EXTENT TO WHICH TECHNOLOGY RISKS AFFECT INFORMATION TECHNOLOGY AS A COMPETITIVE TOOL IN THE BANKING INDUSTRY IN KENYA

BY

ONGORI WYCLIFFE MOMANYI

A RESEARCH PROJECT SUBMITTED TO SCHOOL OF BUSINESS IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF MASTERS OF BUSINESS ADMINISTRATION, UNIVERSITY OF NAIROBI

NOVEMBER 2012

DECLARATION

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

Signed ..... Date 14/11/2012

Ongori Wycliffe Momanyi

D61/70614//2007

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

Signed ..... Date 15/11/2012

Dr. James Gathungu

Department of Business Administration

School of Business

University of Nairobi

DEDICATION

This research project is dedicated to my family for their inspiration, encouragement, understanding and prayers towards the successful completion of this course. I pay glowing tribute and gratitude to the Almighty God who has given me the wisdom to undertake this course.

ACKNOWLEDGEMENTS

My special and sincere thanks go to my supervisor Dr. J. Gathungu and moderator Mr. Kagwe, for their guidance, support, suggestions, useful comments and constructive critique which were all instrumental to the successful completion of this research project. I also wish to appreciate the support and encouragement from my wife Fridah Nyangara and my children Matthew Momanyi and Isabelle Momanyi during the tough time that I had to balance between the demands of a rigorous academic program and an equally demanding work environment and family obligations. My gratitude to God Almighty who renewed my strength at every single stage of this study.

God bless you all.

TABLE OF CONTENTS

LIST OF TABLES

ABSTRACT

The study sought to establish the extent to which technology risks affect Information Technology as a competitive tool in the banking industry in Kenya. Towards the achievement of the objectives, the study adopted a descriptive research design in which involved distribution of questionnaire to the banks. A good response rate of 79% was realized. The study also established a regression and correlation analysis between the dependent variable and the independent variables.

The findings of the study was that banks in Kenya have adopted the use of Information Technology as a competitive tool for various functions namely email, clearing, core banking, m-banking, internet banking among others, further the research established that indeed technology risks like ATM Skimming, Electronic Funds Transfer, Fake e-mails, Viruses, Keyloggers, Denial of Service among others do affect technology as a competitive tool as banks have lost about substantial amounts in the last five years.

The research also found out that banks in Kenya have created functions specifically dealing in addressing or tackling the technology based risks by having electronic investigative capabilities within their audit, security and forensicdepartments. The banks also use external consultants and ultimately the banking fraud investigations unit within the Central Bank for investigations and subsequent prosecution.

CHAPTER ONE: INTRODUCTION

1.1 Background of the study

Globalized markets are breeding ground for conglomeration where mergers and acquisitions are becoming increasingly popular as a means of growth. For firms to survive, therefore, it has become necessary for them to keep ahead of competitors and predators by differentiating themselves. Creating and sustaining a competitive advantage is one way of achieving this goal. Perreault et. al, (1987) explains that competitive advantage means that a firm has a marketing mix that the target market sees as better than a competitor's mix. This competitive advantage, he argues may result from efforts in different areas of the firm such as cost cutting in production, innovative research and development, more effective purchasing of needed components or financing for a new distribution facility(Kimani,2006).

Strategically successful organizations obtain market feedback continuously and rapidly and adapt to the feedback ahead of their rivals. They exploit the potential strategy as well as competitive and operating information systems (Gilbert, 1995). Some of the information technology variables that can influence a firm's response to competition include the usage of real-time systems, extent of connectivity of distribution channels, as well as the efficiency of the telecommunication systems (Kimani, 2006). In fast-moving competitive environments, sustaining competitive advantage involves creating safe-havens from cutthroat competition by continuously creating gaps through unique resources that cannot be easily imitated.

1.1.1 Risks in Information Technology

Unlike the previous mainframe environment that was much a "closed" environment, the internet was designed to be open and approachable, with control and trust resting with the users (Wasilwa, 2003). With the digital nature of the internet, there are no physical or geographic locations or boundaries. In the early days of computer systems development some sense of security was derived from the fact that a great deal of specialized knowledge and expensive equipment were required to penetrate computer systems according to Wilk (1983). This is not the same in today's rapidly advancing technological world. We can no longer use technical complexity to shield organizations' computer systems from manipulation of unauthorized access.

As computers become more pervasive in every field of human activity, the security of information stored on the computer becomes a societal concern. The potential for abuse has multiplied significantly in a networked environment wherein physical proximity to a computer is no longer a requirement for operating the computer, all that is needed is a connection to the machine over some combination of public and private networks (Amit Das, 1997). There has been a tendency to believe that information held within a computer is secure by virtue of its great mass and by the peculiar nature of the media upon which it is stored. Wasilwa (2003) notes that this may have been true of the past when knowledge of computers was restricted and when computers were few and far between. The rapid growth of knowledge about computers and subsequently information technology, their proliferation and the development of freely available software make this belief no longer true.

1.1.2 Information Technology

According to Porter (1985), technological change, especially IT, is amongst the most important forces that can alter the rules of competition. This is because most activities of an organization generate and utilize information. Porter and Millar (1985) contend that IT can also create new businesses from within a company's existing activities. McFarlan et al (1983) contribute that IT offers a scope for product differentiation that enables the company to effectively service the needs of the market niche. In this age of connectivity, customers are getting extremely tech-savvy and demanding. Every day they are exposed to glut of information. In this scenario, financial institutions are forced to get more customer focused, improve customer service and offer innovative products to meet the requirement of their customers. (Wasilwa, 2003).

According to (Dimitris, 1998), successful financial institutions need applications that can address the key issues of this exciting electronic age (e-age) namely invest in a platform that can offer innovative products to meet customer requirements, enable interface with the multiple delivery channels in an integrated manner to ensure 24x7x365 service levels, be agile enough to respond to any market requirement and competition quickly, inter-operate with other business applications on a real time basis, embrace new generation architecture, safeguard IT investments and empower employees in becoming knowledgeable workers, allow financial institutions to take full advantage of the e-commerce revolution, be complete in design and functionality rich and have a sophisticated multi-level security to minimize the risks of unauthorized use of data and illegal access (Financial newsletter, 2002).

