FACTORS CONTRIBUTING TO OCCURRENCE OF CYBERCRIME ON E-BANKING IN COMMERCIAL BANKS IN KENYA

BY

MARYANNE NYAMBURA MWAI

UNITED STATES INTERNATIONAL UNIVERSITY

SUMMER 2015
FACTORS CONTRIBUTING TO OCCURRENCE OF CYBERCRIME ON E-BANKING IN COMMERCIAL BANKS IN KENYA

BY

MARYANNE NYAMBURA MWAI

615648

A Research Project Report Submitted to the Chandaria School of Business in Partial Fulfillment of the Requirement for the Degree of Masters in Business Administration (MBA)

UNITED STATES INTERNATIONAL UNIVERSITY

SUMMER 2015
STUDENT DECLARATION

I, the undersigned, declare that this is my original work and has not been submitted to any other college, Institution or university other than the United States International University in Nairobi for Academic Credit.

Signed--------------------------------------- Date--------------------------------------

Maryanne Mwai (ID: 615648)

This project has been presented for examination with my approval as the appointed supervisor

Signed--------------------------------------- Date--------------------------------------

Mr. D. Ndirangu

Signed--------------------------------------- Date--------------------------------------

Dean, Chandaria School of Business
COPYRIGHT

This project has been submitted in partial fulfillment of requirement of degree of Masters in Business Administration at United states International University (USIU). All rights Reserved. This Material can be used for scholarly purposes. Any commercial use of whatever kind is prohibited.
ABSTRACT

The purpose of the study was to investigate the factors contributing to occurrence of Cybercrime on the E-Banking Industry in Commercial Banks in Kenya. The study addressed the following objectives:

i. To determine the level of cyber security on commercial banks in Kenya.

ii. To assess the effectiveness of existing regulation on cybercrimes in Kenya.

iii. To determine how employee awareness and competence influences occurrence of cybercrimes in commercial banks in Kenya.

The research design used was descriptive. The results showed data was collected from 41 ICT experts. To select the respondents for this study, random sampling technique was used. Primary data was first edited, coded and then analyzed using Microsoft Excel and SPSS computer packages. The interpreted data was grouped into common themes and was presented in the form of pie-charts, percentages, figures, tables and bar graphs.

The findings of the first specific objective regarding the level of cyber security on commercial banks in Kenya revealed that, 100% of the respondents indicated that they understood the importance of cyber security. Ninety two point Seven Percent of the respondents indicated that they had network security policies in place while 92.5% agreed to having a disaster recovery site. 75% of the respondents said that they serviced their disaster recovery site between 0-6 months, Ninety five point one percent of the respondents indicated that they use an antivirus.

The second specific objective was assessing the effectiveness of existing regulation. Sixty one point one percent of the respondents cited that they had not reported any cases of cybercrime. 40% of the respondents indicated that they strongly agreed that their Cyber Security policies described on how to get back from an attack. Sixty Seven point five percent (67.5%) of the respondents expressed they were aware of the proposed national
cyber security policy. 76.9% of the respondents expressed that they agreed that the computers in their organizations were secure from cyber criminals.

The responses of the third specific objective on how employee awareness and competence influences occurrence of cybercrimes in commercial banks in Kenya. Seventy one point Eight percent of the respondents indicated that they strongly agreed that exiting employees are removed from the system during the exit process. Eighty four point six point six percent of the respondents indicated that they agreed that their organizations vet potential employees prior to employment. 53.8% of the respondents felt that their organizations handled disgruntled employees well.

The study concludes that the level of Cyber Security in commercial banks in Kenya, and employee awareness and competence needs to be improved so as to curb cybercrime. The necessary regulation in terms of policies have been formulated and documented. Commercial banks understand what cybercrime is and the effect of the same on their institutions. IT was evident that despite commercial banks being aware that there has been an increase in the cases of cybercrime they were not reporting the cases to the authorities.

The study recommends that commercial banks enhance their security by implementing timed access control mechanisms. These should be combinations of ‘Something you are’ and ‘something you know’. Commercial banks should report cases of cybercrime within their organizations this will help to enhance the existing national policies and regulations. It is further recommends that commercial banks educate all employees and customers to protect themselves against social engineering and develop strategies of dealing with disgruntled employees.
ACKNOWLEDGEMENT

This study could not have been completed without the help and encouragement of several people.

Many thanks to God who has availed the resources, given me good health, strength, courage, persistence and determination to see me through attaining this Degree.

Secondly, I wish to thank my family which has constantly encouraged and reminded me of the ultimate goal.

Thirdly to my supervisor who has tirelessly given me guidance and direction throughout the duration of this project.

Finally I wish to thank my friends and colleagues for their support, discussions and engagement in the Subject of this project.
DEDICATION

This work is dedicated to my parents. From them I have the gift of Life and Education; the greatest gifts parents can give to their children.

This work is also dedicated to my husband Conrad and son Ethan, My siblings Carol and Njomo, Mark, Diana and Auntie Winnie. Thank you for the encouragement when my levels of motivation ran low.
# TABLE OF CONTENTS

COPYRIGHT .................................................................................................................. iv

ABSTRACT ...................................................................................................................... v

DEDICATION .................................................................................................................. viii

TABLE OF CONTENTS ................................................................................................. ix

CHAPTER ONE ............................................................................................................... 1

1.0 INTRODUCTION .................................................................................................... 1

1.1 Background of the Study ......................................................................................... 1

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

1.3 General Objective .................................................................................................... 6

1.4. Specific Objectives ................................................................................................. 7

1.5 Importance of Study ................................................................................................. 7

1.6 Scope of the Study ................................................................................................... 8

1.7 Definition of Terms ................................................................................................. 8

1.8 Chapter Summary .................................................................................................... 9

CHAPTER TWO .............................................................................................................. 10

2.0 LITERATURE REVIEW .......................................................................................... 10

2.1 Introduction ............................................................................................................. 10

2.2 Determining the Level of Cyber Security ............................................................... 11

2.3 Assessing the Effectiveness of Existing Regulation on Cybercrime ....................... 15

2.4 Determining Employee Competence and Awareness in Influencing Cybercrime in Banks .............................................................................................................. 21

2.5 Chapter Summary .................................................................................................. 29

CHAPTER THREE ......................................................................................................... 30

3.0 RESEARCH METHODOLOGY ............................................................................... 30

3.1 Introduction ............................................................................................................. 30
3.2 Research Design ................................................................................................................. 30
3.3 Population and Sampling Design ....................................................................................... 30
3.5 Research Procedures .......................................................................................................... 33
3.6 Data Analysis Methods ...................................................................................................... 33
3.7 Chapter Summary ............................................................................................................... 34

CHAPTER FOUR .................................................................................................................... 34

4.1 Introduction ......................................................................................................................... 35
4.2 Demographic Information ................................................................................................. 35
4.3 Factors Contributing to the Occurrence of Cybercrime on E-Banking in Commercial Banks in Kenya .............................................................. 42
4.6 Chapter Summary .............................................................................................................. 88

CHAPTER FIVE ..................................................................................................................... 91

5.0 DISCUSSION, CONCLUSIONS AND RECOMMENDATIONS .................................. 91

5.2 Summary......................................................................................................................... 91
5.3 Discussion ......................................................................................................................... 92
5.4 Conclusions ..................................................................................................................... 99
5.5 Recommendations for Further Study .............................................................................. 101

REFERENCES ...................................................................................................................... 104

APPENDICES ....................................................................................................................... 112

Appendix A: Introductory Letter ......................................................................................... 112
Appendix B: QUESTIONEIRE ............................................................................................... 115
LIST OF TABLES

Table 1: Threat Activity Vs Internet usage in Kenya 2013 (Paula, Carol, Kevin, Martin, & Barbara, 2014) .......................................................................................................................... 1
Table 3.1: Sample Size ...........................................................................................................43
Table 4.2.4: Computerized Operations ..................................................................................38
Table 4.3.1: Relationship between Level Of Education Vs Knowledge Of Cybercrime ....55
Table 4.3.9: Correlation between Biometrics used as Authentication Method Vs Highest Level of Education ........................................................................................................49
Table 4.3.16: Correlation between how Often the Banks Updates/Patches their Software versus Average Income per Month .........................................................................................68
LIST OF FIGURES

Graph 4.2.1: Gender of Population.................................................................35
Graph 4.2.2: Age of Respondents.................................................................35
Graph 4.2.3: Highest Level of Education.......................................................36
Graph 4.2.4: Position within the Bank.........................................................37
Graph 4.2.5: Average Income Per Month.....................................................37
Graph 4.2.6: Bank has e-banking Services...................................................38
Graph 4.2.7: Importance of Cyber Security..................................................39
Graph 4.2.8: Number of Account Holders.....................................................40
Graph 4.2.9: Number of Account Holders using E-Banking Services.............41
Graph 4.3.1: Impact of using Technology on Customer Levels......................42
Graph 4.3.2: Know what Cybercrime is.........................................................42
Graph 4.3.4: Existence of Network Security Policy......................................43
Graph 4.3.5: Existence of a Disaster Recovery Site.....................................44
Graph 4.3.6: How Often the Disaster Recovery Site is serviced..................45
Graph 4.3.7: Existence of a Firewall...............................................................46
Graph 4.3.8: Frequency of Reviewing Firewall Configurations....................46
Graph 4.3.9: ICT Staff in have Undergone Cyber Security Training.............47
Graph 4.3.10: Bank employs the use of Antivirus.......................................48
Graph 4.3.11: Authentication Methods Used: Biometrics............................48
Graph 4.3.12: Authentication Methods Used: Passwords............................49
Graph 4.3.13: No Authentication Method being used..................................51
Graph 4.3.14: Authentication Methods Used..........................................................51
Graph 4.3.15: Bank has an Intrusion Detection System for Logical Intrusions........52
Graph 4.3.16: Relationship between Organizations has Reported Cases of Cybercrime and Bank has an Intrusion Detection System for Logical Intrusions....................... ....53
Graph 4.3.17: Bank Stores Data in Encrypted Format..........................................67
Graph 4.3.18: Relationship between Organization Banks that Stores Data in Encrypted Format Vs Bank has an Intrusion Detection System for Logical Intrusions................... …54
Graph 4.3.19: How Often the Banks Updates/Patches their Software.........................55
Graph 4.3.20: Bank has Employees Charged with the Responsibility of Media Monitoring.............................................................................................................56
Graph 4.3.21: Bank having a Risk Department.............................................................57
Graph 4.4.1 Reporting Any Cases of Cybercrime.........................................................57
Graph 4.4.2: How Often the Bank Reviews the Firewall Policies.................................58
Graph 4.4.3 Bank has a Cyber–Security Policy...............................................................59
Graph 4.4.4 Cyber Security Policy Addresses how to get back from an Attack.............60
Graph 4.4.5 Awareness of the Proposed National Cyber Security Policy.....................61
Graph 4.4.6 the Cyber Security Policy in Kenya Serves the Banking Industry Adequately62
Graph 4.4.7 Computers in Banks are Secure from Cyber Criminals..........................63
Graph 4.4.8 Bank Employed the use of Automated Teller Machines..............................64
Graph 4.4.9 Bank has employed the use of Technology to serve its Customers..........65
Graph 4.4.10: Aspects of the Proposed National Cyber Security Policy to Incorporate…66
Graph 4.4.11: Bank had educated its Customers to Protect Themselves from Cyber Stalking

Graph 4.4.12: E-Banking Guidelines are Sufficient

Graph 4.5.1: Number of non ICT Staff in Organization

Graph 4.5.2: No of Staff Using the Computer as a Tool

Graph 4.5.3: No of Non ICT Staff Trained on Cyber Security

Graph 4.5.4: How Often Employees are required to Change Access Codes

Graph 4.5.5: How Often the Bank Audits Logical Access Logs

Graph 4.5.6: Bank Allows Mobile Banking for its Customers

Graph 4.5.7: Number of ICT in Organization

Graph 4.5.8: No of ICT Staff with Training on Cyber Security

Graph 4.5.9: Systems in Place Lock out Users after Several Failed Log on Attempts

Graph 4.5.10: Exiting Employees are Removed from the System During the Exit Process

