of best practices (framework) for information technology (IT) management created by Information Systems Audit
and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1996. COBIT’s IT controls objectives are organized by IT process; therefore, the framework provides a clear link among IT governance requirements, IT processes and IT controls. COBIT is focused on what is required to achieve adequate management and control of IT.

COBIT enables the development of clear policies and good practice for IT control throughout the enterprise, hence it has become the integrator for IT good practices and the umbrella framework for IT governance that helps in understanding and managing risks and benefits associated with IT. COBIT 4.1 has 34 high level processes that cover 210 control objectives categorized in four domains: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring and Evaluation providing an end to end view of IT. Security of information is a general control embedded in IT processes and services. Under COBIT framework deliver and support process, DS5 (ensure systems security) emphasis on the need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibility, policies, standards and procedures. This framework will be used in the evaluation of security of information in the Kenyan banking industry.

2.8 Summary of Literature Review

There are various threats that the Kenyan banking industry must deal with by ensuring that there is adequate security of their information systems. In summary, the analysis clearly points to the need for executive and senior management and the information security manager to forge a relationship that enables a consistent message with regard to the priority the organization places on protecting valuable information and intellectual property assets.

However, the analysis also points to the strong need for the message to be backed up with visible and consistent action. That action, say the results, is the establishment and consistent implementation of company policies and standards. Furthermore, the results indicate that without the highest level visibly monitoring the successful implementation of an information security strategy, inconsistent compliance will continue to erode progress and give false comfort regarding the asset protection.
Day-to-day priority conflicts continue to affect the quality and consistency of information asset protection. To ensure that associated risks are taken seriously by every employee and agent of the organization, executive and senior management must become visibly interested in ensuring the information security program's success within their organizations. Biano (2001) observes that the role of technology is paradoxical when it comes to security because technology is one of primary causes of the majority of security risks. For example, sophistication of technology adds to complexity and a steeper learning curve; complexity leads to oversights thereby creating security holes. But paradoxically, most people turn to technology once again for solutions to these security problems! Familiarity of the technology and being informed of the latest developments is one of the primary requirements of a security practitioner.
CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Research Design
The objective of this study was to evaluate information security systems in the Kenyan banking industry. A descriptive survey was undertaken to provide details of interest at a single point in time. As Kolter et al (2001), puts it, the descriptive survey is best suited for gathering descriptive information, and it is used to obtain information concerning the current status of a phenomena with a purpose of describing “what exist” with respect to situation variables. A descriptive survey was appropriate because of the size of sample size under study. Usually, descriptive surveys are ideal where the population of study is not so large like in this case. Factor analysis was used to analyze the data collected in this study.

3.2 Population of Study
The population of study consisted of all the 46 registered commercial banks in Kenya (see appendix 3 as obtained from the Central Bank of Kenya dated June, 2009). The bank branches were not considered as separate entities. Given the size of the population, a census survey was done. All the 46 commercial banks were studied.

3.3 Data Collection
Primary data was collected using questionnaires which will be administered personally by the researcher. Where this method of administration will not be possible, the questionnaires will be dropped and picked later at an agreed time with the respondents. The questionnaires were developed from the literature review. The questionnaires contained statements that reflected the research problem and sought answers to the research questions.

The questionnaire was categorised into four sections to simplify the work of the respondents and for purposes of clarity in presentation. Section A captured the organization’s details, Section B captured the information security systems deployed in the Kenyan banks, Section C captured the benefits derived from the implementation of information security, while Section D captured the challenges in undertaking such implementation. A five-point likert scale was constructed to test the differences between the various factors. The respondents of the questionnaires were the bank’s ICT Managers or Information Security Managers (where position exists) and any other
persons who were deemed to have the necessary information of information security system in their respective banks.

3.4 Data Analysis and Reporting

The Statistical Package for Social Sciences (SPSS) package was used to analyze the data from the correctly filled and collected questionnaires. Descriptive statistics was used to analyze data in this study. This included the use of frequencies, percentages and measure of central tendency to analyze data collected in Section A and B of the questionnaire. Factor analysis was used to identify and isolate factors related to benefits and challenges in implementation of information systems security captured in Section C and D of the questionnaire. The analysis sought to establish information security systems that were widely used in the banking industry, the major benefits derived from implementation in information security as well as establish the main challenges the banks faced in implementation of information security.
CHAPTER FOUR: RESULTS AND FINDINGS

4.0 Introduction

This chapter provides statistical presentation and analysis of the data collected. The data has been presented in tables and figures with summaries being given for each table and figure. The objective of this chapter is to explain the data rather than draw conclusions and interpretations. The first part deals with information security systems, the second part on benefits of implementing information systems security, the third part deals with analyzing challenges in implementation of information systems security in the banking industry in Kenya. A chapter summary that includes the major findings of the study is presented in the last part. Out of 46 questionnaires conferred to the respondents, 33 were returned filled hence the researcher attained a 71.74 percent success rate.