1.1.3 Competitive Advantage

The way a firm views its businesses, customers and competition is critical to successfully aligning its business and IT strategy. IT is used to automate processes and to augment the skills of the organization's staff (Luftman, 1996). Competitive advantage can result either from implementing value-creating strategy not simultaneously being implemented by any current or potential competitors (Barney et al, 1989) or through superior execution of the same strategy as competitors. (Schendel et al, 1978) described competitive advantage as "the unique position an organization develops vis-à-vis its competitors".

Competitive advantage is mainly derived from resources and capabilities. Resources have been termed as "assets", "strengths and weaknesses" and "stocks of available factors" (Shoemakers et. al 1993; Wernerfelt, 1984). The capabilities of the firm are what it can do as a result of teams of resources working together. Competitive advantage does not only come from being different, it is also achieved if and when real value is added to customers. This often requires companies to stretch their resources to achieve higher returns (Prahalad et. al, 1993; Kimani, 2006). A Competitive Advantage is an advantage gained over competitors by offering customers greater value, either through lower prices or by providing additional benefits and services that justify similar or possibly higher prices.

1.1.4 The Banking Industry in Kenya

The banking industry in Kenya is governed and regulated by the companies Act, the Central Bank of Kenya Act CAP 491 and the Banking Act CAP 488. These Acts are used

together with prudential guidelines issued by the Central Bank of Kenya from time to time to regulate how banks in Kenya operate. The Kenyan Banking industry was liberalized in 1995 and the effect was lifting of controls (Banking Act Chapter 488, 2011; Central Bank of Kenya Act Chapter 491, 2011; Central Bank of Kenya Prudential Guidelines, 2006; Banking in Kenya, 2012).

The Central Bank of Kenya is tasked with the formulation and implementation of monetary policy directed to achieving and maintaining stability in the general level of prices, foster the liquidity, solvency and proper functioning of a stable market-based financial system, support the economic policy of the Government, including its objectives for growth and employment. Further, Central Bank's subsidiary mandate includes to formulate and implement foreign exchange policy, hold and manage its foreign exchange reserves, license and supervise authorized dealers, formulate and implement such policies as best to promote the establishment regulation and supervision of efficient and effective payment, clearing and settlement systems, act as banker and adviser to, and as fiscal agent of the Government, and issue currency notes and coins.

1.2 Research Problem

Financial Institutions have been at the forefront in adoption of the use of Information Technology as a competitive tool, this is evidenced by the use of ATM machines, Mobile phones for banking purposes, Internet banking etc. Many banking customers in the developed world have enjoyed the convenience of home banking as well as phone banking (Wasilwa, 2003). Rayport and Sviokla (1995), state that competition is defined

along two dimensions; the physical world of resources and a virtual world of information. Information supports and enhances every activity in the organization, and it can itself be a source of added value and hence competitive advantage, provided organizations are able to draw that value.

Financial institutions in Kenya adapted to the use of Information Technology as a competitive tool for some time now. Whereas this scenario seems ideal, there are inherent risks with the use of technology that had not been strategically assessed at adoption. Some of the risks have resulted in huge losses despite having elaborate policies and procedures in place. This research therefore seeks to answer the following question:, do technology risks affect the use of Information Technology as a competitive tool in the banking industry in Kenya, if so to what extent?

1.3 Research Objectives

The objectives of this study are to establish:

i) the extent to which Information Technology is used as a competitive tool in banking institutions in Kenya;

ii) the extent to which technology risks affect the use of information technology as a competitive tool in the banking industry in Kenya;

iii) the various approaches banks in Kenya have taken to mitigate technology risks.

1.4 Value of the study

The study will add to the existing body of knowledge by highlighting the various risks associated with information technology and how to avoid the hurdles associated with the Information Technology related risks to reap maximum benefits.

The study will further contribute to the industry players and the regulator, Central Bank of Kenya, on the challenges faced by banking institutions in their quest to use Information Technology as a competitive tool and the mitigation strategies they have employed.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This chapter presents the literature review of technology risks, information technology, competitiveness and competitive advantage in the banking industry and technology frauds.

2.2 Technology Risks

Application vendors develop their systems with the primary purpose of meeting the customers' requirements, Computer security being considered the last area of concern / priority. The users on the other hand measure the affectability of a system by establishing how easy it is to manipulate, user friendly screens and availability without assessing the security aspects of the system. Thus a good system to the vendor is what can satisfy the end user processing / transaction requirements while a good system to the end user is how user friendly it is and whether it can address their day-to-day operations. Banks that used to operate legacy systems were not prone to security threats, as the new systems that have come in to replace them have very vulnerable risks. This made most of the users within the Banking industry who still operate within the mainframe environments to assume the security aspect of systems and imagined that any system was above any kind of threat or attack (Chorafas, 1998). The banking industry should be aware of the security issues that affect the competitiveness of IT as "Passwords", "Software Flaws", Inattention to Security (i.e. Lack of Awareness), "Content Management" and "Access Control". IT

savvy fraudsters, exploit these flaws to their advantage to circumvent the controls that have been put in place and perpetrate frauds.

The greatest asset of the internet, which is its openness, also presents at the same time the biggest risk to security for both companies and customers. Since information about commercial of financial transactions passes through many computers, where it is captured, monitored and stored and processed, e-business ventures are particularly susceptible to outside penetration. Numerous problems include stolen credit card details. These threats in the online environment are similar to those in the offline world; they include burglary, breaking and entering, embezzlement, trespass, malicious destruction and vandalism. Some of the most prominent security threats that e-business companies and their customers face today include, malicious code refers to security threats such as viruses, worms or Trojan horses, phishing refers to deceptive attempts by third parties to obtain financial information from financial gain, phishing does not involve malicious code but instead relies on misrepresentation and fraud. One well-known example of a phishing attack is the email from a rich uncle in Nigeria who is seeking a bank account to store millions of dollars for a short time. In return, he is willing to give you a few hundred thousand dollars. Some people are fooled and provide their bank account information (Jelassi and Enders 2008).

Hacking and cyber-vandalism refer to acts committed by individuals who attempt to gain unauthorized access to a computer system. They do so by finding weaknesses in the security procedures of websites and computer systems, credit card fraud is one of the

most feared occurrences on the internet. This fear prevents many users from providing their credit card information online. In reality, however, this type of fraud is much lower than what users think, since it represents less than 2% of all online card transactions (Jelassi and Enders 2008).