Graph 4.5.11: Prior to Employment Bank Vets Potential Employees

Graph 4.5.12: The Bank Handles Disgruntled Employees well

Graph 4.5.13: Bank Employees had Been Educated to Recognize Social Engineering

Graph 4.5.14: Bank Allows for Access to Personal Emails on Work Computers

Graph 4.5.15: The Bank Employed Sending of Authentication Messages to Mobile Device
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABM</td>
<td>Automated Banking Machine</td>
</tr>
<tr>
<td>AOP</td>
<td>Annual Operation Plans</td>
</tr>
<tr>
<td>ATM</td>
<td>Automated Teller Machine</td>
</tr>
<tr>
<td>BoP</td>
<td>Base of the Pyramid</td>
</tr>
<tr>
<td>E-Banking</td>
<td>Electronic Banking</td>
</tr>
<tr>
<td>ICTD</td>
<td>Information and Communication Technologies and Development</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Providers</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>MFS</td>
<td>Mobile Financial Services</td>
</tr>
<tr>
<td>MNOs</td>
<td>Mobile Network Operators</td>
</tr>
<tr>
<td>SP</td>
<td>Strategic Plan</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications System</td>
</tr>
<tr>
<td>VB</td>
<td>Virtual Bank</td>
</tr>
</tbody>
</table>
CHAPTER ONE

1.0 INTRODUCTION

1.1 Background of the Study

Identification of Information and Communication Technology (ICT) as an essential tool for sustainable development has proved to be worth every investment. The advent of digital technology gave birth to modern communication hardware, internet and powerful computer systems to process data. Thus, the internet has given a safe haven for internet platform, which has created geometric growth and accelerated windows for opportunities for business and removal of economic barriers hitherto faced by nations of the world (Okonigene, 2010). As a result of this, internet usage in Kenya has grown rapidly resulting in explosion of Internet Service Providers (ISP’s) and internet access points (Peterson, Gladys, & Christopher, 2011). In this present time, modern technology is being introduced in all the fields and it is changing the world with lots of innovations. In banking, electronic devices play a dominant role in order to satisfy the growing needs of the customers. The rapid advancement in electronic distribution channels has produced tremendous changes in the financial industry in recent years, with an increasing rate of change in technology, competition among players and consumer needs (Hughes, 2001).

Table 1: Threat Activity Vs Internet usage in Kenya 2013

<table>
<thead>
<tr>
<th>Data/Internet Subscriptions</th>
<th>No. of Malware Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1 2013</td>
<td>800000</td>
</tr>
<tr>
<td>Q2 2013</td>
<td>1170000</td>
</tr>
<tr>
<td>Q3 2013</td>
<td>1430000</td>
</tr>
<tr>
<td>Q4 2013</td>
<td>2000000</td>
</tr>
</tbody>
</table>

The Graph above is borrowed from the Kenya Cyber Security report of 2014. It shows trend of the uptake of internet connectivity over the four quarters of the year. From the
Graph, The increase in internet connectivity over the period has been steady and gradual. Malware Attacks have also increased progressively over the same period of time.

The proliferation of, and rapid advances in, technology-based systems, especially those related to the internet, are leading to fundamental changes in how companies interact with customers (Parasuraman, 2002). Internet banking has become the self-service delivery channel that allows banks and various other businesses to provide information and offer services to their customers with more convenience via the web services technology. In addition to this, the challenging business processes in the financial services pressurized banks to introduce alternate business channels to attract customers and improve customer perception (Bauer, 2005). The evolution of e-banking has fundamentally transformed the way banks traditionally conduct their businesses and the ways consumers perform their banking activities (Sayar, 2007).

The electronic transaction services are aimed at improving the market share and business growth of the financial industry in Kenya. The challenges of generating interdisciplinary dialogue about electronic banking in the developing world are illustrative of long-running dynamics within the community of scholars and practitioners concerned with Information and Communication Technologies and Development (ICTD). The electronic banking case adds new wrinkles to broader discussions about technology and development, and about mobile communication technology gadgets in the society and the perceived socio-economic benefits that can be cultivated in the context of improving financial performance for sustained market share and business growth.

With the advent of computers (and especially the Internet) businesses are subject to threats like malicious activities and cyber-crimes. Few criminally minded youth in the country, which are mostly not educated or graduates are stealing and committing atrocities through the aid of the internet online business transactions (Okonigene, 2010). Cyber criminals use computers and technology to carry out the destructive activities that have been around for decades. In July of 2013 the Banking regulators website was hacked and the exchange rate section of the site flooded with messages in both English and French. It is reported that the hacking blocked many visitors from around the world. Similarly in March 2014, Ministry of Transport website was hacked. This raised concerns
over the security of Government Websites. Whether it is insiders or unknown intruders involved in hacking (i.e., the unauthorized use or attempt to circumvent the security mechanisms of an information system or network), cracking (i.e., breaking into a computer system), phishing (i.e., attempting to acquire identifiers and passwords), or phreaking (i.e., cracking a phone or communication network), as long as people are the weakest link, there really is no safe harbor from cyber-crime. Due to high rate of cybercrime, banking institutions have been using huge part of their revenues to prevent cyber-crime. In the market, various IT-based banking products, services and solutions are available such as Phone Banking; ATM facility; Credit, Debit and Smart Cards; Internet Banking & Mobile Banking; SWIFT Network & INFINET Network; Connectivity of bank branches to facilitate anywhere banking.

The banking sector in India is on the verge of revolutionary changes in the way it functions and delivers its services to customers. The bank branches are getting networked and becoming an integral part of the enterprise core banking solution. He asserted that cyber-related crimes, present an especially high risk to certain industries and types of businesses, including banking industry. Cyber-crimes have had negative consequences to the increased use of computers and the related technology in banking institutions. Although cyber-crime has appeared like myth, it poses a real threat to the continued use of computers. A Phoenix-based bank accidentally allowed an employee of a small business to con her owner out of $91,000 in line-of-credit advances and $75,000 in credit card charges and cash advances. Cyber-Crimes are Commonly Perpetrated against Banks

Electronic banking (e-banking), also known as Internet banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels (Daniel, 1999). E-banking includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the internet. Customers access e-banking services using an intelligent electronic device, such as a personal computer (PC), personal digital assistant (PDA), automated teller machine (ATM), kiosk, or Touch Tone telephone. The terms computer crime, high-tech crime,
digital crime, e-crime and cyber-crime can be used interchangeably with electronic crime. E-crimes are essentially crimes where the computer is used either as a tool to commit the crime, as a storage device, or as a target of the crime. As a storage device, computers can either store information that will assist in the execution of the crime or information that is illegal for the owners to possess, such as stolen intellectual property. Computers are classified as a target if the information that they contain is altered or retrieved in an unlawful way, such crimes can range from amateur hacking to terrorism.

Cybercrime or computer crime refers to the criminal activities or criminal network which takes place through the internet (Choo, 2008); it is any crime which committed through the use of computer or computer network. Therefore cybercrime including crimes like fraud, theft, blackmail, forgery, embezzlement, and other in which a computer or computer network is the tool, source, target, or generally the place where the criminal activity takes place. It is a crime that involves the information technology infrastructure which includes illegal access, interception, and interference with the data, interference systems, and others. Computer crimes have become an issue of concern especially those involving hacking, infringement of copyright, and others which are likely to interference with the privacy and confidentiality of information (Choo, 2008).

Perpetrators against banks can use several kinds of cyber-crimes. The most common are outlined Phishing (pronounced “fishing”) is growing rapidly. The Anti-Phishing Common Cybercrime Risks for Financial Institutions, Phishing, Identity Theft, Worms and Trojan horses, Spyware, Search engines/Google and Blackmail, Denial-of-service/distributed-denial-of-service attacks, data acquisition and storage (stealthily access to systems, identity collection and theft, botnets among others (DeZabala, T., & Baich, R. (2010)).

Current security models are minimally effective against cyber criminals and organizations remain unaware of that fact. Cyber criminals seem to be reinvesting portions of their significant profits in developing new capabilities for circumventing today’s security technologies. In the article by Deloitte titled combating the Fastest Growing Cyber Security Threat, they noted that even the major antivirus vendors find it difficult to keep up with the amount of new Malware (Deloitte, 2010). Cyber criminals routinely exploit
the resulting vulnerabilities. More recently the cybercriminals are targeting that which is the weakest link the user. This is done through the internet by way of social Engineering. The cybercriminal will make one believe that they are working with a colleague or other legitimate party and in the process drive information out of the unsuspecting employee (DeZabala & Baich (2010).

Cybercrime is a global phenomenon that is threatening the economy of nations. It is a major threat in India as is in Nigeria and Kenya. Punjab National bank suffered a loss of close to Rs.1.39 crore when the computer recorders were manipulated to create false transactions. Cybercrime is difficult to prove as it lacks the traditional paper trail (Okonigene, 2010).

The future looks grim. This is because cybercrime attacks will continue to be more severe, more complex, more difficult to prevent, detect and address than current ones. The perpetrators also continue hoarding their skills as malware authors for hire provide their skills, capabilities, products and outsourced services to other cyber employee (DeZabala, et al. (2010).

So as to fight Cybercrime, the global cyber security agenda has seven main strategic goals namely legal measures, technical procedures and measures, organizational structures, capacity building and international cooperation (Gecko, 2012).

1.2 Statement of the Problem

The exponential growth of technology, the increase in its capacity and accessibility, and the decrease in its cost, has brought about revolutionary changes in commerce, communications, entertainment, and education. Along with this greater capacity, however, comes greater vulnerability. Information technology has begun to provide criminal opportunities of which the olden days criminals would never have dreamed (Olasanmi, 2010).

The computer was invented to hasten data processing with effortless ease. However, as the understanding of the use of the computer has increased across various levels of knowledge, so as its use for committing crimes increased (Olasanmi, 2010). The financial
sector in the East African region is losing over Sh170 billion every year through cybercrime (Wahito, 2012). Cybercrimes cost the Kenyan economy about 3 billion shillings (about $36.14m) annually with banking sector alone recording losses of about 2.1 billion shillings ($25.3m) yearly in cybercrime (Anonymous, 2012).

The increasing rate at which systems can connect together to share information has not only increased the number of prospective victims of computer related crime, it also increased the number of prospective offenders. Yet the complexity of these crimes and the elusive nature of computer criminals have made it increasingly difficult to detect or prevent these crimes. Computer crimes have quickly increased in recent years and have overtaken the ability of the government and the various sectors to fully protect their systems (Olasanmi, 2010).

Estimating the incidence, prevalence, cost, or some other measure of computer related crime is a difficult challenge because such crimes are not easily detected and even when detected, reports to the appropriate authorities are not always made (Olasanmi, 2010). Businesses do not always want to report problems because there is a perception that their information will be disclosed publicly, which could, in turn, cause harm to their business (Wagner, 2007).

Several developments have heightened the Cybercrime wave. These developments are Social Networking and constant online communication, Online banking, investing, retail and wholesale trade, foreign rogue governments, terrorist organizations and related actors, financial hardships employee (DeZabala et al, 2010).

The effect of cyber-crime E-banking in Kenya has not been documented, thus this study sought to contribute to the occurrence of cybercrime in Kenya to establish the factors

1.3 General Objective

The general objective of the study was to establish the factors contributing to occurrence of Cybercrime on the E-Banking Industry in Commercial Banks in Kenya.
1.4. Specific Objectives

The study sought:

1.4.1 To determine the level of cyber security on commercial banks in Kenya.

1.4.2 To assess the effectiveness of existing regulation on cybercrimes in Kenya.

1.4.3 To determine how employee awareness and competence influences occurrence of cybercrimes in commercial banks in Kenya.

1.5 Importance of Study

The study will be beneficial to the following groups:

1.5.1 The Government and Policy Makers

The study will be significant to the government as policy makers regarding cyber-crimes in banking industry where basic protection methods and specific defensive tools to minimize cyber risks could be formulated. In general, the policy makers will gain insight on the factors contributing to cybercrime in banks.

1.5.2 The Central Bank of Kenya

This study will help the Central Bank of Kenya know the causes of cyber-crime. In so doing, they will be able to make sound decisions concerning various rules and regulations to be observed by the Commercial banks so that the effects of this vice may be minimized.