The broad objective of the study was to undertake an evaluation of security of information systems in the Kenyan banking industry

The specific objectives of the study were:

1. To identify information security systems and practices
2. To establish the benefits of implementing information systems security.
3. To analyze challenges in implementation of information systems security in the banking industry in Kenya.

4.1 Demographic Analysis

4.1.1 Period of operation

This section aimed at identifying the period of operation of the banks captured. Figure 4.1 below shows the results.
Most of the banks captured in the survey had been in operation for a period of over 30 years. These formed 26% of the businesses covered while those that had been operational for 0-10 years had a 26% share. A paltry 24% had operated for a period of between 11 and 20 years.

4.1.2 Ownership of bank

This area of study aimed at identifying the description of the respondents concerning the ownership of the banks interviewed. Figure 4.2 below shows the results.

Data presented in figure 4.2 above shows that 62 percent of the banks interviewed were locally owned with 29 percent foreign owned. Only 9 percent were both locally and foreign owned.
4.1.3 Employees in the bank

This part of study was carried out with an aim of identifying the number of employees amongst the banks that were interviewed.

| TABLE 4.1: EMPLOYEES IN THE BANK |
|------------------------------|----------------|-----------|
| Number of employees         | Frequency | Percent  |
| Less than 100               | 13        | 38        |
| 101 to 500                  | 15        | 44        |
| 501 to 1000                 | 1         | 3         |
| Over 1000                   | 4         | 15        |
| Total                       | 33        | 100       |

Source: Author

The study established that majority of the interviewed banks, 44 percent had 101 to 500 numbers of employees, followed by 38 percent who had less than 100 employees.

4.1.4 Number of branches.

This area of study aimed at identifying the number of branches amongst the banks. Figure 4.3 below shows the results.

**FIGURE 4.3: NUMBER OF BRANCHES**

The study revealed that majority of the banks had less than 50 branches, 70 percent, with 51 percent having 51 to 100 branches. Only 9 percent had over 100 branches.

4.1.5 Spread of bank’s network

The study went on to establish the spread of the interviewed bank’s branch network.
TABLE 4.2: SPREAD OF BANK’S NETWORK

<table>
<thead>
<tr>
<th>Spread</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Within Nairobi</td>
<td>7</td>
<td>21</td>
</tr>
<tr>
<td>Within Kenya</td>
<td>18</td>
<td>56</td>
</tr>
<tr>
<td>Within east and central Africa</td>
<td>7</td>
<td>21</td>
</tr>
<tr>
<td>Globally</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>33</td>
<td>100</td>
</tr>
</tbody>
</table>

Source: Author

Majority of the banks were located within Kenya, (56 percent) with 21 percent specifically located within Nairobi. 21 percent were within East and Central Africa while 3 percent were globally located.

4.1.6 Bank dependence on IT

Even in a challenging economic climate, the banking industry is more dependent on information technology than ever before. This area of study was carried out with an aim of identifying the level of bank dependence on Information Technology amongst the interviewed banks.

TABLE 4.3: BANK DEPENDENCE ON IT

<table>
<thead>
<tr>
<th>Level of dependence</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very high</td>
<td>22</td>
<td>68</td>
</tr>
<tr>
<td>High</td>
<td>10</td>
<td>29</td>
</tr>
<tr>
<td>No comment</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Total</td>
<td>33</td>
<td>100</td>
</tr>
</tbody>
</table>

Source: Author

68 percent of the interviewed banks had very high dependence on IT; with 29 percent having a high dependence on IT. 2 percent gave no comment.

4.1.7 Level of security measures

Delivering banking services requires a solid security framework that protects the institution's data from outside intrusion and banks are always committed to working with internet service and communications providers to produce the safest operating environment possible for its customers. This section aimed to identify the level of security amongst the interviewed banks.
The study concluded that all banks maintained high levels of security measures.

4.1.8 Presence of an overall security officer
This area of study aimed at identifying the presence of an overall security officer in charge at the banks.

FIGURE 4.5: PRESENCE OF AN OVERALL SECURITY OFFICER

Data presented above revealed that a majority of the interviewed banks did not have an overall security officer (56 percent) while 46 percent had an overall security officer.