Spoofing or pharming takes place when hackers misrepresent their true identity or misrepresent themselves by using fake e-mail addresses. When a hacker spoofs a website, it is called pharming, which involves redirecting a web link different from the intended one. Once an unknowing user has been redirected to the fake website, hackers then collect and process orders, effectively stealing business from the real site (Jelassi and Enders 2008).

Denial of Service (DOS) refers to large scale e-mail attacks on websites with useless traffic. The goal of these e-mail floods is to shut down websites. When they succeed, the costs for the affected website operator are substantial, since, while the site is shut down, customers cannot inform themselves through the site and, more importantly, they also cannot make purchases. For instance, in April 2007 a series of DOS attacks disrupted Estonia's most vital websites of the president, the parliament, almost all of the government ministries, two of the biggest banks and firms specializing in communication. The government had to take emergency measures and block access to the websites from the outside world, which resulted in substantial economic losses. There are a number of different ways to protect against security threats. These include, on the one hand, technological measures such as encryption, firewalls or virtual private

networks (VPNs). On the other hand, companies can also implement procedures and policies to limit the danger of outside attacks on their systems. These measures include clear online authentication and authorization for users of the system and conducting routine reviews of access that identify how outsiders are using the website (Jelassi and Enders 2008).

2.3 Information Technology

Passwords are in many cases, the first and last line of defense. Often, passwords are not changed frequently, are shared between users on a common desktop computer or are displayed in easy-to-see places such as on the computer itself. These habits, while perhaps more on a day-to-day basis, create more security threats and attack risks for the organizations. Network administration software and security vulnerability products like Lopht that can scan all passwords for common words or easy to break codes, identify inactive log-on and alert administrators as to which passwords have not been used and or updated. This can act as another layer of password security insurance and can keep possible security holes closed (Wasilwa, 2003).

Known software flaws are perhaps the most preventable security risks and those often overlooked by organizations in their quest to strengthen their networks. Each year security teams, security institutes and software companies issue hundreds of alerts and patches for these known flaws. Microsoft is known to release patches on a regular basis which focus on security vulnerability and system stability. If the said patches are not well implemented or not implemented at all could cause the system to suffer losses as a result

of vulnerability and instability. Security holes in software can have a negative impact on business. With a single breach, a malicious intruder can change and or install malicious software that can enable them gain access and fraudulently post fraudulent transactions to accounts belonging to accomplices; needless to say such events can affect banks reputation (Wasilwa, 2003).

While the alerts raise awareness for banking organizations, they also raise red flags for hackers and people who can then use the identified vulnerabilities to access networks. Therefore, patches must be applied to correct bugs, flaws and security holes. Additionally, patches must be updated and organizations must continuously scan their networks for these flaws.

General Inattention to Security or lack of awareness, while it is hard to imagine that any organization could ignore security, it's not hard to understand why security is often pushed to the periphery as continued "uptime" is essential as "downtime" could mean losses of millions of shillings, and loss in confidence by their customers thus losing their competitiveness, therefore organizations are focused on keeping systems running. Serious organizations that focus on security can help increase this "uptime" as a safer system will be more secure when up against hackers, viruses and bugs. Again, software programs that continuously scan systems or that automate queries and automatically generate reports can help organizations by cutting down on the time it takes to tend to system security.

Content Management, many IT professionals pay attention only to the security of the core system, thus giving little consideration about how the outputs of those systems are stored and managed. Storage of an output from a core banking system which is subsequently stored in a spreadsheet format would be a classic example as the security around the spreadsheets is not as thorough as for the core banking system.

Access Control, whereby a manager of a unit is given more rights due to his or her position in the organizations hierarchy whereas in actual sense requires very minimal access rights and further lacks the requisite security knowledge. This becomes dangerous when the manager decides to be adventurous or cause some damage to the organization's data as the access granted allows him to do more damage (Wasilwa, 2003).

2.4 Competitiveness

Competition in business is defined as the "the effort of two or more parties acting independently to secure the business of third party by offering the most favourable terms", seen as the pillar of capitalism in that it may stimulate innovation, encourage efficiency or drive down prices, competition is routed as foundation upon which capitalism is justified (Kohn A., 1985). According to micro economics theory, no system of resource allocation is more efficient than pure competition. Competition, according to theory, causes commercial firms to develop new products, services and technology. This gives consumer greater selection and better products.

Superior performance can be achieved in competitive industry through the pursuit of a generic strategy which is defined as the development of an overall cost leadership, differentiation or focus approach to industry (Porter 1980, 1985). Competitive methods consist of skills and resources that are available for use by firms in competitive industry. Superior skills in terms of staff capability, systems or marketing savvy not possessed by competitors. A superior resource is defined in terms of physical resources that are available to help strategic implementation according (Day and Wesley, 1988).

2.5 Competitive Advantage

The key for survival in the global market for a service firm is to offer a service that is in some way superior to its competition. Besides, it must be sustainable over time. This concept is known as sustainable competitive advantage (Clow, et. al, 1999, Kimani2006). Clow et al (1999) highlight four requirements for a competitive advantage to qualify to be sustainable: the concept must be valued by customers as to result to additional sales, it must not be substitutable, the firm must have the resources and capability of delivering sustainable competitive advantage to customers and finally, it must not be easily copied by customers.

Schendel (1978) further argues that the extent of the return a firm can obtain from a competitive advantage, however, depends upon the sustainability of the competitive advantage, which the resources and capabilities confer upon the firm. The term "competitive advantage" has traditionally been described in terms of the attributes and

resources of an organization that allow it to outperform others in the same industry or product market (Fahey, et. al, 1984; Kay, 1994; Porter, 1980).

2.6 Technology Frauds

Banks in Kenya are today facing a lot of challenges in dealing with both internal and external fraud cases that often come up and are related to the risks mentioned above. Statistics from the Banking Fraud Investigating Unit of Central Bank of Kenya, indicate that in the year 2010, banks, up to the third quarter, had suffered fraud related to transfers using the electronic channels amounting to Kshs. 700 million whereas up to Kshs. 240 million was lost in the same period in 2011. We can deduce that the said frauds will only continue to grow as various channels in the electronic frontier continue being adopted by banks. Development in technology has highly contributed to this sad state of affairs.

Other than affecting the bank's profitability, fraud also impacts negatively on an organization's reputation and competitiveness. There is therefore need for banks to respond appropriately to these challenges. Organizations must continually review and improve their internal controls as the primary defense against fraud and abuse. This involves establishment of structures that have the capacity to pick potential frauds proactively, a fraud management system (FMS) is an example. Effective controls warn potential fraudsters that management is actively monitoring the business and that in turn deters fraud.