1.5.3 The Customers of Commercial Banks

This will enable the customers to understand that they also have a role to play in mitigation of the risk that is cybercrime. Through being conscious of the banking information that they give out about them, customers can drastically reduce the occurrence of cybercrime.

1.5.4 Researchers and Academicians.
Being that there are limited studies that link cybercrimes in banking sectors, the outcome of this study will be invaluable empirical study and also act as local reference on cybercrimes in banking for future research for example assessing impact of cybercrimes on visual banking. The findings of this study would provide information and advice on the possible opportunities that research institutions can use to expand the research, availability, and impact of information and knowledge of security in E-banking for the development of the upcoming commercial banks.

1.6 Scope of the Study

This study focused on determining the factors contributing to occurrence of Cybercrime on E-Banking Banking Industry in Commercial Banks in Kenya. The study focused on contribution of internet security, legal framework, cybercrime awareness and reporting on how they lead to cyber-crimes in commercial banks.

1.7 Definition of Terms

1.7.1 Mobile Banking

This is a form of banking transaction carried out via a mobile Phone. Mobile banking allows bank customers to check their account balances, perform Credit card transaction as well as provide information on the latest transaction made by customers.

1.7.2 Electronic Banking

E-banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels. E-banking includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Internet. Customers access e-banking services using an intelligent electronic device, such as a personal computer (PC), personal digital assistant (PDA), automated teller machine (ATM), kiosk, or Touch Tone telephone.

1.7.3 Cybercrimes
These are crimes committed using new technologies. It include offences against computer systems, data, and crimes where networked computers and other devices are used to facilitate the commission of an offence (Campbell, 2014).

1.7.4 Cyber Security

Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets (Definition of Cyber Security, 2010).

1.7.5 Awareness

Knowledge that something exists, or understanding of a situation or subject at the present time based on information or experience (Press, 2013).

1.7.6 Employee Competence

A skill performed to a specific standard under specific conditions. It is the combination of skills and attributes and behaviors that are directly related to successful performance of a job. (Division, 2013).

1.8 Chapter Summary

This chapter has looked a brief history of the emergence of computers, and has attempted to bring out the various forms of cybercrime and in specific described the forms and effects of cybercrime. Within this chapter various terms relating to the subject matter have been defined.

The next chapters will define the research methodology, the findings of the research and finally the conclusions and recommendation.

The immediate next chapter is the Literature Review, we shall be taking an in-depth look at what others have written as regards to factors contributing to occurrences of cybercrime in commercial banks in various countries.
CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Introduction
This chapter aims to assess what others have written about the factors which drive cybercrime in commercial banks. The focus shall be on the effect of the existence or lack of cyber security counter measures, regulation and the effect of staff’s awareness of the cybersecurity. Finally a summary of the chapter gives a brief of what has been covered in the chapter.

2.2 The Level of Cyber Security in Commercial Banks

2.2.1 Current Practice in Prevention and Policy of Cyber Security

Robust cyber-security (detection and prevention) and cyber-resilience (ability to continue functions and/or bounce back quickly during and after an attack) are important factors in mitigating impacts from cyber-crime. Non-existent or ineffective cyber-security and cyber resilience creates a tempting opening for ‘would-be’ cyber-criminals and may mean that even relatively simplistic cyber-attacks can get in and cause damage (Tendulkar, 2013).

According to Tendulkar (2013), cyber-security measures in financial institutions should be proactive (attempting to anticipate new forms of risk and potential vulnerabilities) as well as reactive. Reliance only on ‘reactive preventative mechanisms such as firewalls, an antivirus and intrusion detection system is no longer sufficient. This is because many of these sorts of mechanisms are ‘signature based’, which means that a particular form of virus, malware etc. must be widespread, identified and then logged before it can be protected against. There will always be some customers suffered as collateral, before the anti-virus software can notice the new threat and update.

Threats can filter through standard defense mechanisms undetected, especially if the attack is tailored for a single target entity. Nevertheless, prevention and detection alone is not sufficient, robust cyber-resilience is also important. Cyber-resilience refers to the ability for technological infrastructure and a firm’s reputation, critical operations etc. to continue during (or recover quickly) after a successful attack. Cyber-resilience can be facilitated through clear disaster recovery protocols and can be considered as a subset of business continuity (Tendulkar, 2013).
Stewart (2001), elucidated that having clear protocols in place can be essential in maintaining stability of an organization, and can also assist in ensuring the stability of the greater financial system.

A look at the recent Carbanak attack on commercial banks which is known as the largest bank Heist ever where cybercriminals successfully filtrated nearly $1 billion dollars from commercial banks and financial institutions around the world. The Malware which infected networks through Phishing attacks served as remote back doors to infected computers. The criminals used these to take over control of ATM Machines, to adjust account balances and to transfer money. In addition to this the cyber criminals go ahead and study the configuration of the network and install additional tools for their use. These tools include Ammy Remote administration tool and even compromise the Secure Shell Servers.

According to the Kaspersky report ‘Cabanak APT The Great Bank Robbery’ the criminals used SWIFT network to transfer money to their accounts and in other cases manipulated oracle databases to open payments or debit card accounts. Cyber security experts say cyber-attacks are becoming more sophisticated as criminals seek out weaknesses in the financial system, forcing banks and companies to make changes to security practices and improve their procedures. Bank boards in particular are worried about the risk, as new technologies such as mobile banking are making banks more vulnerable and as costs from a break-in are rising.

Tom Curry’s words which are summarized by Snyder (2014) describe the complexity of the exposure very well by saying that; from a vulnerability perspective, banks are at increased risk due to our banking system’s significant reliance on technology and telecommunications, and the interconnections between these systems. Banks not only operate their own networks, they also rely on third parties to support their systems and business activities. Some of these third parties have connections to other institutions and servicers. Each new relationship and connection provides potential access points to all of the connected networks and introduces different weaknesses into the system.

2.2.2 Constituents of the Threat Model and Prevention
According Verizon (2012) report, agents, action, asset and attribute were identified as the main drivers of E-crime: He further defined them as follows: Agents are those who cause or contribute to an incident. These may be external (from outside the organization), internal (from within the organization) or from partners (these are third party sharing business relationship with the organization). Action was defined as the activities done or performed. The result of which affects the asset. Asset was defined as the vital thing which is affected. It may be the system or the data therein. Finally, attribute was defined as how the asset is affected by the action. The report emphasized that the measures put in place to counter these activities should be strong enough to ensure that they block out as much of these attacks as possible. Moreover the controls put in place should be very varied and range from software fixes, that are required from users, software updates, and complex and expensive solutions. The solution to be applied according to Verizon report depends on the amount of pressure the attacker is applying and where the attacker is attacking (Verizon, 2012).

One of the findings of the Verizon 2012 report is that at the initial stage of an attack, the attacker has to gain entry into the systems they are aiming at. Thus in such a case the Kenyan banks need to consider the strength of their network security, they need a comprehensive approach with regards to physical, technical and administrative controls. In attempting to prevent such intrusions they should consider the use of secure card readers for authentication of the users prior to entering the systems, encrypt data so that even when one gains access, they would not be able to make out anything from the data they see or obtain and they should also have policies and procedures in place which address cyber security

Siddique and Rehman (2011), proposed three security preventive measures. Firstly, they stated that banks should ensure that they have a protection program that has power over cookies, which prevent internal information from being forwarded to other destinations outside the organization. Secondly, it is important to have the latest software which is updated with the latest patches. This means that all known loopholes and bugs which have been discovered by the vendors have been patched and bugs resolved. Thirdly, banks should have a firewall in place.
Limited (2011), defines a firewall as a security system that controls access to a protected network. A firewall is located so that every access request from a public network to the protected network must pass through the firewall, eliminating the need for individual protection of every server and host in the protected network. Some things also need to be considered prior to placing the firewall. A network security policy needs to be in place. This help the organization in defining the resources that need to be protected and the threats against them. (Firewalls & Virtual Private Networks, 2009). The Verizon report recommends that it is vital to stop the attackers even before they get in. Attackers will not spend much time on already hardened targets whereas there are other softer ones where they can make quick wins (Verizon, 2012).

After entry into a network, the Verizon report informs that the attackers will install various types of malware, these may require some degree of customization, escalate privileges’, set up remote entry and control mechanisms and explore the network to establish where the ‘goodies’ are stored (Verizon, 2012). Internal network security measures need to be set in place. Measures such as access controls and updating of software to the most current version should be regularly done, having up to date operational antivirus and intrusion detection software (Siddique & Rehman, 2011). On finding the ‘goodies’ the attackers will compromise the data. Protecting the goodies should be another factor to be strongly and diligently exercised. Banks are constantly transmitting data over the networks. They should thus put in place measures such as encryption of data (that which is in storage and that which is in transit), use of virtual private networks and use of IPsec protocols (Schulz, 2006).

It is important to know that some organizations will remain lucrative to attackers despite improving and strengthening the level of cyber security. This is because of the nature of business in those attacked organizations (Verizon, 2012).

According to cyber-insurance, while perhaps not useful in ensuring functioning during and in the immediate aftermath of an attack, can assist in cost recovery over the longer-term. In addition, cyber-attacks do not only target technological vulnerabilities, but vulnerabilities arising from the behavior of staff, suppliers and clients. Even with robust cyber-security measures in place, a single organization may find it difficult to control the
cyber-security practices of its suppliers and any outsourced services that they are networked with (Jopson, 2013).

Furthermore, cyber-security measures could be easily side-stepped if the crime is perpetrated by an ‘insider’ (an employee) (Tendulkar, 2013). Human users are often the most vulnerable and unpredictable part of a firm’s technological infrastructure and by taking advantage of the ‘human element’ of cyber systems rather than exploiting technological or network weakness, the threat becomes almost impossible to eliminate.

Training for all staff (not just IT staff) is important and given the innovation of cybercrime, training is best executed periodically (rather than a one-off) with staff being kept up-to date on new threats and trends (Tendulkar, 2013).

2.3 Effectiveness of Existing Regulation on Cybercrime

2.3.1 Dealing with Cybercrime on the International Scene

According to Wang (2007), new technologies open doors for new crimes and there has been an increase in the number of cybercrimes reported. It is also said that there isn’t enough evidence to show the number of cybercrime that is done, this is because many of the cases go unreported (Moitra, 2005).

The international nature of cybercrime makes it difficult to detect, prosecute and execute. Jurisdictional conflict and ambiguity when it comes to cybercrime can accentuate the possibilities for regulatory arbitrage and create confusion around legal channels to find reprieve (Tendulkar, 2013). In an attempt to resolve this issue there was a committee which was set up to develop cyber legislation for commonwealth states. The Cybercrime Legislation of Commonwealth States used Budapest Convention and Commonwealth Model Law’ that establish three areas of cooperation namely: that the members are to provide extensive cooperation to each other and to minimize impediments so as to smooth the rapid flow of information and evidence internationally. Secondly, that this cooperation is to be extended to all criminal offences related to computer systems and data as well as collection of electronic evidence. Thirdly, co-operation is to be carried out both "in accordance with the provisions of this Chapter" and "through application of relevant international agreements on international co-operation in criminal matters,"
arrangements agreed to on the basis of uniform or reciprocal legislation, and domestic laws” (Division, 2013).

Over the past three decades, large numbers of banking customers depend on Technology to conveniently meet their banking needs. In the recent years, there have been a large number of accidents of technology related frauds. It is necessary to manage the risk associated with this technology aided fraud as well as diminishing its impact on the important issues that face financial institutions as fraud techniques to become more advanced with increased occurrences (Mehta, 2011).

2.3.2 Insight into Some Existing Cyber Regulation

The cybercrime laws of the United States cover laws inhibiting online identity theft, hacking, intrusion into computer systems, child pornography, and intellectual property and online gambling. The laws stipulate heavy penalties such as imprisonment for a period of not more than 15 years for cybercrimes committed in banking sector

Al Rees (2006), reveals that in the same country, the case of fraudulent activity in connection with computers such as knowingly accessing data that one is not authorized to, with the belief that that data is being obtained to cause harm to the nation or an organization, obtains information from a financial institution or a card issuer, causes transmission of a program, information, code or command, causes damage to a computer used by the government, the punish meant for these is a fine under his title or imprisonment for not more than ten years or both.