4.1.9 Current job profile
This area sought to establish the current job profiles of the various respondents who were interviewed.
TABLE 4.4: CURRENT JOB PROFILE

<table>
<thead>
<tr>
<th>Role</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief information officer</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Chief security officer</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>System administrator</td>
<td>11</td>
<td>35</td>
</tr>
<tr>
<td>IT manager</td>
<td>11</td>
<td>35</td>
</tr>
<tr>
<td>Network/system manager</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>IT security officer</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td>Others</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>33</strong></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>

Source: Author

Majority of the interviewed respondents were system administrators and IT managers (35 percent) while 15 percent were IT security officers, 3 percent were Chief information officers while others were 6 percent.

4.2 Information security systems

Because security is a problem for the whole organization, it simply is no longer effective or acceptable to manage it from the information technology department. Chief Security Officers have the one of the most difficult jobs in executive-level management because their success depends on utilizing many of the organization’s skills and resources.

This section aimed at identifying the levels of utilization on information security systems at the interviewed banks.

TABLE 4.5: INFORMATION SECURITY SYSTEMS

<table>
<thead>
<tr>
<th></th>
<th>Lowest utilization</th>
<th>Low utilization</th>
<th>Moderate utilization</th>
<th>High utilization</th>
<th>Highest utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusion detection</td>
<td>9%</td>
<td>3%</td>
<td>12%</td>
<td>29%</td>
<td>47%</td>
</tr>
<tr>
<td>Access control</td>
<td>3%</td>
<td>3%</td>
<td>3%</td>
<td>56%</td>
<td>35%</td>
</tr>
<tr>
<td>Policies, standards,</td>
<td>0%</td>
<td>0%</td>
<td>9%</td>
<td>44%</td>
<td>47%</td>
</tr>
<tr>
<td>procedures and</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

38
Data from table 4.5 above shows that majority of the banks highly utilized firewalls (62 percent) and Intrusion detection systems (47 percent). 35 percent had moderately utilized Intrusion prevention systems and Security awareness and training programs. In conclusion, only 9 percent had the lowest utilization on Incident management process while 3 percent had the lowest utilization of access control systems.

### 4.3 Benefits of implementation of information security

Information is a vital resource for organizations and hence it is important that information security activities be integrated into the corporate governance structure. Organizations that invest in information security crave to see the benefits of their efforts. Data collected on the information security was analyzed using factor analysis. Factor analysis is a technique that attempts to identify underlying variables, or factors, that explain the pattern of correlation with a set of variables (Field, 2005). Factor analysis is used in data reduction to identify a small number of factors that explain most of the variance observed in a much larger number of manifest variables.

#### 4.3.1 Total variance explained

Table 4.6 below shows the variance of the 11 variables, the percentages of variables attributable to each factor and the cumulative variance of all the factors. Principle component analysis was used and it extracted 3 orthogonal (independent) principle factors. These were the factors with Eigen values greater than 1.
TABLE 4.6: TOTAL VARIANCE EXPLAINED

<table>
<thead>
<tr>
<th>Component</th>
<th>Initial Eigen values</th>
<th>Extraction Sums of Squared Loadings</th>
<th>Rotation Sums of Squared Loadings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>% of Variances</td>
<td>% of Variances</td>
<td>% of Variances</td>
</tr>
<tr>
<td>Total</td>
<td>37.493</td>
<td>37.493</td>
<td>3.320</td>
</tr>
<tr>
<td>1</td>
<td>4.124</td>
<td>37.493</td>
<td>37.493</td>
</tr>
<tr>
<td>2</td>
<td>1.380</td>
<td>12.544</td>
<td>12.544</td>
</tr>
<tr>
<td>3</td>
<td>1.263</td>
<td>11.484</td>
<td>11.484</td>
</tr>
<tr>
<td>4</td>
<td>.952</td>
<td>8.655</td>
<td>8.655</td>
</tr>
<tr>
<td>5</td>
<td>.890</td>
<td>8.088</td>
<td>8.088</td>
</tr>
<tr>
<td>6</td>
<td>.603</td>
<td>5.478</td>
<td>5.478</td>
</tr>
<tr>
<td>7</td>
<td>.577</td>
<td>5.242</td>
<td>5.242</td>
</tr>
<tr>
<td>8</td>
<td>.460</td>
<td>4.181</td>
<td>4.181</td>
</tr>
<tr>
<td>9</td>
<td>.385</td>
<td>3.502</td>
<td>3.502</td>
</tr>
<tr>
<td>10</td>
<td>.218</td>
<td>1.983</td>
<td>1.983</td>
</tr>
<tr>
<td>11</td>
<td>.149</td>
<td>1.350</td>
<td>1.350</td>
</tr>
</tbody>
</table>

Source: Author

Extraction Method: Principal Component Analysis.