In today's technological age, fraud has become very complicated and increasingly difficult to detect especially when it is collusive in nature and committed by top management who are capable of concealing it. Consequently, auditors have argued that the detection of fraud should not be their responsibility. Two matters analyzed by (Baker, 1999) with significant potential for misleading and fraudulent practices and the issue of fraud on the internet: they are securities fraud on the internet, especially activities that violate security laws like stock price manipulation and non-existent products; and fraud arising from the rapid growth of internet companies that lacked traditional management and internal controls.

Digital technologies play an important role in the daily activities of the public now-d-days. Benefits can be derived from digital technologies as the governments can deliver services electronically to everyone (Spira and Page, 2003). Russell stressed how the developments of delivering services electronically by governments led to improper use and how the growing use of computer technologies by government agencies created additional challenges of illegal and fraudulent conduct.

Computer crime and fraud were more perilous to organizations today. It presented statistics about the growth of fraud, the causes of fraud in the workplace. They elaborated on the common computer frauds; techniques used to commit fraud, the computer based controls, as well as how business assets can be protected. They stated that no one of the organization in the world can be 100 per cent free of risk and assessing an organizations

risk to fraud was not easy. However, the risk could be mitigated by implementing a proper internal control system with good employment practices (Harvey, 1993).

Computer related frauds caused a lot of losses in organizations and it could be avoided if a more serious approach about the prevention and deterrence strategies were taken. Businesses and organizations were trying to cope with the intricacy and mystique that surrounds computer systems. He further stated that it seems that less security was applied to data or information held in computer systems than held in manual systems. Typically, only IT departments were concerned about computer security, but other professionals did not give it the adequate attention to it. He emphasized that more proactive security administration was needed to avoid losses caused by computer fraud (Drummond, 2002).

The rapid rising tide of internet fraud in electronic commerce suggests that frauds grew in conjunction with the expansion of legitimate internet use (Rose and Rose, 2003). The author quoted the report of International Chamber of Commerce's Commercial Crimes Services Division that internet fraud in 2000 was "rising dramatically", more than twice as much as in 1999. The emerging data suggested that the problem of internet fraud was becoming global in scope and impact, as criminals could plan and execute fraudulent schemes from anywhere in the world and victims might be located anywhere in the world. The paper illustrated that the criminal statutes that apply to other types of white collar crime – conspiracy, mail and wire fraud, credit card fraud, securities fraud, money laundering and identity theft – were equally applicable to various forms of internet fraud.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents a discussion of the research methodology which will be used in the study. It discusses the research design identifying the population of study, sample and data collection methods as well as data analysis.

3.2 Research design

Research is defined as the process of arriving at a dependable solution to a problem through planned and systematic collection analysis and interpretation of data. The research methodology highlights the overall approach to be taken in the research in terms of research design, data collection respondents, and data collection procedure and data analysis.

This will be a census study. The major purpose of the descriptive research design is to describe the state of affairs as it is at present. It is a process of collecting data in order to test hypotheses or answer questions concerning the current state of affairs of the subjects in the study. The purpose of a descriptive research is to determine and report the way things are done. The census study is preferred as it will enable us to cover the entire banking industry in the country.

3.3 Population

The population of study will comprise of all banks in Kenya as per the Central Bank of Kenya regulations and are using Information Technology to support their business. The research will be carried out in Nairobi where these banks have their headquarters. It will target ICT Managers, Internal Audit and Investigation departments on account of their knowledge in controls and frauds in the banking industry.

The choice of these companies was based on the strength of their track record of conducting good Banking practices. This is supported by the report from the Banking Fraud Investigations Unit of the Central Bank of Kenya.

3.4 Data Collection

The information will be collected using structured questionnaire to gather primary data. A questionnaire is a set of questions that the interviewer asks that enable the researcher meet specific objectives of the study. The questionnaire will contain both open-ended and close-ended questions. The questions were developed from the study of relevant literature. Audit Managers, Forensic Manager, Security Managers, Information Security Manager and Investigation Managers will be used in the data collection process.

3.5 Data Analysis

Content analysis and description analysis will be used to analyze the responses obtained from the questionnaire and interviews. Kothari (2004) argues that content analysis is a central activity whenever one is concerned with the study of the nature of verbal materials.

The data will then be cross tabulated. After tabulation, the data will then be coded to facilitate statistical analysis. Descriptive statistics such as frequency distribution, percentage tables, pie-charts as well as bar graphs will be used for data presentation. Qualitative data will be presented through narratives.

CHAPTER FOUR: DATA ANALYSIS AND INTERPRETATION

4.1 Introduction

The research objective was to establish the extent to which technological risk affect information technology as a competitive tool in banks in Kenya. This chapter presents the analysis and findings with regard to the objective and discussion of the same. The findings are presented in percentages and frequency distributions, mean and standard deviations. A total of 43 questionnaires were issued out. The completed questionnaires were edited for completeness and consistency of the 43 questionnaires issued, 34 were returned. This represented a response rate of 79%.

4.2 Independent variables, Technology Risks

These are the inherent risks that affect technology leading to frauds, namely Electronic / Swift funds transfer, Fake e-mails, Malicious codes (Viruses), Keyloggers, Internet Banking based frauds (Phishing, Pharming), Denial of Service (DoS) and Remote Access.

Table 4.1: Electronic / Swift Funds Transfer frauds

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	None	5	14.7	14.7	14.7
	1-10	18	52.9	52.9	67.6
	11-20	6	17.6	17.6	85.3
	21-30	4	11.8	11.8	97.1
	More than 30	1	2.9	2.9	100.0
	Total	34	100.0	100.0	

(Researcher data, 2012)

The results from Table 4.1 indicates that 14.7% of the banks in Kenya have not experience Electronic / Swift transfer frauds whereas 52.9% have experienced more than 1 but less than 10 incidents, 17.6% have experienced more than 10 but less than 20 incidents while 11.8% have experienced between 21 and 30 incidents. Only 2.9% have experienced more than 30 incidents.