In India, they have enacted the Information Technology Act 2000. This legislation addresses the use of digital signatures to authenticate electronic documents and the use of private and public keys to authenticate the sender and authorize users to decrypt data.

Further, evidence may be given in a court of law in electronic form. In their legislation they define the penalties for a crime committed to a computer or a computer system. It states that if one practices cybercrime and causes damage, then the perpetrator are to pay the victim not more than an equivalent of 13.7 Million Kenya shillings. The information
act of 2000 creates the position of a Cybercrime Appellate Tribunal; the mandate of this is to advice on cybercrime matters (India, 2000).

Ineffective regulation also means that cyber-criminals are less likely to be deterred. Potential indicators include perceptions on the effectiveness of deterrence and enforcement of regulation, instances of jurisdictional conflicts/ambiguity, and possibilities for regulatory arbitrage. Despite some efforts towards global harmonization in the fight against cyber-crime, there is still jurisdictional fragmentation in terms of definitions, legal frameworks and enforcement actions and there is no global governance mechanism for cyber-crime related cases (Wall, 2001).

There are legal and political barriers to overcome, especially dealing with a potential criminal from another jurisdiction due to sovereignty, privacy and human. An in-depth report into cyber-crime by the UNODC elaborates on some of these issues; essentially pointing out those current national legal frameworks may be unfit to engage with the transnational nature of cyber-crime. For some cyber-crime cases, numerous jurisdictions may claim authority over handling a cyber-crime act. This may be particularly problematic if cyber-crime offences are treated differently in different jurisdictions. For example, the UNODC reports notes that the production, distribution and possession of cyber-attack tools e.g. malware, is criminalized in some countries but not others (Suri & Chhabra, 2003).

Cyber-criminals may thus take advantage of lax or non-existent cyber-crime laws in certain jurisdictions, even if their attacks are focused towards jurisdictions with stricter rules. Complicating the situation further, is the issue of attribution. The nature of cyberspace makes it easy to both wipe any identifiers and create fake ones, raising challenges for the correct identification of criminals. Cyber-criminals can also take-over the computers of innocents, in order to carry out their crimes (Sheng, 2005).

Cyber security has to be strongly supported by clearly defined national frameworks and strategies of enforcement. In the COMESA region, the COMESA Cyber Security Program was developed. Its aim is to provide effective public private partnership for cyber security to ensure secure network environments thorough standardized security
programs. Kenya Cyber Security Policy is currently being steered by the ICT Authority. The key elements of the policy are Training and awareness, Economic Impact, Governance, Policy and Legal framework. In June 2013, a committee was formed to spearhead efforts against cybercrime under the Communications Act of Kenya. The Kenya Information and Communications bill 2013 incorporated and defined the term cyber security in the amendments further stipulating the penalties of the crimes for both individuals as well as organizations found committing them. In addition to this, the office of the Director of Public Prosecution (ODPP) established a dedicated unit to tackle the prosecution of cyber criminals. The ODPP is also organizing a workshop to review existing laws and develop a complete draft bill on cybercrime based on international best practices.

2.3.3 Cybercrime in the Banking Industry in Kenya

The prevailing contemporary era has replaced long-established monetary instruments from a paper and metal based currency to “plastic money” in the form of credit cards, debit cards, etc. This has resulted in the escalating utilize of ATM all over the world. The use of ATM is not only safe and sound but also suitable. This safety and convenience, has an evil side which is reflected in the form of “ATM FRAUD” that is an international problem (Mehta, 2011). He further revealed that the use of plastic money is increasing for payment of shopping bills, electricity bills, school fees, phone bills, insurance premium, traveling bills and even petrol bills.

Kenya is in the process of formulating its Cyber Security Framework. (Authority, 2013). In development of this piece of legislation, there is need to uphold the issue of security on national networks as captured in the Kenya National ICT Master plan.(Communication, 2013). The Master plan identifies that ICT has a critical role in driving the economic, social and political development of Kenya as espoused in Vision 2030.

The Kenya National ICT Master plan identifies that ICT Authority has implemented electronic systems in various State Departments and other state-owned institutions, including national tax systems, immigration information system, legal information
system, the integrated financial management system and education system. Most of these systems are to be found in the National Treasury, Kenya Revenue Authority, Home Affairs State Department and Immigration Office. In addition, information is manually exchanged by and between departments and institutions using fax, e-mail and electronic media. These systems provide partial electronic services to citizens and businesses through Government portals. The goal for organizations with no business tolerance for downtime is to achieve a state of business continuity, where critical systems and networks are available no matter what happens. This means thinking proactively; engineering availability, security and reliability into business processes from the outset—not retrofitting a disaster recovery plan to accommodate ongoing business requirements.

The national cyber security policy takes cognizance of the fact that Cyber-attacks are continuously evolving—to a great extent faster than cyber defenses—resulting in an ever-increasing frequency of attacks and the probability of success over time. These cyber-attacks may come from hacktivists seeking to publicize political views, from criminal organizations seeking financial gain, from terrorist groups seeking to inflict economic or political damage, or from state-sponsored intelligence and security organizations advancing their own economic or national security aims. Many attacks involve extremely sophisticated technological and social engineering techniques; however, low-technology penetrations—such as insider threats—remain a danger. The strategy goes on to identify the four strategic goals.

i. These are Enhance National cybersecurity posture to protecting critical information infrastructure.

ii. Building National capacity through Creation of awareness and Training of citizenry to secure the national Cyberspace.

iii. Foster information sharing and collaboration through the development of a comprehensive governance framework to leverage resources, reduce conflict and duplication of effort and work towards Kenya’s long term security goals and also by Cultivate a culture of information sharing that facilitates the real time exchange of cybersecurity information.
iv. Provide National Leadership through Develop and Coordinate Implementation of the National Cybersecurity Strategy and Master Plan

As a way forward then there is need to look at the cybercrime legislation in other countries that are ahead in this aspect and try and borrow a leaf and learn from their experiences and existing legislation.

A false accusation could have political consequences and damage foreign relations, especially if nation state actors are involved. This all makes cyber-crime investigations “complex, lengthy and expensive. Furthermore, authorities may struggle to allocate budget away from localized, physical threats towards these more global, intangible ones (Tendulkar, 2013).

Owing to the worldwide impact of internet crime, various countries are using legal, organizational, and technological approaches to fight it. The legal approach aims to restrict cybercrime activities through legislation. The organizational approach aims to enforce laws, to promote cooperation, and to educate the public through the establishment of dedicated organizations. The technological approach aims to increase the effectiveness and efficiency of cybercrime analysis and investigation with the help of new technologies (Chung, 2004).

A situation where banks would have to invest much on acquiring information technology software without attracting enough customer patronage necessary to justify the huge expenditure does not make for a progressive chance for rapid growth in Internet banking in developing countries. With the deficiencies in the existing electronic banking guidelines and the seemingly lack of proactive measures in other banking regulations, in the country, the right environment for Internet banking remains presently not in existence (Mehta, 2011). He further concludes that the important advances can only be made if banking industry, law enforcement, victims, service providers, support groups, and others work together to develop a more comprehensive and effective response to this problem. Ultimately, however, the first line of defense will involve banking industry efforts that educate and empower individuals to protect themselves against cyber stalking and other
online threats, along with prompt reporting to law enforcement agencies trained and equipped to respond to cybercrimes (Mehta, 2011).

2.4 Influence of Employee Competence and Awareness in Commercial Banks

2.4.1 Response to Cybercrime Incidences

The computer has exclusive characteristic of storing data in a very comparatively small space. This makes the user more comfortable to steal the data either physically or virtually through any electronic medium. New skills, technologies and investigative techniques, applied in a global context, are to detect, prevent and respond to cyber-crime. This ‘new business’ will be characterized by new forms of crime, a far broader scope and scale of offence and victimization, the need to respond in a much more timely way, and challenging technical and legal complexities.

Innovative responses such as the creation of ‘cyber-cops’, ‘cyber-courts’ and ‘cyber-judges’ may eventually be required to overcome the significant jurisdictional issues that law and order agencies are currently facing (KPMG, 2012). Authorities on the other hand, lack necessary skills that afford them the capacity to employ efficient strategies in detecting and in collecting digital evidence crucial in prosecuting cyberspace offenders (Peterson, Gladys, & Christopher, 2011).

2.4.2 Effect of Staff on Cybercrime

In the Verizon data breach report of 2012, it was reported that 4% of the 174 Million reported cybercrime done, was perpetrated by the internal agents; that is the internal staff. Many of these internal attacks go unreported because they are not detected in the first place (Verizon, 2012).

In their 2014 Kenya Cyber Security Report, identifies 8 major threats which facilitate cybercrime. Three of these eight threats are perpetrated by employees. The three threats are namely Insider Threats, Social Media and Cyber Espionage.
In the Serianu report it is written that insider threats entail deliberate and malevolent activities performed by the existing and present employees. These employees probe the existing systems for unauthorized access and attacked the systems for various reasons including displeasure, retribution, competitive advantage and blackmail. The report goes ahead to also explain Social Media as threat. They explain that social media is a platform where disgruntled employees can engage in posting of derogatory material, hate speech and cyber bullying. The third threat is Cyber Espionage where the same report explains that this refers to stealing of secrets stored in digital formats. Such information may be released to competitors or used to inform outsiders so as to impact negatively on the organization.

Majority of the financial crime is perpetrated by insiders and employees. It is therefore necessary for organizations to take action to ensure that computer and physical security is well addressed. Personnel should be well vetted, and their references checked prior to employment. These same measures should be taken when promoting staff this is because the staff shall have access to more vital and confidential data as they move up the corporate ladder.

Employees leaving organizations should also be removed from the security clearance lists and organizations’ authentication platforms. Examples of these crimes committed by internal staff, is where an employee of an oil company managed to steal $473,541 through E-theft. She transferred the money to her husband’s business. Employees may also take part in Net espionage where they may obtain vital data from their own organization and provide it to a competing firm (Panel, 2006).

When assessing the risk posed by cyber-crime, it is important to distinguish between simple and complex attacks. The complexity of attacks can provide information about the resources of cyber-criminals and depth of attacks. Simple attacks are more likely to be detected quickly with impacts mitigated. More complex attacks may take longer to detect, with longer-term impacts and may imply quite sophisticated capabilities on the side of the cyber-criminal (Tendulkar, 2013).
In the financial system cyber-attacks are reported as more sophisticated than ever, with attacks coming from not only fraudsters but political activists aiming to disable financial institutions. Cyber-attacks can involve various stages of implementation (monitoring, real world physical interaction, distraction, information stealing, creation of backdoors and be executed persistently over a number of years (sometimes to distract from the ‘real’ attack, sometimes to simply probe for weaknesses). The attacks often combine a variety of traditional cyber-crime ‘techniques’ so that if even one form is blocked, another form could get through (Tendulkar, 2013)

According to Youga and Singh (2013), staffs requires more skill on social engineering to enable them to identify an attempted breach. Social engineering may be carried out in various ways; the information revealed by the person, gives the attacker more ammunition to use so as to gain access to some data and identity theft. The perpetrator over time is able to obtain adequate data to perform any action they may wish to in a particular system (Youga & Singh, 2013).

2.4.3 Effect of Social Engineering Cybercrime

Social engineering makes it more difficult for one to identify an attempted breach. Most users may recognize that viruses can infect their computer if they were to click on a link from an unrecognized email sender, riddled with spelling and grammatical errors. Today, cyber-attacks in financial market can easily imitate trusted email addresses, text messages, media or websites. The information to make cyber-attacks appear trustworthy can be extracted from social media and other online personal or professional data (Tendulkar, 2013).