The results in Table 4.6 above shows that three (3) components explained total of 61.521% of the variance. It also shows that component 1 represents 37.493% importance, whereas components 2 and 3 are represented by 12.544% and 11.484% of variance across all items respectively. Hair et al (2006) proposes as a rule of thumb that loadings greater than 0.3 are considered significant; loadings of at least 0.4 are considered more important and if loadings are at least 0.5, then they are very significant. If a variable loaded on more than one factor, then the factor with a higher loading of the variable was picked.

4.3.2 Rotated Component Matrix
### TABLE 4.7: ROTATED COMPONENT MATRIX

<table>
<thead>
<tr>
<th>Rotated Component Matrix</th>
<th>Component</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect the bank from legal and civil liability's a result of information inaccuracy (VAR 1)</td>
<td>0.593</td>
<td>0.470</td>
<td>-0.036</td>
<td></td>
</tr>
<tr>
<td>Increase predictability and reduces uncertainty of business operation (VAR 2)</td>
<td>0.124</td>
<td>0.822</td>
<td>-0.034</td>
<td></td>
</tr>
<tr>
<td>May lead to increased share value as result of practice good information security governance (VAR 3)</td>
<td>0.633</td>
<td>0.467</td>
<td>-0.221</td>
<td></td>
</tr>
<tr>
<td>Ensure the reputation of your bank is protected (VAR 4)</td>
<td>0.201</td>
<td>0.772</td>
<td>-0.044</td>
<td></td>
</tr>
<tr>
<td>Ensure that there is firm foundation for efficient and effective risk management (VAR 5)</td>
<td>0.634</td>
<td>0.302</td>
<td>0.331</td>
<td></td>
</tr>
<tr>
<td>Increases level of assurances that critical decisions are not based on faulty information (VAR 6)</td>
<td>-0.027</td>
<td>-0.159</td>
<td>0.614</td>
<td></td>
</tr>
<tr>
<td>Lead to improved trust in customer relationship (VAR 7)</td>
<td>0.381</td>
<td>-0.012</td>
<td>0.639</td>
<td></td>
</tr>
<tr>
<td>Enables new and better ways to process electronic transactions reducing operational costs by providing predictable outcomes (VAR 8)</td>
<td>0.736</td>
<td>0.359</td>
<td>0.007</td>
<td></td>
</tr>
<tr>
<td>Enable banks to have a competitive advantage over their competitors (VAR 9)</td>
<td>0.676</td>
<td>0.211</td>
<td>0.693</td>
<td></td>
</tr>
</tbody>
</table>

Source: Author
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization. (Rotation converged in 9 iterations.)

#### 4.3.3 Factor Isolation

Isolation of factors involves isolating each factor based on the factor loading. These are the correlation between the factors and the factors encountered. The compositions of the two factors as shown in Table 4.7 are presented as follows:

**Factor 1:** consists of 5 items. These items are numbered 1, 3, 5 and 9. These items are associated bank based benefits of implementation of information security.
- **VAR 1:** Protect the bank from legal and civil liability's a result of information inaccuracy
- **VAR 3:** May lead to increased share value as result of practice good information security governance
- **VAR 5:** Ensure that there is firm foundation for efficient and effective risk management
- **VAR 9:** Enable banks to have a competitive advantage over their competitors

**Factor 2:** consists of 2 items. These are represented by item numbered 2 and 4. The items address business based benefits of information security.
WAR 2: Increase predictability and reduces uncertainty of business operation

WAR 4: Ensure the reputation of your bank is protected

Factor 3: consists of 3 items. These are represented by item numbered 6, 7 and 8. The items address business based benefits of information security

WAR 6: Increases level of assurances that critical decisions are not based on faulty information

WAR 7: Lead to improved trust in customer relationship

WAR 8: Enables new and better ways to process electronic transactions reducing operational costs by providing predictable outcomes

4.4 Challenges in implementation of information system security

Modern organizations have a huge challenge on their hands, on a scale unlike anything they've seen since the Y2K crisis. They must “secure” the organization in the face of increasing complexity, uncertainty, and interconnection brought about by an unprecedented reliance on technology to accomplish their mission. This section aimed at identifying the various confronts in implementation of information system security amongst the interviewed banks. In this section of study, two factors were extracted using Varimax rotation from thirty-two variables.

4.41 Total variance explained

Table 4.8 shows the variance of the 13 variables, the percentages of variables attributable to each factor and the cumulative variance of all the factors. Principle component analysis was used and extracted 2 orthogonal (independent) principle factors. These were the factors with eigen values greater than 1.