Table 4.2: Fake E-mails fraud

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	None	11	32.4	32.4	32.4
	1-10	20	58.8	58.8	91.2
	11-20	1	2.9	2.9	94.1
	More than 30	2	5.9	5.9	100.0
	Total	34	100.0	100.0	

(Researcher data, 2012)

The results from Table 4.2 indicates that 32.4% of the banks in Kenya have not experience Fake E-mails fraud whereas 58.8% have experienced more than 1 but less than 10 incidents, 2.9% have experienced more than 10 but less than 20 incidents while 5.9% have experienced more than 30 incidents. This means majority of banks have experienced less than 10 fake E-mails frauds.

Table 4.3: Malicious Codes (Virus) fraud

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	None	18	52.9	52.9	52.9
	1-10	13	38.2	38.2	91.2
	11-20	2	5.9	5.9	97.1
	21-30	1	2.9	2.9	100.0
	Total	34	100.0	100.0	

(Researcher data, 2012)

The results from Table 4.3 indicates that 52.9% of the banks in Kenya have not experienced Virus based frauds whereas 38.2% have experienced more than 1 but less than 10 incidents, 5.9% have experienced more than 10 but less than 20 incidents while 2.9% have experienced more than 30 incidents. This means majority of banks have not experienced Malicious code frauds.

Table 4.4: Keyloggers (Hardware / Software) fraud

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	None	9	26.5	26.5	26.5
	1-10	24	70.6	70.6	97.1
	11-20	1	2.9	2.9	100.0
	Total	34	100.0	100.0	

(Researcher data, 2012)

The results from Table 4.4 indicates that 26.5% of the banks in Kenya have not experienced Keylogger based frauds whereas 70.6% have experienced more than 1 but less than 10 incidents, 2.9% have experienced more than 10 but less than 20 incidents. This means majority of banks have experienced between 1 and 10 Keylogger based frauds.

Table 4.5: Internet Banking Frauds

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	None	25	73.5	73.5	73.5
	1-10	6	17.6	17.6	91.2
	11-20	2	5.9	5.9	97.1
	21-30	1	2.9	2.9	100.0
	Total	34	100.0	100.0	

(Researcher data, 2012)

The results from Table 4.5 indicates that 73.5% of the banks in Kenya have not experienced Internet Banking based frauds whereas 17.6% have experienced more than 1 but less than 10 incidents, 5.9% have experienced more than 10 but less than 20 incidents while 2.9% have experienced more than 30 incidents. This means majority of banks have not experienced Internet Banking based frauds.

Table 4.6: Denial of Service fraud

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	None	25	73.5	73.5	73.5
	1-10	8	23.5	23.5	97.1
	11-20	1	2.9	2.9	100.0
	Total	34	100.0	100.0	

(Researcher data, 2012)

The results from Table 4.6 indicates that 73.59% of the banks in Kenya have not experienced Denial of Service whereas 23.5% have experienced more than 1 but less than 10 incidents, 2.9% have experienced more than 10 but less than 20 incidents. This means majority of banks have not experienced Denial of Service.

Table 4.7: Remote Access fraud

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	None	22	64.7	64.7	64.7
	1-10	9	26.5	26.5	91.2
	11-20	3	8.8	8.8	100.0
	Total	34	100.0	100.0	

(Researcher data, 2012)

The results from Table 4.7 indicates that 64.7% of the banks in Kenya have not experienced Remote Access based frauds whereas 26.5% have experienced more than 1 but less than 10 incidents, 8.8% have experienced more than 10 but less than 20 incidents. This means majority of banks have not experienced Remote Access based frauds.

4.3 Dependent variable, Competitiveness

Competitiveness is captured through repercussions of the incidents brought about by Technology risks that affect Information Technology mostly leading to shutdown / temporary halting of the system and enhanced security procedures and policies.

Table 4.8: Repercussions of the fraud

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Shutdown / Temporary Halt	8	23.5	23.5	23.5
	Enhanced Security & Procedures	26	76.5	76.5	100.0
	Total	34	100.0	100.0	

(Researcher data, 2012)

The results from Table 4.8 indicates that 23.5% of the banks in Kenya experienced risks that led them to Shutdown or Temporarily Halt the System while 76.5% of them Enhanced their Security Procedures and Policies following the risk incidents. The research has found out that in Technological risks in Kenya have not had serious impact leading to shutdown, however, it is expected that this number will increase with the increased usage of technology.

4.4 Regression analysis

Our dependent variable in the model was Repercussions to Competitiveness from Technology risks whose predicators were Electronic / Swift Transfers, Fake e-mails, Malicious codes, Keyloggers, Internet Banking, Denial of Service (DoS) and Remote Access frauds.

Table 4.9: Regression model summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	1.000[a]	1.000	1.000	.00000

(Researcher data, 2012)

The Table 4.9 shows there is a strong correlation between all the Technological Risk factors and the Repercussions on Competitiveness.

Table 4.10: Regression ANOVA Table

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	6.118	6	1.020	.	.000[a]
	Residual	.000	27	.000		
	Total	6.118	33			

(Researcher data, 2012)

Table 4.10 shows that the regression models define the repercussions on competitiveness without influence from the error term (Residual)

Table 4.11: Regression Equation

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.407	.000		4.884E8	.000
	Has your bank experienced Bank frauds - Electronic / Swift Funds Transfer	-.222	.000	-.506	-7.074E7	.000
	Has your bank experienced Bank frauds - Fake E-mails	-.667	.000	-1.465	-1.508E8	.000
	Has your bank experienced Bank frauds - Malicious Codes (Virus)	.593	.000	1.023	1.123E8	.000
	Has your bank experienced Bank frauds - Keyloggers (Hardware / Software)	-.148	.000	-.171	-2.858E7	.000
	Has your bank experienced Bank frauds - Denial of Service	-.556	.000	-.676	-8.568E7	.000
	Has your bank experienced Bank frauds - Remote Access	.815	.000	1.249	1.452E8	.000

(Researcher data, 2012)

4.5 Regression Equation

Repercussions = 3.407 – 0.222 (Electronic / Swift transfer) -0.667 (Fake e-mails) + 0.593 (Malicious Codes) -0.148(Keyloggers) – 0.556(DoS) + 0.815 (Remote Access).

The above model indicates that Electronic, Fake emails, Keyloggers and Denial of Service attacks will most probably lead to shutdown of the system, whereas Malicious codes and Remote Access attack might not necessarily lead to shutdown temporarily halt the system.

The sig column in Table 4.11 indicates that all these factors have a direct impact on the repercussions (competitiveness) of use of technology in banks.