Mobile malware is also being used. This is because banks are now enabling people to operate their bank accounts from their mobile phones. Mobile malware are now being used to disguise as fake online transaction modules. They collect customer credentials and intercept the authentication details via sms. (Rashid, 2011). In fact, last year Verizon reported that almost one third of cyber-attacks in 2012 involved social engineering (Verizon, 2012).
Especially troubling, is the rise of the ‘Advanced Persistent Threats’ (APTs), which infiltrate a specific computer or networks through targeted and persistent attacks, orchestrated over many years (Boaz, 2012). The perpetrators behind these attacks tend to be driven by political or ideological motives, rather than financial gain (Tendulkar, 2013). These attacks slowly chip away at any defenses and are constantly scanning for weaknesses. Cyber-criminals entrap users through utilizing sophisticated social engineering and the focus on ‘information’ rather than ‘systems’ means that they can be orchestrated without obviously affecting the functioning of a computer or network even as they steal, manipulate or damage information contained on it. The advanced and stealthy nature of these attacks means that they can go undetected for years (Tendulkar, 2013).

2.4.4 Mitigation Options Available

It is important to educate the users who are the key decision makers. The most current computer security education initiatives involve teaching awareness to end users and about password protection and show how to handle devices that contain data within them. It is now necessary to emphasize the importance of following the set security policy rules. In his book Protecting National Infrastructure, emphasizes the use of Security auditors. The role of these is to perform spot checks in target environments that would involve quizzing random individuals about their knowledge and interpretation of the local security policy. He however is quick to clarify that total compliance cannot be achieved and that the staff in an organization and in this case the staff in commercial banks be educated and made aware of the risks in any actions that they may take that could damage the security in the given environment.

Vetting of potential employees is vital. Most people might find it unseemly were you to run background checks on potential dates prior to asking them out. But the same does not hold true when hiring a new employee. While taking a chance on a blind date might result in a bad evening, there’s absolutely no doubt that making a wrong hiring decision can haunt your company, other employees and your client base. Kris in his article ‘Background Checks’ goes on to support the vetting of employees prior to employment. He says that a Society for Human Resource Management survey shows that, overall, employers are moving away from examining an applicant’s actual work history and are
turning instead to credit, criminal, and character data checks before hiring. The effort and investment in narrowing down your candidate pool can be completely negated by a failure to conduct effective background checks. Human capital is the largest asset an organization possesses. Failure to complete due diligence can include litigation costs if a candidate feels wrongfully treated and decides to sue, damage to your company reputation, reduced staff productivity, and additional staffing replacement costs.

For the protection of such vital networks, the key decision makers who should spearhead cyber security in their organizations are: Senior managers, these are the people who set financial and operational priorities. Secondly are the developers and designers who do the necessary networking and configure the functionality of the system. Thirdly are the administrators who perform the day to day tasks of maintaining and running the systems in use. Fourthly are the security team members who are charged with protection of the organizational systems and assets.

Email has become an essential tool for communicating, which is why it is so popular with scammers, cybercriminals, and advertising companies. In order to protect ourselves from phishing scams and malware, it is essential that we learn how to safely manage our mail. Spam is another term for junk email or unwanted email advertisements. Today, a majority of emails are spam. This is because it's easy and inexpensive for spammers to send an email to thousands of people at the same time, and they can do it anonymously, making anti-spam laws difficult to enforce. Phishing scams and malware are often included in spam, so it is important to be able to effectively manage the spam we receive in our inbox. Mail filters are often implemented and uses a wide range of heuristic algorithms on mail headers and message body text to identify unsolicited email. This software is capable of eliminating more than 98% of all SPAM messages. Its performance depends on the individual configuration, which can be tuned by each website owner. Once identified, the mail is tagged as "SPAM" for later filtering using the user's desktop mail client.

The introduction of authentication mechanisms more or less complex as the one-time-use passwords (OTPS) or sending codes for authentication through mobile devices has actually increased the level of security for each transaction. Banks reveal a
serious lack of awareness and a degree of complacency on the part of IT organizations, and perhaps security officers, vis-à-vis the threat of cybercrime (Jain 2005). Much of this belief is predicated on the notion that cyber-crime technologies and techniques are so effective at eluding detection that the actual extent of the problem may be grossly underestimated. Although financial institution cannot quantify the financial impact of cyber-criminal activity, Organizations can develop situational awareness in various ways, and thus detect and recognize threats and damages that now go undetected and unrecognized. Attention to behavioral indicators tied to fraudulent activities is a must (Deloitte, 2010).

Businesses need to use social media. Gone are the days of recommendations to keep social media usage out of the enterprise. Social media use is no longer the exception, but rather the rule. Business units such as research and development, marketing, human Capital, Marketing, and customer service are realizing the potential for utilizing social media tools to motivate revolution, create brand recognition, hire and retain employees, generate revenue, and improve customer satisfaction. Social media use is no longer just an option for enterprises that want to lead in today’s business environment. Use of social media has created highly effective communication platforms where any user, virtually anywhere in the world, can freely create content and disseminate this information in real time to a global audience ranging in size from a handful to literally millions. The enterprise should consider the risks of using social media as a business tool to communicate with customers or constituents, Enterprises must also consider the risks of employee access to social media sites while on the corporate network enterprises should consider that employees also use social media tools from their corporate issued mobile devices. Although mobile devices may be an organizational asset, they are often not subject to the same controls and monitoring as the enterprise’s computers. Exposures such as insecure requests may exist on an employee’s personal social media page; those exposures may cause improper exposure on a corporate network. In addition, malicious outsiders could use employee social media pages to promote targeted attacks by gathering material to execute erudite social engineering campaigns.
In addition to this Technologies used for the initiation and control of the secure transfer of information between the organization and an archive, whether the archive is operated in-house or by a third-party service provider, should be documented. Using cryptographic techniques can be one way to ensure authentication of the sender and the electronic document. The method of ensuring that received and subsequently stored information is identical to that originally sent should be documented. Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance, when sending record media to another location, e.g., the off-site backup facility.

Over time, as computing ease and functionality have grown, users have an ever-expanding desire for more information. With the web presence today, one can hardly imagine a day going by without accessing the web many times. Data are generated by the minute and are growing in variety and size; the costs of servers grew as the server farms grew. To ease the pains of underutilization, virtualization emerged, which made it possible for servers to attend to more than one application. Capacity utilization thus improved and cost of services came under some degree of control. So the concept of sharing or abstracting through virtualization beyond just servers grew and produced a bigger picture, known as cloud computing. Some of the benefits realized from subscribing to cloud services include achieving Economies of scale, globalizing workforce is now cheaper, minimized cost of new software, improved accessibility to software. The various options available to institutions as solutions on the cloud include Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The business of data processing has grown accustomed to cloud computing terms and concepts such as application hosting, including Software as a Service (SaaS) and application service providers (ASP); storage virtualization, including cloud storage and online backup; IT outsourcing (ITO); and business process outsourcing (BPO), including help desks, virtual data centers and hosted (platform) data centers. The potential for harm from centralizing and sharing resources has grown to a level that can quickly exceed the business case for cloud computing. Some important questions to be asked include: What are its own data and information worth to an enterprise? How much would the organizational data be worth to a cybercriminal? What could a hacker do with the information stored on the cloud? What would it cost the enterprise if another company
unintentionally accessed and altered the data? What would the enterprise do if its information vanished, or they lost access to it, due to an adversity at the cloud provider? How would the enterprise know if someone altered the data? What is an enterprise authorized by law to do if its data were unprotected?

Awareness of cyber-based risks in different sectors is gradually increasing and has already been at least partially addressed in some regulations around the world, taken up through practical industry-wide initiatives and captured in a number of reports and surveys. World leaders, experts and prominent figures have also openly acknowledged the cyber-threat to society and the economy and Governments are actively and transparently elevating cyber-related risks into a national security issue (Jain, 2005).

Furthermore, the potential reach of cyber-crime is vast - including much of our economy. 70 per cent of households and 94 per cent of businesses with 10 or more employees are online. There is exponential growth of internet-connected mobile devices and social media is now used profusely for both personal and business pursuits; many businesses are turning to cloud computing to store data. Due to cost efficiencies, banking and other financial services providers all rely on technology of some kind to disseminate information and execute business rapidly (Tendulkar, 2013).

In the financial sector, views on the potential severity of cyber-attacks are mixed. On one hand, a number of prominent figures and experts highlight the increasing scale of the risks posed by cyber-crime in the financial sector, and the urgency faced warning of an impending terrorism act. In fact, the U.S. House Intelligence Committee suggested that it could be a successful and large-scale attack on financial institutions that brings about the ‘doomsday’ scenario or ‘cyber-crisis’ many fear (Tendulkar, 2013).

On the other hand, an environment of low awareness and transparency for example through lack of information sharing arrangements could exacerbate the impact of cyber-attacks. A lack of awareness may mean that actors are more likely to be ‘blindsided’ by a new attack and find themselves without the appropriate tools and protocols to mitigate damage. Furthermore, where there is a lack of transparency around emerging forms of
cyber-crime, there could be a hidden build-up of risk. (Tendulkar, 2013). Another way to protect the bank when all else fails is to buy cyber insurance

2.5 Chapter Summary

This chapter covered an evaluation of works in line with the research objectives. The first section underlined the effect of existing level of cyber security on commercial banks. The second looked at the effect of existing regulation on the level of cybercrime in a country. Lastly, the literature review outlined the effect of staff on cybercrime.

The next chapter outlines the research methodology which shall look at the research design, the population, research procedures, data analysis methods and presentation.
CHAPTER THREE

3.0 RESEARCH METHODOLOGY

3.1 Introduction

This chapter covered the methodology and procedures that was used to collect and analyze the data collected for the study. The chapter dealt with the type of research design, the population, the sampling design, data collection methods and data analysis methods. The chapter summary provided an outline of the areas covered in this chapter.

3.2 Research Design

Research design as a plan for selecting the sources and types of information used to answer research questions. This study adopted a descriptive research design. Descriptive research design is a type of consultative research that gives a description of something (Malhotra, 1996), usually a phenomenon or characteristics associated with a subject population (Cooper & Schindler, 2003). The main objective of descriptive design is to give a description of the situation as it is (Malhotra, 1996).

Cooper & Schindler (2003), further describe this method as a study based on univariate questions or hypothesis where it seeks to determine the state of the existing relationships between variables, and characteristics of those variables by attempting to answer who, What, Where and how questions. Descriptive design is appropriate in providing the information on the factors contributing to occurrence of cybercrime on E-banking in Commercial banks in Kenya. The dependent variable of the study is occurrence of cybercrime on E-banking in Commercial banks in Kenya. And the independent variables are level of existing cyber security, effectiveness of the existing regulations, employee competence and awareness.

3.3 Population and Sampling Design

3.3.1 Population

The population defines the whole set of the objects or events under investigation about which inferences are made (Cooper & Schindler, 2003). The population is the larger set
of observations in which a smaller set called a sample is drawn. The population of the study was the 41 ICT experts working of the Commercial banks based in Nairobi. A sample was drawn from this population.

3.3.2 Sampling Design and Sample Size

3.3.2.1 Sampling Frame

A sampling frame is an objective list of the population from which a searcher can make a selection (Martin, 1998). The basic idea of sampling is that of selecting some of the elements in the population, where one can draw conclusions about the entire population. Therefore a sample frame is a representation of the elements of the target population that consists of all the elements of that population (Cooper & Schindler, 2003). In this study the sampling frame is the ICT experts working in commercial banks based in Nairobi.

3.3.2.2 Sampling Technique

Sampling is a means of selecting some or part of a group to represent the entire group or the population of interest. Sampling reduces the length of time to complete a research. It cuts costs, is manageable, it increases accuracy and is almost a mirror of the sample population (Babbie, 2004). For this study, random sampling technique was used. According to Black (1999), random sampling technique gives strengthen the validity of evaluation results and each element is given equal chance hence the reason for adopting it in this study.

3.3.2.3 Sample Size

A sample is a finite part of a statistical population whose properties are studied to gain information about the whole. Determining the appropriate sample size is vital. This is because an inadequate sample size may lead to results which are not significant statistically and which cannot be generalized to the whole population (Kitchenham & Lawrence, 2002).
For this study, the sample size of is informed by the sample size used by Soni R, Soni Neena and Anwar Rajasthan in their research Investigative Study of Banking Cyber frauds with Special reference to Private and Public sector Bank.