**TABLE 4.8: TOTAL VARIANCE EXPLAINED**

<table>
<thead>
<tr>
<th>Component</th>
<th>Initial values</th>
<th>Eigen</th>
<th>Extraction Sums of Squared Loadings</th>
<th>Rotation Sums of Squared Loadings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Total</td>
<td>% of Variance</td>
<td>Cumulative %</td>
<td>Total % of Variance</td>
</tr>
<tr>
<td>1</td>
<td>7.5231</td>
<td>57.87048</td>
<td>57.8704</td>
<td>7.52</td>
</tr>
<tr>
<td></td>
<td>63</td>
<td>8</td>
<td>316</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>1.4067</td>
<td>10.82137</td>
<td>68.6918</td>
<td>1.40</td>
</tr>
<tr>
<td></td>
<td>78</td>
<td>5</td>
<td>677</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>0.9094</td>
<td>6.996052</td>
<td>75.6879</td>
<td></td>
</tr>
</tbody>
</table>
The results in Table 4.8 above shows that two (2) components explained total of 68.69185% of the variance. It also so that component 1 represents 57.87048% importance, whereas the second component represented 10.82137% of variance.

4.4.2 Rotated component matrix explained

The initial component matrix was rotated using Varimax (Variance Maximization) with Kaiser Normalization and gave the component transformation matrix as shown on table 4.9. This matrix shows the loading of the 13 variables on the two factors extracted. The higher the absolute value of the loading the more the factor contribute to the variable. These results aid in identification of variables that falls under each of the extracted factors. The gaps on the table represents loading that are less than 0.5. This omission ensures easier readability.

TABLE 4.9: ROTATED COMPONENT MATRIX

<table>
<thead>
<tr>
<th>Component</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of senior management commitment to information security initiatives</td>
<td>0.665595</td>
<td>0.516077</td>
</tr>
<tr>
<td>Failure of management to understand the information security issues</td>
<td>0.648504</td>
<td>0.522155</td>
</tr>
<tr>
<td>Lack of information security planning prior to implementation of new</td>
<td>0.456436</td>
<td>0.750917</td>
</tr>
<tr>
<td>Technologies</td>
<td>Factor Loadings</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>-----------------</td>
<td></td>
</tr>
<tr>
<td>Lack of Integration between business and information security</td>
<td>0.098575 0.810174</td>
<td></td>
</tr>
<tr>
<td>Lack of alignment of information security with the organization's objectives</td>
<td>0.136166 0.850818</td>
<td></td>
</tr>
<tr>
<td>Lack of executive and line management ownership and accountability for implementing, monitoring and reporting on information security</td>
<td>0.540717 0.601742</td>
<td></td>
</tr>
<tr>
<td>Lack of appropriate employee education and awareness on information asset protection</td>
<td>0.413198 0.713721</td>
<td></td>
</tr>
<tr>
<td>Lack of consistent enforcement of information security policies and standard</td>
<td>0.742405 0.348917</td>
<td></td>
</tr>
<tr>
<td>Low placement of information security within the organization hierarchy</td>
<td>0.694498 0.298307</td>
<td></td>
</tr>
<tr>
<td>Lack of budget for information security strategy and tactical plan</td>
<td>0.647112 0.298117</td>
<td></td>
</tr>
<tr>
<td>Lack of consistent board/executive management message with regard to information security priorities</td>
<td>0.805461 0.348188</td>
<td></td>
</tr>
<tr>
<td>Inability to cost-justify information security</td>
<td>0.736228 0.498344</td>
<td></td>
</tr>
<tr>
<td>Failure of applying generally accepted information security best practices/metrics</td>
<td>0.824163 -0.14342</td>
<td></td>
</tr>
</tbody>
</table>

Source: Author

4.3 Factor Isolation

Isolation of factors involves isolating each factor based on the factor loading. These are the relationships between the factors and the factors encountered. The compositions of the two factors shown in Table 4.9 are presented as follows:

Factor 1: consists of 8 items. These items are numbered 1, 2, 3, 4, 5, 6, 7, and 8. These items are associated with information system issues hence can therefore be treated as information based challenges.

Factor 2: consists of 5 items. These are represented by item numbered 9 through to 13. The items address issues of cost and finances in implementation of information system security.
CHAPTER FIVE: SUMMARY OF FINDINGS, DISCUSSION, CONCLUSIONS AND RECOMMENDATION

Introduction
The general objective of the study was to undertake an evaluation of security of information systems in the Kenyan banking industry with the aim of

i. Identifying information security systems and practices.

ii. Establishing the benefits of implementing information systems security.

iii. Analyzing challenges in implementation of information systems security in the banking industry in Kenya.

This chapter presents a summary and conclusions derived from the findings in the previous chapter. The purpose of these conclusions is to answer the research questions. Finally, recommendations for management, and suggestion for future study are presented.

5.2 Summary and Discussions of the findings
Most of the banks captured in the survey had been in operation for a period of over 30 years. The study revealed that 62 percent of the banks interviewed were locally owned with 29 percent foreign owned. Only 9 percent were both locally and foreign owned.