CHAPTER FIVE: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents the summary, conclusions and recommendations from the findings. The overall purpose of the study was to determine the extent to which Information Technology is used as a competitive tool, extent to which technology risks affect the use of Information Technology as a competitive tool and approaches banks in Kenya have taken to mitigate technology risks. From the findings, it was observed that technology risks indeed affect Information Technology as a competitive tool.

5.2 Summary

The study found out that Kenyan banks use information technology as a competitive tool which can be affected by inherent technology risks. Some of the technologies in use include Core Banking Systems, Clearing System, Swift System / RTGS, E-mails, M-banking and Internet Banking, which are prone to various risks which include Electronic / Swift Funds Transfer, Fake e-mails, Malicious codes (Viruses), Keyloggers, Internet Banking, Denial of Service (DoS) and Remote Access.

5.3 Conclusion

Electronic / Swift Transfer frauds affect about 85.3% of the banks, whereas frauds due to Fake e-mails affected 67%. 47% of the banks are affected by frauds due to Malicious codes (Viruses) and 74% of the banks are affected with Keyloggers based frauds. 26% of

the banks were affected by internet banking based frauds this could be due to slow adoption of Internet Banking, though this is expected to grow with the increase adoption of the technology. Denial of Service (DoS) affected 26% of the banks whereas Remote Access based frauds affected 35% of the banks.

The figures indicated could be low due limited knowledge of the risk factors to the correspondents especially on the risks from Denial of Service and Remote Access based frauds, further, banks in the country are unwilling to share information especially around the area of fraud as this affects their reputation negatively.

Banks in Kenya have mitigated the technological risk challenges by establishing various units including Audit, Security, Investigations and Forensic with appropriately skilled personnel.

5.4 Recommendations

The study found out that all have been affected by technological based risks which seem to be investigated mostly by Audit units. These frauds seem to be increasing and changing with diverse technologies which cannot be effectively handled by the Audit units.

This study therefore recommends that banks should establish fully fledged Forensic units to proactively and actively manage the technology based incidents more so at new system installation. Further, bank employees need to be up skilled in the later day technologies

with an eye for risks, as system convenience always seems to take priority during systems Implementation, this can be achieved through issuance of such guidelines by the regulator.

5.5 Limitations of the study

The nature of the data which was collected from respondents who could have been subjective as information about fraud is secretively guarded by banks as it could negatively affect their reputation.

The sample of thirty banks out of a possible 43 further reinforces the opinion of banks being secretive about fraud information, time and resource limitations also affected data collection.

5.6 Suggestions for further Research

The results of this study can be further utilized to suggest several directions for future research. A further study in the area of how Internet Banking frauds affect information technology should be undertaken when its usage reaches maturity in the banking industry.

REFERENCES

Angara, E. A. (2010). *Strategic Responses Adopted by Kenya Commercial Bank to changes in Environment.* Unpublished MBA project, School of Business, University of Nairobi.

Baker, D. R. (1999). *Relationship of Internal Accounting Controls and Occurrences of Computer Fraud,* Nova University: Michigan.

Cheptumo, N. K. (2010). *Response Strategies to Fraud-Related Challenges by Barclays Bank of Kenya.* Unpublished MBA project, School of Business, University of Nairobi.

Chorafas, D. N. (1998). *Cost-effective IT solutions for financial services.* London & Dublin: Lafferty Publications Ltd.

Das, A. (1997). *Determinants of Computer Security Practices:* Nanyang Business School, Nanyang Technical University, Singapore

Day, G.S., & Wensley, R. (1988). Assessing Advantage: A framework for Diagnosing Competitive Superiority, *Journal of Marketing,* Vol. 52, pp. 1-20

Diffu, J. N. (2010). *Strategice Responses to competition by Kenya Commercial Bank Limited in Kenya.* Unpublished MBA project, School of Business, University of Nairobi.

Drumond, H. (2002). *Living in a fool's paradise: the collapse of Barings Bank, Managerial Decision,* Vol. 40 No.3, pp 232-8.

Gilbert, X. (1995). *It's strategy that counts,* Financial Times, Mastering Management Services, No. 7, 8 December.

Harvey, C. (1993). *The role of commercial banking in recovery from economic disaster in Ghana, Tanzania, Uganda, Zambia.* IDS Discussion Paper, No. DP. 325. Brighton: Institute of Development Studies, University of Sussex.

Jelassi, T & Enders A. (2008). *Strategies for e-business – Creating Value Through Electronic and Mobile Commerce. Concepts and Cases (*2nd ed.). England: Prentice Hall

Karuga, C. M. (2010). *A survey on impact of ICT on business value creation in Kenyan Banking Sector.* Unpublished MBA project, School of Business, University of Nairobi.

Kimani, E.W. (2006). *Application of Marketing Information System by Savings and Loan (Kenya) Limited in creating sustainable competitive Advantage.* Unpublished MBA project, School of Business, University of Nairobi.

Kiptugen, E. J. (2003). *Strategic Responses to a changing competitive environment: The case study of Kenya Commercial Bank.* Unpublished MBA project, School of Business, University of Nairobi.

Kohn, A. (1986). *No Contest. The Case against Competition.* New York : Houghton Mifflin.

Kothari, C.R. (1990). *Research Methodology: Methods and Techniques (2nd ed.).* New Delhi: Wishira Prakashan.

Luftman, J. N. (1996). *Competing in the information age: Strategic Alignment in Practice.*,New York: Oxford Printing Press.

Spira, L. F., & Page, M. (2003), Risk Management: the reinvention of internal control and the changing role of internal audit, *Accounting, Auditing & Accountability Journal,* Vol. 16 No. 4, pp. 640-62.

McFarlan, F. W., McKenney, J. L., & and Pyburn, P., (1983), *The Information Archipelago – Plotting a Course,* Havard Business Review, January – February

Porter, M. E (1985). *Competitive Advantage: Creating and Sustaining Superior Performance*. New York: Free Press.

Rayport, J. F & Sviokla, J. J (1995). *Exploiting virtual value chain, Harvard Review, November – December.*

Rose, A. M., & Rose, J. M. (2003). *The effects of risk assessments and a risk analysis decision aid on auditors' evaluation of evidence and judgment, Accounting Forum*, Vol. 27 No.3, pp.312-38.

Wasilwa, O. M. (2003). *A survey of Computer Security Vulnerability in the Banking Industry in Kenya.* Unpublished MBA project, School of Business, University of Nairobi.

Wilk, R. J (1993). *Security and Control of your PC Network.* International Association for Computer Systems Security.