A confidence interval of 95% was employed which is according to Saunders, Lewis and Thornhill (2005), is the level of certainty of the characteristics collected represented as the characteristics of the whole population. The margin of error expected which is the accuracy required by the researcher for the estimates made from the sample is 2, representing a total of 14 commercial banks from which 41 respondents expected to take part in the survey.

Table 3.1: Sample Size

<table>
<thead>
<tr>
<th>No.</th>
<th>Name of Commercial Bank</th>
<th>Number of Questionnaires</th>
<th>Percentage of the Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>African Banking Corporation Ltd.</td>
<td>2</td>
<td>4.88</td>
</tr>
<tr>
<td>2</td>
<td>Bank of Africa Kenya Ltd</td>
<td>2</td>
<td>4.88</td>
</tr>
<tr>
<td>3</td>
<td>Bank of Baroda (K) Ltd.</td>
<td>2</td>
<td>4.88</td>
</tr>
<tr>
<td>4</td>
<td>Barclays Bank of Kenya Ltd.</td>
<td>3</td>
<td>7.32</td>
</tr>
<tr>
<td>5</td>
<td>CFC Stanbic Bank Ltd</td>
<td>4</td>
<td>9.76</td>
</tr>
<tr>
<td>6</td>
<td>Chase Bank (K) Ltd.</td>
<td>4</td>
<td>9.76</td>
</tr>
<tr>
<td>7</td>
<td>Citibank N.A Kenya</td>
<td>1</td>
<td>2.44</td>
</tr>
<tr>
<td>8</td>
<td>Commercial Bank of Africa Ltd.</td>
<td>3</td>
<td>7.32</td>
</tr>
<tr>
<td>9</td>
<td>Development Bank of Kenya Ltd.</td>
<td>1</td>
<td>2.44</td>
</tr>
<tr>
<td>10</td>
<td>Equity Bank Ltd.</td>
<td>3</td>
<td>7.32</td>
</tr>
<tr>
<td>11</td>
<td>Family Bank Limited</td>
<td>5</td>
<td>12.20</td>
</tr>
<tr>
<td>12</td>
<td>Kenya Commercial Bank Ltd</td>
<td>4</td>
<td>9.76</td>
</tr>
<tr>
<td>13</td>
<td>K-Rep Bank Ltd</td>
<td>3</td>
<td>7.32</td>
</tr>
<tr>
<td>14</td>
<td>National Bank of Kenya Ltd</td>
<td>4</td>
<td>9.76</td>
</tr>
</tbody>
</table>

41  100.00

3.4 Data Collection Methods
The study used both primary and secondary data. Primary data was collected by use of a structured questionnaire and secondary data was drawn from review of organizations’ profiles and journals, the internet, books, magazines, past research findings among others. Cooper and Schindler (2003), defines primary data as original search where data being collected is designed specifically to answer the research questions.

Data was collected using a questionnaire developed by the researcher drawn from the three research questions. This questionnaire was self-administered and shared with respondents in two different ways. One was by hand delivery and the second was through emails. The researcher ensured that confidentiality was maintained and the respondents were not expected to reveal their identity while filling in the questionnaires.

The questionnaire comprised of both open ended and closed ended questions. It was divided into two sections; section one comprised of general questions which assisted the researcher to get general information on the respondent while section two had closed ended questions with multiple choice options for the respondent to select from.

### 3.5 Research Procedures

Prior to administering the questionnaire to the intended respondents the tool was pretested. This step is critical as it assisted the researcher in determining whether the questionnaire was well understood by the intended respondents, in determining the time requires in answering the questions and in establishing whether from the questions asked, the researcher could obtain the information which was intended. With the feedback collected from the pretest, the researcher amended the tool and issued it to the intended respondents for their responses.

So as to ensure that the response rate is high, a cover letter from the University was attached on to the questionnaires, the researcher constantly follow up on the respondents to check on the progress of filling the questionnaires, the researcher also assured the respondents of confidentiality of their responses.

### 3.6 Data Analysis Methods
This process includes several stages. Data preparation entailed obtaining information and insights from the data which was obtained. This was necessary as it helped in avoiding erroneous judgments and conclusions.

Sorting was done by uniquely identifying each of the questionnaires for ease of reference. Editing was used to check and adjust data to ensure that omissions, legibility and consistency are appropriately were handled. The next step was coding. This entailed identifying and assigning numerical scores onto the edited data. The researcher contacted the respondents in cases where researcher needed to clarify some issues identified with the specific questionnaires. The data was transcribed into SPSS. This entailed keying in the data into the data analysis tool for it to be analyzed.

The data was analyzed using both descriptive and inferential statistics such as regression analysis to identify the relationship between variables. The results from the analysis was presented in table and figures.

3.7 Chapter Summary

This chapter covered the methodology and procedures that was used to collect and analyze the data collected for the study. This chapter dealt with the type of research design, the population, the sampling design, data collection methods and data analysis. The data was collected from 41 IT managers from commercial banks who are based in Nairobi. Questionnaires were developed and used for purposes of collecting data which was analyzed by use of SPSS. The methodologies mentioned above facilitated the presentation of the research findings in form of charts and graphs. The next chapter presents the findings of the research.
CHAPTER FOUR

4.0 RESULTS AND FINDINGS

4.1 Introduction

The study sought to find out factors contributing to occurrence of cybercrime on e-banking in commercial banks in Kenya. The specific objectives were to determine the level of cyber security on commercial banks in Kenya, to assess the effectiveness of existing regulation on cybercrimes in Kenya and to determine how employee awareness and competence influences occurrence of cybercrimes in commercial banks in Kenya. Methodology on how to carry out the research was then provided allowing successful collection of data from a sample of 41 respondents. Data was collected using a questionnaire instrument containing 52 items.

This chapter dealt with the report of the research findings based on the data collected from a total population of 14 banks. Data was collected from 41 ICT experts. This study was targeting a sample of 41 respondents attaining a 100% response rate of the total response rate. The questionnaires were then coded individually and input into SPSS for analysis. Data was tabulated and presented in the form of frequencies and percentages, in charts and tables. The chapter is structured on the basis of background information, that is, general report of the respondents, the way they responded to each of the variables contained in the questionnaire regarding, factors contributing to occurrence of cybercrime on e-banking in commercial banks in Kenya. The chapter ends with summary.

4.2 Demographic Information

This section provided personal information on the ICT professionals sampled, for validity. Validity provides personal data on the sample population for authentication. This is achieved by describing the respondents’ views as indicated on the questionnaires on determinants of the level of cyber security on commercial banks in Kenya, assessment of effectiveness of existing regulation on cybercrimes in Kenya and determinants of employee awareness and competence influences occurrence of cybercrimes in commercial banks in Kenya. The results are presented next.
4.2.1 Gender of Population

Table 4.2.1 shows that there was a total of 41 respondents. 68% of the total sample indicated that they were male while 32% indicated that they were females.

Graph 4.2.1: Gender of the Population

4.2.2 Age of Respondents

Fifteen Percent (15%) of the respondents said that they were below 25 years, 12% said that they were between 36 to 50 years and 73% said that they were aged between 25 to 35 years. Graph 4.2.2 shows these representations diagrammatically

Graph 4.2.2: Age of Respondents
4.2.3 Highest Level of Education

The level of education was important for the study because it showed that majority of the respondents were IT experts and therefore able to respond to the research questions accordingly. Fifty three percent (53%) of the respondents said that their highest level of education was a first degree followed by 28% of the respondents said that their highest level of education was a master’s degree and 20% of the respondents said that their highest level of education was a professional certificate. Graph 4.2.2 diagrammatically represents the above pinions.

Graph 4.2.3: Highest Level of Education

<table>
<thead>
<tr>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Masters</td>
</tr>
<tr>
<td>1st Degree</td>
</tr>
<tr>
<td>Professional Certification</td>
</tr>
</tbody>
</table>

4.2.4 Position within the Bank

The study tried to find to find out the positions the respondents held in their organizations. 36.6% of the respondents responded that they were IT Managers, 14.6% responded that they were System Administrators, 9.8% responded that they were IT Assistants, 7.3% responded that they were Assistant System Administrators, 4.9% responded that they were Data Analysts and 2.4% of the respondents said to hold the positions of ICT Administrator, Network Administrator, Network Associate, Security Officer and Senior Database Administrator. The above is shown in Graph 4.2.4.
Graph 4.2.4: Position within the Bank

4.2.5 Average Income per Month

This information was useful in asserting that the majority of the sampled respondents were employees of banks. 51.3% of those sampled said that they earn between 50001-150000, 38.5% said that they earn between 150001-300000 and 10.3% said that they earn below 50,000 per month. The above is illustrated in Graph 4.2.5 below.

Graph 4.2.5: Average Income Per Month
4.2.6 Computerized Operations

The study sought to find out whether the banks had computerized their operations. 100% of the sampled respondents said that their banks had computerized their operations. The respondent’s responses are tabulated in table 4.2.4 below.

Table 4.2.4: Computerized Operations

<table>
<thead>
<tr>
<th>Computerized Operations</th>
<th>Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Frequency</td>
</tr>
<tr>
<td>Yes</td>
<td>41</td>
</tr>
</tbody>
</table>

4.2.7 Existence of E-Banking Services

The study sought to find out whether the banks have e-banking services in place. The results as reflected in Graph 4.2.6, showed that 97.6% of the sampled banks offer e-banking services while only 2.4% of the banks indicated they did not have e-banking services.

Graph 4.2.6: Bank has e-banking Services

4.2.8 Importance of Cyber Security
The study sought to find out how important cyber security matters were with reference e-banking services on the sampled banks. 87% of the respondents pinioned that cyber security was very important while 13% of the respondents pinioned that cyber security was important. 4.9% of the respondents did not respond on this.

Graph 4.2.7: Importance of Cyber Security

<table>
<thead>
<tr>
<th>Importance of Cyber Security with Reference to E-Banking Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very important: 87%</td>
</tr>
<tr>
<td>Important: 13%</td>
</tr>
</tbody>
</table>

4.2.9 Number of Account Holders

The study sought to find out the number of account holders in each bank. Graph 4.2.8 shows that Nine or 22% of the respondents said that they have 2000,000 account holders; 12.2% of the respondents said that they have 1000,000 account holders; 7.3% of the respondents said that they have 3000,000 account holders; 4.9% of the respondents said that they have 5000000 account holders, 4.9% of the respondents said that they have 4000,000 account holders; 4.9% of the respondents said that they have 150,000 account holders. 2.4% of the respondents said that they have 1000,000, 1-500000, 1,250,000, 6000, 000 and 1250000 account holders.
4.2.10 Number of Account Holders Using E-Banking Services

The study sought to find out the number of account holders using e-banking services. As shown in graph 4.2.9, 38% of the respondents said that 50,000 account holders were using e-banking services followed by 28% of the respondents said that 5001-20,000 account holders were using e-banking services; 18% of the respondents said that between 20,000-50,000 account holders were using e-banking services.
4.3 Factors Contributing to the Occurrence of Cybercrime on E-Banking in Commercial Banks in Kenya

The study sought to find out the factors contributing to the occurrence of cybercrime on e-banking in commercial banks in Kenya. This information was important because it provides ways of streamlining gaps that are contributing to the occurrence of cybercrime hence reduce cybercrime incidences. The next section provides the results on factors contributing to the occurrence of cybercrime in e-banking in commercial banks in Kenya.

4.3.1 Determining the Impact of Using Technology on Customer Levels

The study sought to find out the impact of using technology on customer levels. The results as shown in Graph 4.3.1 revealed that 88% of the respondents said that the customer numbers had increased as a result of using of technology. 5% of the respondents said that the customer numbers had reduced as a result of using of technology and 7% of the respondents said that there had been no change resulting from the use of Technology.
4.3.2 Knowledge of What Cybercrime is

The study sought to find out the respondents’ knowledge of what cybercrime is. Ninety Four point Four Percent (94.4%) of the respondents indicated that they understood what is all about while 5.6% of the respondents indicated they did cybercrime not know what cybercrime is all about. This is represented in graph 4.3.2 below.

Graph 4.3.2: Know what Cybercrime is

The results also revealed that there was a significant positive relationship between level of education and knowledge of cybercrime through cross tabulation. The results, table...
4.3.1 showed that majority of those with certification in cybercrime also had 1<sup>st</sup> degrees 52.9% and 100% of them said that they knew what cybercrime is as opposed to some masters holders without certification in cybercrime and said that they did not know what cybercrime is.