In addition, the study also revealed that majority of the banks had less than 50 branches, 70 percent, with 51 percent having 51 to 100 branches. Only 9 percent had over 100 branches.

Majority of the banks were located within Kenya, 56 percent with 21 percent specifically located within Nairobi. 21 percent were within East and Central Africa while 3 percent were globally located. On information technology, 68 percent of the interviewed banks had very high dependence on IT; with 29 percent having a high dependence on IT. 2 percent gave no comment.

Majority of the interviewed banks did not have an overall security officer (56 percent) while 46 percent had an overall security officer. In addition, majority of the banks highly utilized firewalls, (62 percent) and Intrusion detection systems (47 percent). 35 percent had moderately utilized Intrusion prevention systems and Security awareness and training programs.

The study also found out that majority of the banks agreed that they needed to ensure that there is firm foundation for efficient and effective risk management (65 percent), closely followed by 47
percent who also strongly agreed that information security lead to improved trust in customer relationship, 38 percent agreed that information security lead to increase in predictability and reduced uncertainty of business operation

In conclusion, 18 percent agreed that lack of consistent enforcement of information security within the organisation hierarchy was a challenge. In addition, Lack of integration between the business and information security was a moderate challenge among 38 percent of the respondents while, failure of applying generally accepted information security best practice was a low extent challenge among 27 percent amongst the respondents.

Banks must preserve their image and reputation to guarantee their credibility in the eyes of the public as “custodians” of the information concerning financial markets and entities. The information security function shares the responsibility in the conception and study of feasibility and the development and implementation of an application. Both the security and continuity must be periodically tested to ensure their effectiveness; in this respect, the control areas of different organizations can help by verifying the effectiveness of the measures implemented.

It is necessary to guarantee information protection in any form of electronic or other kind of support and have information security committees in which all the departments or at least those considered to be critical for the strategic functions of the bank are represented. It is also necessary to implement an institutional information security management system because the different departments must be considered as proprietors of their information, and therefore responsible for its security.

The information must be classified, but each organization will decide on the most suitable form of classification. In some cases three levels are used: confidentiality, availability and, in some central banks, asset classification. Nevertheless, although there is no single pattern, it is essential to have one classification. Management of more than three levels is very complicated and could lead to failure.
Information security

Information system security is the application of managerial and administrative procedures and technical and physical safeguards to ensure not only the confidentiality, integrity and availability of information which is processed by an information system, but also of the information system itself, together with its environment. Such procedures and safeguards not only need to deter and delay improper access to information systems, they must also ensure that any improper access is detected; that is, individuals have to be made accountable for their actions.

5.3 Conclusion and Recommendations

Cyber-crime cases in the region led to blacklisting the countries, thus inhibiting e-commerce development. Banks need coordination, concrete action and strengthening capacities of relevant institutions in order to decrease computer crime influence and to improve the negative image. Employee awareness should also be raised that building a firm information system is not an IT experts' job, but that all employees are responsible for this process. The necessary mainstreaming of information systems is aided by using clear, unambiguous and non-technical terminology in the process of policy creation.

IT Security

The study recommended that banks should have a strong information security system to curb any of risks associated with threats to the information arising directly or indirectly from human error or deliberate subversion. An Information Security Management System (ISMS) is a systematic approach to managing sensitive company information so that it remains secure. It encompasses people, processes and IT systems.

The establishment of a decentralized information security administration is recommended in banks. That is, involving the persons in charge of the department that are proprietors of the information in the administration of their systems' security. To this end, they should be furnished with user-friendly information tools, given courses in the good use of administration and the total support of the IT department.

Information security officer (ISO)

In addition, the study also recommended that banks and other financial related institutions should
Recruit an overall security officer in charge of information security. An ISO (information officer) is in charge of setting up of a sound information security program. He/she also plays a critical role in informing, advising, and alerting the general management on matters regarding information security. The ISO's duties are essentially managerial, and entail recruiting engineers and operations technicians, whose work he/she organizes and controls.

**Competent security systems**

The study went further to advice that banks need to encompass competent security systems that reduce the likelihood of violation of privacy providing greater confidence when interacting with business partners and protects the bank from loss of customers and business revenue through loss of employee productivity and inability to meet business requirements. The study also recommended the use of external services e.g. consultancies to promote security initiatives. The system function (internal and external) is also valuable for security, although its action will be a posteriori.

**Limitation of the Study**

The study only covered evaluation of information security in the banking industry. The study never did not cover areas such as components of information security. In addition, the study did not disclose information security on risk management which is effective in recognizing the use of information and defining appropriate procedures and protection requirements for the organization. The study was also limited in its evaluation of threats and vulnerabilities that the organization faces.