APPENDICES

Appendix 1: Data Collection Checklist

Section A: Respondent Profile

Name of correspondent:_____

Name of department:_____

Job Title:_____

No. of Years on the Job:_____

Section B: About The Bank

1. How many members of staff does your bank have? Tick one

1. Less than 1000 [ ]
2. 1000 – 1999 [ ]
3. 2000 – 2999 [ ]
4. 3000 – 3999 [ ]
5. 4000 – 4999 [ ]
6. More than 5000 [ ]

2. Which of the following control departments do you have in your bank? (Tick as necessary)?

1. Risk [ ]
2. Compliance [ ]
3. Audit [ ]
4. IT Security [ ]

3. How many of the following computing technologies do you have in your bank? (Tick as necessary)

1. Mainframe 0 [ ] 1 – 10 [ ] 11 – 20 [ ] 21 – 30 [ ] More than 30 [ ]
2. Minicomputer 0 [ ] 1 – 10 [ ] 11 – 20 [ ] 21 – 30 [ ]More than 30 [ ]
3. Desktop PC's 0 [ ] 1 – 10 [ ] 11 – 20 [ ] 21 – 30 [ ]More than 30 [ ]
4. Laptop PC's 0 [ ] 1 – 10 [ ] 11 – 20 [ ] 21 – 30 [ ] More than 30 [ ]
5. Notebooks 0 [ ] 1 – 10 [ ] 11 – 20 [ ] 21 – 30 [ ] More than 30 [ ] (/Palms/Ipads/Tablets)

Section C: Information Technology

4. When was your Core Banking System Implemented? (Tick one)?

- 1-2yrs [ ]
- 2-3yrs [ ]
- 4-5yrs [ ]
- 5-10yrs [ ]
- More than 10yrs [ ]

5. Approximately how much (in Kshs) has your bank invested in the Core Banking System? (Tick one)

a) Less than 50 million [ ]

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

c) Less than 150 million but more than 100 million [ ]

d) Less than 200 million but more than 150 million [ ]

e) Less than 250 million but more than 200 million [ ]

f) More than 250 million [ ]

6. What is the level of IT literacy vis-à-vis age in your bank? (Please use the Key)

Key: **1** Very Low **2** Low **3** Average **4**Above Average **5** Excellent

1. 20 – 29 yrs [ ]
2. 30 – 39 yrs [ ]
3. 40 – 49 yrs [ ]
4. 50 – 59 yrs [ ]

7. Does your bank have access to the Internet and World Wide Web?

- Yes [ ]
- No [ ]

8. Does your bank have a written, formal IT Security Policy?

- Yes [ ]
- No [ ]

9. What is the level of IT literacy vis-à-vis jobs hierarchy in the following categories? (Please use the Key)

Key: **1** Very Low **2** Low **3** Average **4** Above Average **5** Excellent

- Board / Executive [ ]
- Senior Management [ ]
- Supervisory [ ]
- Clerical [ ]

10. Which IT systems are in use in your bank? (Tick as necessary)

- Core Banking System [ ]
- Clearing System [ ]
- Swift System [ ]
- E-mail [ ]
- RTGS [ ]
- Firewall [ ]
- CCTV [ ]
- M-banking [ ]
- Internet Banking [ ]
- Others (Please specify)

_____

_____

_____

_____

11. Does the Core Banking System provide access logs? Yes [ ] No [ ]

a) If No, what do you use

_____

_____

_____

_____

_____

b) If yes, can you get access to logs? Yes [ ] No [ ]

i) If No, who has access to the logs?

_____

_____

_____

_____

_____

ii) If yes (you can get access to logs)

iii) Do you need specific rights to access the logs?

Yes [ ] No [ ]

iv) If yes, who assigns the access rights to the logs?

- Database Administrator (DBA) [ ]
- IT Security [ ]
- Business Manager [ ]

12. Are the logs backed up? Yes [ ] No [ ]

i) If yes, whose responsibility is it to backup the logs?

- Database Administrator (DBA) [ ]
- IT Security [ ]
- My Manager [ ]

Section D: Risk & Fraud

13. Has your bank experienced any frauds?

Yes [ ] No [ ]

14. If yes, which kind of frauds has your bank experienced? (Tick as necessary)

TYPOLOGY	NUMBER
1. ATM Skimming	[ ]
2. Credit Card Fraud	[ ]
3. Loans	[ ]
4. Staff Complicity	[ ]
5. Cheque	[ ]
6. Credit Advice Slips	[ ]
7. Electronic / SWIFT Funds Transfer	[ ]
8. Fake E-mails	[ ]
9. Malicious Codes (Viruses)	[ ]
10. Keyloggers (Hardware / Software)	[ ]
11. Internet Banking	[ ]
12. DOS (Denial Of Service)	[ ]
13. Remote Access	[ ]
14. Others (Please specify)	

_____

_____

_____

_____

15. Does your bank have an Investigation Unit?

Yes [ ] No [ ]

16. If yes, please tick the name of unit:

1. Audit Unit [ ]
2. Security Unit [ ]
3. Investigations Unit [ ]
4. Forensic Unit [ ]

17. How many staff does the unit tasked with investigations have? (Tick one)

1. Less than 3 [ ]
2. Less than 5 but more than 3 [ ]
3. Less than 10 but more than 5 [ ]
4. More than 10 [ ]

18. Please indicate the number of staff in your investigation's unit in the following age groups? (Tick as appropriate)

	Age	**Number**
1.	20 – 29yrs	[ ]
2.	30 – 39yrs	[ ]
3.	40 - 49yrs	[ ]
4.	50 – 59yrs	[ ]

19. What number of staff in your investigation's unit are IT literate? (Enumerate as appropriate)

	Age	Number
1.	20 – 29yrs	[ ]
2.	30 – 39yrs	[ ]
3.	40 - 49yrs	[ ]
4.	50 – 59yrs	[ ]

20. Please indicate the percentage of Internal Frauds (i.e. perpetrated by insiders) and External Frauds (i.e. perpetrated by outsiders) experienced in your bank

- Internal Frauds [ ]
- External Frauds [ ]

21. Has your bank experienced Computer / Information Technology related frauds?

Yes [ ] No [ ]

i) If yes, kindly provide the number of incidences in the last 5 yrs as enumerated below