Table 4.3.1: Relationship between Level Of Education Vs Knowledge Of Cybercrime

<table>
<thead>
<tr>
<th>Highest Level of Education</th>
<th>Know what Cybercrime is</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Professional Certification</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>% within Know what Cybercrime is</td>
<td>23.5%</td>
<td>0.0%</td>
</tr>
<tr>
<td>1&lt;sup&gt;st&lt;/sup&gt; Degree</td>
<td>18</td>
<td>0</td>
</tr>
<tr>
<td>% within Know what Cybercrime is</td>
<td>52.9%</td>
<td>0.0%</td>
</tr>
<tr>
<td>Masters</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>% within Know what Cybercrime is</td>
<td>23.5%</td>
<td>100.0%</td>
</tr>
<tr>
<td>Total</td>
<td>34</td>
<td>1</td>
</tr>
<tr>
<td>% within Know what Cybercrime is</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

4.3.3 Existence of Network Security Policy

The study sought to find out whether the commercial banks had a network security policy. As shown in Graph 4.3.3. Ninety two point Seven Percent (92.7%) of the respondents indicated that they have a network security policy while 7.3% of the respondents indicated they did not have a network security policy.
Graph 4.3.4: Existence of Network Security Policy

4.3.4 Existence of a Disaster Recovery Site

The study sought to find out whether the commercial banks had a disaster recovery site. As shown in table 4.3.5, 92.5% of the respondents agreed to have a disaster recovery site while 7.5% of the respondents disagreed to having disaster recovery site.

Graph 4.3.5: Existence of a Disaster Recovery Site
4.3.5 Duration of Servicing the Disaster Recovery Site

The study sought to find out how often the disaster recovery site is serviced. As shown in table 4.3.4, 75% of the respondents said that they serviced their disaster recovery site between 0-6 months while 25% of the respondents said that they serviced their disaster recovery site between 12-24 months. Two Point Four percent (2.4%) of the respondents did not respond to this question.

Graph 4.3.6: How Often the Disaster Recovery Site is serviced
4.3.6 Existence of a Firewall

Ninety Seven point five percent (97.5%) of the respondents articulated that their organizations used firewalls and 2.5% of the respondents articulated that their organizations did not use firewalls. The results of these responses are shown on Graph 4.3.7.

Graph 4.3.7: Existence of a Firewall

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>Missing</th>
</tr>
</thead>
<tbody>
<tr>
<td>97.5</td>
<td>2.5</td>
<td>2.4</td>
</tr>
</tbody>
</table>

4.3.7. Frequency of Reviewing Firewall Configurations

The study sought to find out the frequency of reviewing firewall configurations by the commercial banks. Graph 4.3.8 diagrammatically represents the respondent’s responses that 50% of the respondents indicated that they review the configurations of their
firewalls often; 48% indicated they review their firewalls very often while 3% indicated they review their firewall configurations sometimes.

Graph 4.3.8: Frequency of Reviewing Firewall Configurations

4.3.8 ICT Staff in have Undergone Cyber Security Training

The study sought to find out if ICT staff have undertaken cyber-security training. Seventy Five percent (75%) of the respondents stated that they agreed that the ICT staff had been trained; 14.6% stated that they strongly agreed that their ICT Staff had undergone Cyber Security training while 9.8% stated that they disagreed that their ICT Staff had undergone Cyber Security training. These responses are in table 4.3.9 below.

Graph 4.3.9: ICT Staff in have Undergone Cyber Security Training
4.3.9. Bank Employs the Use of Antivirus

The study sought to find out if the commercial banks in Kenya employ the use of an antivirus. Ninety five point one percent (95.1%) of the respondents indicated that they use an antivirus while 4.9% of the respondents indicated that they do not employ the use of an antivirus. Graph 4.3.10 below tabulates the respondent’s views.

Graph 4.3.10: Bank employs the use of Antivirus

4.3.10 Authentication Methods Used: Biometrics
The study sought to find out the authentication methods used in the Kenyan commercial banks. As per the diagrammatic representation in Graph 4.3.11, 58.5% of the respondents indicated that they use biometrics as a method of accessing a network while 39% of the respondents indicated that they do not use biometrics as a method of accessing a network while.

Graph 4.3.11: Authentication Methods Used: Biometrics

<table>
<thead>
<tr>
<th>Authentication Methods Used: Biometrics Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>58.5</td>
</tr>
</tbody>
</table>

As per the responses given by the respondents, there was a significant positive relationship between biometrics used as authentication method and highest level of education $r (39) = .445$. $p=0.004$ as shown in table 4.3.9

Table 4.3.9: Correlation between Biometrics used as Authentication Method Vs Highest Level of Education
<table>
<thead>
<tr>
<th>Pearson Correlation Significance (2-Tailed)</th>
<th>.445**</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>0004</td>
</tr>
<tr>
<td></td>
<td>40</td>
</tr>
</tbody>
</table>

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

### 4.3.11 Authentication Methods Used: Passwords

The study sought to find out the authentication methods used in the Kenyan commercial banks. As per the illustration on Graph 4.3.12, 82.9% of the respondents indicated that they use a password as a method of accessing a network while 17.1% of the respondents indicated they did not use passwords as an authentication method in their banks.

Graph 4.3.12: Authentication Methods Used: Passwords

<table>
<thead>
<tr>
<th>Authentication Methods Used: Passwords Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>82.9</td>
</tr>
<tr>
<td>17.1</td>
</tr>
</tbody>
</table>

### 4.3.12 Authentication Methods Used: Cards

The study sought to find out the authentication whether the commercial banks were using cards as a method of preventing cybercrime. As per the illustration on Graph 4.3.13,
63.4% of the respondents mentioned that they use cards as a method of accessing a network while 36.6% of the respondents mentioned that they did not use passwords as an authentication method in their banks.

Graph 4.3.13 Authentication Methods Used: Cards

<table>
<thead>
<tr>
<th>Authentication Methods Used: Cards Percent</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Methods Used:</td>
<td>63.4</td>
<td>36.6</td>
</tr>
</tbody>
</table>

4.3.13 No Authentication Methods Used

The study sought to find out if the commercial banks had methods of authenticating a customer or user into the network. Ninety Percent (90%) of the respondents pronounced that they use authentication methods and only 10% of the respondents pronounced that they did not use authentication methods. graph 4.3.13 Shows these responses in a Graph.

Graph 4.3.13: No Authentication Method being used
4.3.14 Authentication Methods Used- Rankings

Table 4.3.12 shows the rankings of the authentication methods used as per the responses of the various respondents. Majority of the respondents ranked the use of no authentication method the highest, followed by the second highest ranking as per the respondents responses was the use of biometrics, this was followed by the use of cards which ranked third by the respondents and finally the use of passwords which was ranked least by the respondents. Graph 4.3.14 shows these rankings diagrammatically.

Graph 4.3.14: Authentication Methods Used

4.3.15 Bank has an Intrusion Detection System for Logical Intrusions
The study sought to find out whether the banks have an intrusion detection system for logical intrusion as a constituent of threat model and prevention. Graph 4.3.15 diagrammatically shows the respondents responses. Twenty Nine point three percent (29.3%) of the respondents expressed that they strongly agreed that their banks employed the use of intrusion detection systems, 68.3% of the respondents expressed that they agreed that their banks employed the use of intrusion detection systems agreed and 2.4% of the respondents expressed that they disagreed that their banks employed the use of intrusion detection systems.

Graph 4.3.15: Bank has an Intrusion Detection System for Logical Intrusions

<table>
<thead>
<tr>
<th>Bank has Intrusion Detection Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Agree</td>
</tr>
<tr>
<td>29.3</td>
</tr>
</tbody>
</table>

There was a significant negative relationship between bank has an intrusion detection system for logical intrusions and marital status $r (39) = -.457. p=003$. Graph 4.3.16 shows that as per the respondents’ responses, there was an inverse relationship between
the two variables. This is was revealed by the respondents indicating that they strongly agree or agree 17% and 44% respectively, that organizations which have reported cases of cyber-crime did not have an intrusion detection system for logical intrusion and those had an intrusion detection system for logical intrusions seldom report cases of cyber-crime.

Graph 4.3.16: Relationship between Organizations has Reported Cases of Cybercrime and Bank has an Intrusion Detection System for Logical Intrusions

4.3.16 Bank Stores Data in Encrypted Format

The study sought to find out whether the banks store data in encrypted format as a constituent of threat model and prevention. As represented in table 4.3.17, 75.6% of the respondents pinioned that their banks store data in encrypted format while 24.4% of the respondents pinioned that their banks store do not data in encrypted format.

Graph 4.3.17: Bank Stores Data in Encrypted Format
A cross tabulation showed that there was a positive relationship intrusion detection system in banks that store data in encrypted format. The results in graph 4.3.18 showed that majority of the respondents either strongly agreed or agreed 46% that banks with an intrusion detection system for logical intrusion store data in encrypted format.

Graph 4.3.18: Relationship between Organization Banks that Stores Data in Encrypted Format Vs Bank has an Intrusion Detection System for Logical Intrusions
4.3.17 How Often the Banks Updates/Patches their Software

The study sought to find out how often the banks update/patch their software as a constituent of threat model and prevention. The results in Graph 4.3.18 showed that 70.7% or the respondents expressed that they update/patch their software between 0-6 months, 24.4% or the respondents expressed that they update/patch their software between 12-24 months and 4.9% of the respondents expressed that they update/patch their software within a period of more than 24 months.

Graph 4.3.19: How Often the Banks Updates/Patches their Software

<table>
<thead>
<tr>
<th>Duration of Updating Software</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 6 Months</td>
<td>70.70%</td>
</tr>
<tr>
<td>12-24 Months</td>
<td>24.40%</td>
</tr>
<tr>
<td>More than 24 Months</td>
<td>4.90%</td>
</tr>
</tbody>
</table>

Table 4.3.1: Correlation between how Often the Banks Updates/Patches their Software versus Average Income per Month
Correlation Test | How often bank updates/patches its software vs average income per month
--- | ---
Pearson Correlation Significance (2-Tailed) | -.553**
N | 39

*. Correlation is significant at the 0.05 level (2-tailed).
**. Correlation is significant at the 0.01 level (2-tailed).

### 4.3.18 Bank has Employees Charged with the Responsibility of Media Monitoring

The study sought to find out whether the banks have employees charged with the responsibility of media monitoring as a constituent of threat model and prevention. The results in Graph 4.3.19 revealed that 65.9% of the respondents stated that their organizations had employees charged with the responsibility of media monitoring while 34.1% of the respondents stated that their organizations did not have employees charged with the responsibility of media monitoring.

Graph 4.3.20: Bank has Employees Charged with the Responsibility of Media Monitoring
4.3.19 Bank having a Risk Department Dealing with Risk Associated with Technology

The study sought to find out whether the banks had a risk department dealing with risk associated with the technology as a constituent of threat model and prevention. The results in Graph 4.3.20 enumerated that 46.3% of the respondents indicated that they strongly agreed that their firms had risk departments dealing with risk associated with technology; 51.2% of the respondents indicated that they agreed that their firms had risk departments dealing with risk associated with technology agreed while 2.4% of the respondents indicated that they disagreed that their firms had risk departments dealing with risk associated with technology.