**Suggestions of further Study**

The study has done an evaluation of information security in the banking industry; this study can be extended to other sectors of the economy. Further there is need to undertake an in-depth search what these sectors are doing to mitigate the challenges in the implementation of information security. Further research should also be done on whether information security in enterprise risk management has an impact on the share value of a company. The study also proposes that research be done on the success of Information Security Management Systems (ISMS) in ensuring confidentiality, integrity and availability of organization’s information.
REFERENCES


Dear Respondent,

I am a post graduate student at University of Nairobi pursuing a course in Masters of Business Administration (MBA), specializing in Management Information Systems. In Partial fulfillment of the course requirements, I am undertaking an evaluation of Security of Information Systems in the Kenyan Banking Industry.

Your bank has been selected to participate in the study and therefore you have been selected as one of the respondents. I therefore kindly request you to fill the attached questionnaire. The information from the questionnaire is needed purely for academic research purposes and will be treated with utmost confidentiality. A copy of the final report can be made available to you upon request. If you require any further information, please do not hesitate to contact me on cell phone number +254 722 520423

Your cooperation is highly appreciated.

Thank you in advance

Yours faithfully,

Peter Muraya Kiemo

D61/P/7709/05
Appendix 2

Please fill in the Questionnaire provided

SECTION A: Organization’s details

For each of the question below, please tick the appropriate one.

1. How can long has your bank been in operation in Kenya?
   a) 0-10 years  [ ]
   b) 11-20 years  [ ]
   c) 21-30 years  [ ]
   d) Over 30 years  [ ]

2. How can you describe the ownership of your bank?
   a) Locally owned  [ ]
   b) Foreign owned  [ ]
   c) Both locally and foreign owned  [ ]

3. How many employees does your bank employ?
   a) Less than 100  [ ]
   b) 101-500  [ ]
   c) 501-1000  [ ]
   d) Over 1000  [ ]

4. How many branches does your bank have?
   a) Less than 50  [ ]
   b) 51-100  [ ]
   c) Over 100  [ ]

5. What is the spread of your bank’s branch network?
   a) Within Nairobi  [ ]
   b) Within Kenya  [ ]
   c) Within East and Central Africa  [ ]
   d) Globally  [ ]
SECTION B: Information Security

6. How do you rate your bank's dependence on IT?
   a) Very High [ ]
   b) High [ ]
   c) Low [ ]
   d) Not at all [ ]

7. How do you rate the level of IT security measures in your bank?
   a) Very High [ ]
   b) High [ ]
   c) Low [ ]
   d) Poor [ ]

8. a) Is there an overall security officer in charge of information security?
    Yes [ ] No [ ]
    b) If Yes, What is his job title, and to whom does this person report to? Please specify.

9. (a) Is there a formal forum for structure to oversee and represent information security in your bank?
    (b) If yes, what is the frequency of meetings?
        Weekly [ ] Monthly [ ] Quarterly [ ] Yearly [ ] Ad hoc [ ]

10. Are comprehensive security awareness programs in place?
    Yes [ ] No [ ]

11. Does the Bank provide regular and structured training to its employees on information security & policy?
    Yes [ ] No [ ]

12. Is there a defined process in place to coordinate the implementation of information security policy, measures and programs?
    Yes [ ] No [ ]

13. Are relevant security requirements and policy specifically defined and documented in your organization?
    Yes [ ] No [ ]
14. Which of the following reflect most your current job profile/title/role?

- Chief Information Officer [  ]
- IT Manager [  ]
- Chief Security Officer [  ]
- Network/Systems Manager [  ]
- Systems Administrator [  ]
- IT Security Officer [  ]
- Other (Please specify) ______________________________

15. Has capability been established that provides specialized information security advice to the organization?
   - Yes [  ]
   - No [  ]

16. (a) Are there specific key performance indicators or metrics in place to measure the success of and compliance with security policy in your bank?
   (b) If yes, what are those key performance indicators? Please specify.

---

SECTION B: Information Security Systems

17. On a scale of 1 to 5, indicate the key information security systems programs utilized in your bank to secure information.