	Typology	Number			
1.	Electronic / SWIFT Funds Transfer	0 [ ] 1 – 10 [ ]	11 – 20 [ ]	21 – 30 [ ]	More than 30 [ ]
2.	Fake E-mails	0 [ ] 1 – 10 [ ]	11 – 20 [ ]	21 – 30 [ ]	More than 30 [ ]
3.	Malicious Codes (Viruses)	0 [ ] 1 – 10 [ ]	11 – 20 [ ]	21 – 30 [ ]	More than 30 [ ]
4.	Keyloggers (Hardware / Software)	0 [ ] 1 – 10 [ ]	11 – 20 [ ]	21 – 30 [ ]	More than 30 [ ]

5. Internet 0 [ ] 1 – 10 [ ] 11 – 20 [ ] 21 – 30 [ ] More than 30 [ ]
   Banking
6. DOS 0 [ ] 1 – 10 [ ] 11 – 20 [ ] 21 – 30 [ ] More than 30 [ ]
   (Denial of Service)
7. Remote Access 0 [ ] 1 – 10 [ ] 11 – 20 [ ] 21 – 30 [ ] More than 30 [ ]

ii) Kindly provide the value in (Kshs) of incidences in the last 5 yrs as enumerated below

A. Less than 1 million
B. Less than 5 million but more than 1 million
C. Less than 10 million but more than 5 million
D. Less than 50 million but more than 10 million
E. Less than 100 million but more than 50 million
F. More than 100 million

(Fill in the options above e.g. A, B etc)

1. Electronic / SWIFT Funds Transfer [ ]
2. Fake E-mails [ ]
3. Malicious Codes (Viruses) [ ]
4. Keyloggers (Hardware / Software) [ ]
5. Internet Banking [ ]
6. DOS (Denial Of Service) [ ]
7. Remote Access [ ]

Section E: Competitiveness

22. What were the repercussions of the fraud (tick as necessary)?

1. Shutdown the particular system [ ]
2. Temporarily halted the system [ ]
3. Enhanced the Security of the particular system [ ]
4. Enhanced procedures and controls [ ]

If the answer above is 1 or 2

23.Who authorized the shutdown or halting of the system (tick as necessary)

1. CEO [ ]
2. IT Manager [ ]
3. Investigators [ ]
4. Auditors [ ]

24. Who investigated the fraud? (tick as necessary)

1. Internal Investigators [ ]
2. External Investigators / Consultants [ ]
3. Banking Fraud Investigators [ ]

25. Which of the following Information Systems (IS) do you currently use in your bank (tick if present)?

1. Transaction Processing Systems (TPS) [ ]
2. Management Information System (MIS) [ ]
3. Decision Support System (DSS) [ ]
4. Executive Information System (ESS) [ ]
5. Fraud Management System (FMS) [ ]

Section F: Attention to Security

	Features	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
26	The IS/IT Manager alert users of any new attack such as viruses from e-mails or malicious / fraudulent codes?	☐	☐	☐	☐	☐
27	Everyone in the bank know what to do in the event of an attack?	☐	☐	☐	☐	☐
28	A policy on the use of personal computers exist?	☐	☐	☐	☐	☐
29	A documented procedure exists for adding or removing network users	☐	☐	☐	☐	☐
30	Vendors do not retain their accounts in the system	☐	☐	☐	☐	☐
31	Pre-employment screening is done regarding the applicant's previous employment, formal education, criminal history, personal financial situation, drugs and alcohol abuse	☐	☐	☐	☐	☐
32	Resigned or terminated employees are removed from system and premises	☐	☐	☐	☐	☐
33	Risk assessments are performed and	☐	☐	☐	☐	☐

	Features	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	documented on a regular basis whenever the system, facilities, or other conditions change					
34	Tests and examinations of Key controls routinely made e.g. network scans, analyses of routers and switches setting, penetration testing	☐	☐	☐	☐	☐
35	Security alerts and security incidents are analysed and remedial action taken	☐	☐	☐	☐	☐
36	Management ensures that corrective actions are effectively implemented	☐	☐	☐	☐	☐
37	Computer users have had formal or informal fraud awareness training	☐	☐	☐	☐	☐
38	Policy forbids using unauthorized or illegally obtained software	☐	☐	☐	☐	☐
39	There exist documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties	☐	☐	☐	☐	☐
40	Login attempts are limited to a specific number of the network users	☐	☐	☐	☐	☐

	Features	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
41	Output to third party applications like Excel, Word and Outlook is discouraged for mission critical systems	☐	☐	☐	☐	☐
42	Access to sensitive areas is controlled via access control and CCTV	☐	☐	☐	☐	☐
43	Sensitive data is encrypted before transmission	☐	☐	☐	☐	☐
44	Passwords unique and difficult to guess (alphanumeric special characters etc)	☐	☐	☐	☐	☐
45	Inactive users disabled after a specific period of time?	☐	☐	☐	☐	☐
46	Access files are restricted to logical view	☐	☐	☐	☐	☐
47	You have deployed protection systems like Firewalls and Intrusion Detection Systems	☐	☐	☐	☐	☐
48	Access to audit logs is strictly controlled.	☐	☐	☐	☐	☐

Appendix II: List of Banks

1. ABC Bank
2. Bank of Africa
3. Bank of Baroda
4. Bank of India
5. Barclays Bank
6. CFC Stanbic Bank
7. Chase Bank
8. Charterhouse Bank
9. Citibank
10. Commercial Bank of Africa
11. Consolidated Bank of Kenya
12. Cooperative Bank of Kenya
13. Credit Bank
14. Development Bank of Kenya
15. Diamond Trust Bank
16. Dubai Bank Kenya
17. Ecobank
18. Equatorial Commercial Bank
19. Equity Bank
20. Family Bank
21. Fidelity Commercial Bank Limited
22. Fina Bank
23. First Community Bank

24. Giro Commercial Bank
25. Guardian Bank
26. Gulf African Bank
27. Habib Bank
28. Habib Bank AG Zurich
29. I&M Bank
30. Imperial Bank Kenya
31. Jamii Bora Bank
32. Kenya Commercial Bank
33. K-Rep Bank
34. Middle East Bank Kenya
35. National Bank of Kenya
36. NIC Bank
37. Oriental Commercial Bank
38. Paramount Universal Bank
39. Prime Bank
40. Standard Chartered Kenya
41. Trans National Bank Kenya
42. United Bank for Africa
43. Victoria Commercial Bank

Source: **Central Bank of Kenya - August 2012**