1= Lowest utilization and 5= highest utilization

<table>
<thead>
<tr>
<th>Systems</th>
<th>Degree of Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies, procedures and guidelines</td>
<td>5 4 3 2 1</td>
</tr>
<tr>
<td>Data Encryption</td>
<td></td>
</tr>
<tr>
<td>Firewalls</td>
<td></td>
</tr>
<tr>
<td>Intrusion Detection Systems</td>
<td></td>
</tr>
<tr>
<td>Intrusion Protection Systems</td>
<td></td>
</tr>
<tr>
<td>Anti Virus Software</td>
<td></td>
</tr>
<tr>
<td>User Awareness training programs</td>
<td></td>
</tr>
<tr>
<td>User Authentication Systems/ logical Access Controls (username &amp; password, biometrics, tokens)</td>
<td></td>
</tr>
<tr>
<td>Incident management process</td>
<td></td>
</tr>
</tbody>
</table>
SECTIONS C: Benefits of Implementation of Information Security

18. To what extent do you agree with the following statements as benefits of implementation of information security in your bank?

<table>
<thead>
<tr>
<th>Statement</th>
<th>Strongly agree</th>
<th>Agree</th>
<th>Neutral</th>
<th>Disagree</th>
<th>Strongly disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protects the bank from civil and legal liability as a result of information inaccuracy or the absence of due care</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increases predictability and reduces uncertainty of business operations by lowering information security-related risks to definable and acceptable levels</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>May lead to increased share value as a result of practice good information security governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensures that reputation of your bank is protected</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensures that there is firm foundation for efficient and effective risk management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increases level of assurance that critical decisions are not based on faulty information.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Leads improved trust in customer relationships</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decreases likelihood of violation of privacy providing greater confidence when interacting with trading partners</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables new and better ways to process electronic transactions thus reducing operational costs by providing predictable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
outcomes and mitigating risk factors that may interrupt the process

Protects the bank from loss of customers and business revenue through loss of employee productivity and inability to meet business requirements

Enables banks to have a competitive advantage over their competitors

SECTION C: Challenges in Implementation of Information System Security

To what extent do the following factors pose as challenges in implementation of information systems security?

5= highest  1=Lowest

19. Lack of senior management commitment to information security initiatives
   5 | 4 | 3 | 2 | 1

20. Failure of management to understand the information security issues,
   5 | 4 | 3 | 2 | 1

21. Lack of information security planning prior to implementation of new technologies,
   5 | 4 | 3 | 2 | 1

22. Lack of Integration between business and information security
   5 | 4 | 3 | 2 | 1

23. Lack of alignment of information security with the organization’s objectives,
   5 | 4 | 3 | 2 | 1

24. Lack of executive and line management ownership and accountability for implementing, monitoring and reporting on information security
   5 | 4 | 3 | 2 | 1

25. Lack of appropriate employee education and awareness on information asset protection
   5 | 4 | 3 | 2 | 1

26. Lack of consistent enforcement of information security policies and standard
   5 | 4 | 3 | 2 | 1

27. Low placement of information security within the organization hierarchy

58
28. Lack of budget for information security strategy and tactical plan
5 [ ]  4 [ ]  3 [ ]  2 [ ]  1 [ ]

29. Lack of consistent board/executive management message with regard to information security priorities
5 [ ]  4 [ ]  3 [ ]  2 [ ]  1 [ ]

30. Inability to cost-justify information security
5 [ ]  4 [ ]  3 [ ]  2 [ ]  1 [ ]

31. Failure of applying generally accepted information security best practices/metrics.
5 [ ]  4 [ ]  3 [ ]  2 [ ]  1 [ ]

32. Please provide any other additional information that you feel is important in this research that regards information security in the Kenyan banking industry.

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

Thank you for taking time to fill the questionnaire, your participation is highly appreciate
Appendix 3

Banks in Kenya

1. ABC Bank (Kenya)
2. Bank of Africa
3. Bank of Baroda
4. Bank of India
5. Barclays Bank
6. CFC-Stanbic Bank
7. Charterhouse Bank
8. Chase Bank
9. Citibank
10. City Finance Bank
11. Co-operative Bank of Kenya
12. Commercial Bank of Africa
13. Consolidated Bank of Kenya
14. Credit Bank
15. Development Bank of Kenya
16. Diamond Trust Bank
17. Dubai Bank
18. Ecobank
19. Equatorial Commercial Bank
20. Equity Bank
21. Family Bank
22. Fidelity Commercial Bank
23. Fina Bank
24. Giro Commercial Bank
25. Guardian Bank
26. Habib Bank A.G Zurich
27. Habib Bank
28. Housing Finance
29. Imperial Bank
30. Investment & Mortgages Bank
31. K-Rep Bank
32. Kenya Commercial Bank
33. Middle East Bank
34. National Bank of Kenya
35. NIC Bank
36. Oriental Commercial Bank
37. Paramount Universal Bank
38. Prime Bank
39. Prime Capital and Credit Finance Bank
40. South Arabian bank
41. Savings and Loan Bank
42. Southern Credit Banking Corporation
43. Standard Chartered Bank
44. Transnational Bank
45. United Bank for Africa
46. Victoria Commercial Bank