Graph 4.3.21: Bank having a Risk Department

4.4 Assessing the effectiveness of Existing Regulation

4.4.1. Reporting Any Cases of Cybercrime

The study sought to find out whether commercial banks reported any cases of cybercrime. Sixty one point one percent (61.1%) of the respondents cited that they had not reported any cases of cybercrime while 38.9% of the respondents cited that they had reported any cases of cybercrime. The diagrammatic representation of these citing is shown in Graph 4.4.1
Graph 4.4.1 Reporting Any Cases of Cybercrime

<table>
<thead>
<tr>
<th>Organisations Which Have Reported Cyber Crime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
</tbody>
</table>

4.4.2 How Often the Banks Review the Firewall Policies

The study sought to find out how often the banks reviewed the firewall policies as a way of regulating cybercrime. Graph 4.4.2 is a pictographic representation of the responses from the respondents. Sixty five percent (65%) of the respondents indicated they reviewed their firewall policies in less than 6 months, 32.5% of the respondents indicated they reviewed their firewall policies in a duration of between 7-24 months while 2.4% of the respondents indicated they reviewed their firewall policies in more than 24 months.
Graph 4.4.2: How Often the Bank Reviews the Firewall Policies

From the respondents responses. There was a significant negative relationship between how often the bank reviews the firewall policies and the average income per month $r (36) = -.440. p=006$

4.4.3 Bank has a Cyber –Security Policy

The study sought to find out how often the banks had a cyber-security policy as a way of regulating cybercrime. Graph 4.4.3 is a visual representation of the responses given by the respondents. Of all the respondents, 93% of them specified they had a cyber-security policy while 7% of them specified they did not have a cyber-security policy.

Graph 4.4.3 Bank has a Cyber –Security Policy
4.4.4 Cyber Security Policy Addresses how to get back from an Attack

The study sought to find out whether the banks that had a cyber-security policy, which described how to get back from an attack. Fifty Two point five percent (52.5%) of the respondents indicated that they agreed that their Cyber Security policies described on how to get back from an attack. 40% of the respondents indicated that they strongly agreed that their Cyber Security policies described on how to get back from an attack, 5% of the respondents disagreed that their Cyber Security policies described on how to get back from an attack and 2.5% of the respondents indicated that they strongly disagreed that their Cyber Security policies described on how to get back from an attack. 2.4% of the respondents did not respond to this question.

Graph 4.4.4 Cyber Security Policy Addresses how to get back from an Attack

<table>
<thead>
<tr>
<th>Cyber Security Policy Addresses How To Get Back From An Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Response Percent</th>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
<th>Missing</th>
</tr>
</thead>
<tbody>
<tr>
<td>40%</td>
<td>52.50%</td>
<td>5%</td>
<td>2.50%</td>
<td>2.40%</td>
<td></td>
</tr>
</tbody>
</table>

4.4.5 Awareness of the Proposed National Cyber Security Policy

The study sought to find out whether the banks were aware of the proposed National Cyber Security Policy which is a way of regulating cybercrime. Graph 4.4.5 is a pictorial representation of the responses obtained from the respondents. Sixty Seven point five percent (67.5%) of the respondents expressed they were aware of the proposed national
cyber security policy while 31.7% of the respondents expressed they were not aware of the proposed national cyber security policy.

Graph 4.4.5 Awareness of the Proposed National Cyber Security Policy

4.4.6 The Cyber Security Policy in Kenya Serves the Banking Industry Adequately

The study sought to find out from the banks whether the Cyber Security Policy in Kenya Serves the Banking Industry adequately in tandem with nationally recognized standards. Graph 4.4.6 exhibited that 55% of the respondents pronounced that they agreed the Cyber Security Policy in Kenya serves the banking industry adequately, 14.6% of the
respondents pronounced that strongly agreed the Cyber Security Policy in Kenya serves the banking industry adequately, 26.8% of the respondents pronounced that they agreed the Cyber Security Policy in Kenya serves the banking industry adequately 2.4% of the respondents pronounced that they strongly disagreed that the Cyber Security Policy in Kenya serves the banking industry adequately.

Graph 4.4.6 the Cyber Security Policy in Kenya Serves the Banking Industry Adequately

| The Cyber Security Policy in Kenya Serves the Banking Industry Adequately |
|---|---|---|---|---|---|
| Strongly Agree | Agree | Disagree | Strongly Disagree | Missing |
| 15% | 55% | 27.50% | 2.50% | 2.4 |

4.4.7 Computers in Banks are Secure from Cyber Criminals
The study also sought to assess from the respondents on whether computers in banks were secure from cyber criminals as an insight into existing cyber regulation. The results in Graph 4.4.7 diagrammatically represent the responses where 61.5% of the respondents expressed that they strongly agreed that the computers in their organizations were secure from cyber criminals, while 15.4% of the respondents expressed that they strongly agreed. Twenty three point one percent of the respondents expressed that they disagreed.

Graph 4.4.7 Computers in Banks are Secure from Cyber Criminals

<table>
<thead>
<tr>
<th></th>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Disagree</th>
<th>Missing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response Percent</td>
<td>15.4</td>
<td>61.5</td>
<td>23.1</td>
<td>4.9</td>
</tr>
</tbody>
</table>

4.4.8 Bank employed the use of Automated Teller Machines

The study sought to assess whether banks employ the use of automated teller machines. Ninety Two point five percent (92.5%) of respondents stated that their banks employ the use of Automated teller Machines while 7.5% of respondents stated that their banks did not employ the use of Automated teller Machines. These statements are diagrammatically denoted below in Graph 4.4.8.
Graph 4.4.8 Bank Employed the use of Automated Teller Machines

4.4.9 Bank has Employed the Use of Technology to Serve its Customers
The study sought to assess whether banks employ the use of technology to serve customers. The results from the respondents are denoted in Graph 4.4.9 below. Fifty Two point Six percent (52.6%) of the respondents indicated that they strongly agree that their organizations employed the use of Technology to serve their customers, 47.4% of the respondents indicated that they agree that their organizations employed the use of Technology to serve their customers, seven point three of the respondents did not respond to this question.

Graph 4.4.9 Bank has employed the use of Technology to serve its Customers

<table>
<thead>
<tr>
<th></th>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Missing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response Percent</td>
<td>52.60%</td>
<td>47.40%</td>
<td>7.30%</td>
</tr>
</tbody>
</table>

4.4.10 Aspects of the Proposed National Cyber Security Policy to Incorporate

The study sought to assess the aspects of the proposed National Cyber Security Policy the respondents would incorporate into their organizations cyber security policy. A multiple
response analysis provided the results on Graph 4.4.10. Forty point Two Percent (40.2%) of the respondents indicated that they would incorporate the Information Security Policy followed by the Management Controls and Procedures. The respondents ranked Cyber Security Systems and Access Management systems at 60.9% in their list of priorities.

Graph 4.4.10: Aspects of the Proposed National Cyber Security Policy to Incorporate

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>3</td>
<td>10</td>
<td>15</td>
<td>12</td>
</tr>
<tr>
<td>YES</td>
<td>37</td>
<td>30</td>
<td>25</td>
<td>28</td>
</tr>
</tbody>
</table>

4.4.11 Bank had Educated its Customers to Protect Themselves from Cyber Stalking
The study sought to find out whether the bank has educated its customers to protect themselves from cyber stalking. Fifty Six Percent (56%) of the respondents indicated that they agreed that they had educated customers to protect themselves from cyber stalking while 18% of the respondents indicated that they strongly disagreed that they had educated customers to protect themselves from cyber stalking; 13% of the respondents indicated that they disagreed that they had educated customers to protect themselves from cyber stalking and another 13% of the respondents indicated that they strongly agreed that they had educated customers to protect themselves from cyber stalking.

Graph 4.4.11: Bank had educated its Customers to Protect Themselves from Cyber Stalking
4.4.12 Electronic Banking Guidelines are Sufficient to Provide a Good Banking Environment

The study also sought to assess from the commercial banks whether the electronic banking guidelines were sufficient to provide a good banking environment. The responses collected from the respondents are represented in the Graph 4.4.12 below. Seventy Six point three percent (76.3%) of the respondents mentioned that they agreed that Electronic Banking Guidelines were sufficient to provide a good banking environment, 10.5% of the respondents mentioned that they strongly agreed that Electronic Banking Guidelines were sufficient to provide a good banking environment and 10.5% of the respondents mentioned that they disagreed that Electronic Banking Guidelines were sufficient to provide a good banking environment.

Graph 4.4.12 E-Banking Guidelines are Sufficient to Provide a Good Banking Environment

4.5 Determining Employee Competence and Awareness in Influencing Cybercrime in Banks

4.5.1. Number of non ICT Staff in Organization
The study sought to find out the number of non-ICT staff in commercial banks in Kenya. The results of the respondents feedback is tabulated in Graph 4.5.1. Forty three point six percent (43.6%) of the respondents stated that their organizations had 601-800 non ICT staff members, 28.2% of the respondents stated that their organizations had 0-200 non-ICT staff members, 10.3% of the respondents stated that their organizations had 401-600 non ICT staff in their organizations.

![Graph 4.5.1: Number of non ICT Staff in Organization](image)

### 4.5.2 Number of Staff Using the Computer as a Tool

The study sought to find out the number of staff in the Kenyan commercial bank using computers. The results in Graph 4.5.2 demonstrate that 43.6% of the respondents...
indicated that there were between 601-800 employees using computers as their daily working tool followed by 30.8% of the respondents indicated that there were between 0-200 employees using computers as their daily working tool; 15.4% of the respondents indicated that there were between 401-600 employees using computers as their daily working tool and lastly 10.3% of the respondents indicated that there were between 201-400 employees using computers as their daily working tool companies with 201-400 employees using computers.

Graph 4.5.2  No of Staff Using the Computer as a Tool

<table>
<thead>
<tr>
<th>No of Staff Using Computers as a tool</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-200</td>
<td>30.80%</td>
</tr>
<tr>
<td>201-400</td>
<td>10.30%</td>
</tr>
<tr>
<td>401-600</td>
<td>15.40%</td>
</tr>
<tr>
<td>601-800</td>
<td>43.60%</td>
</tr>
<tr>
<td>Missing</td>
<td>4.90%</td>
</tr>
</tbody>
</table>
4.5.3 Number of Non ICT Staff Trained on Cyber Security

The study sought to find out the number of non ICT staff trained on cyber security. The respondent’s responses are in Graph 4.5.3. Fifty Seven Point Nine Percent (57.9 %) of the respondents indicated that non ICT staff members in their organizations who were trained on cyber security were ranging between 0-200, 23.7% of the respondents indicated that non ICT staff members in their organizations who were trained on cyber security were ranging between 601-800 members, 18.4% of the respondents indicated that non ICT staff members in their organizations who were trained on cyber security were ranging between 201-400 non ICT staff members trained on cyber security.

Graph 4.5.3: No of Non ICT Staff Trained on Cyber Security

4.5.4. How Often Employees are required to Change Access Codes

73
The study sought to find out the effect of social engineering on Cybercrime. The results in Graph 4.5.4 showed majority of the respondents, 80.6% of the respondents articulated that their organizations require the employees to change the access codes in less than 6 months, followed by 10.3% of the respondents articulated that their organizations do not require their employees to change the access codes followed by 5.1% of the respondents articulated that their organizations require the employees to change the access codes between 7-24 months.

Graph 4.5.4: How Often Employees are required to Change Access Codes

<table>
<thead>
<tr>
<th>How Often Employees are Required to Change Access Codes Percent</th>
<th>0 - 6 Months</th>
<th>7-24 Months</th>
<th>Never</th>
<th>Missing</th>
</tr>
</thead>
<tbody>
<tr>
<td>How Often Employees are Required to Change Access Codes Percent</td>
<td>80.60%</td>
<td>5.10%</td>
<td>10.30%</td>
<td>4.90%</td>
</tr>
</tbody>
</table>

4.5.5 How Often the Bank Audits Logical Access Logs

The study sought to find out how often the local commercial banks audit the logical access. Fifty Seven point one percent (57.1%) of the respondents pronounced that their organizations audit the logical access logs in periods less than 6 months, followed by 31.4% of the respondents pronounced that their organizations audit the logical access logs in periods 7-24 months, 5.7% of the respondents pronounced that in the organizations audit their logical access logs are never audited. These pronouncements are represented in Graph 4.5.5 below.

Graph 4.5.5: How Often the Bank Audits Logical Access Logs
4.5.6 Bank Allows Mobile Banking for its Customers
The study sought to find out whether Kenyan banks allow mobile banking for its customers. Ninety three point one percent (93.1%) of the respondents indicated their banks allow mobile banking for their customers while 6.9% of the respondents indicated their banks allow mobile banking for their customers. The indications by the respondents are represented in Graph 4.5.6 below

Graph 4.5.6: Bank Allows Mobile Banking for its Customers
4.5.7 Number of ICT Staff in the Organization

The study sought to find out the number of ICT staff in the organization. Thirty three point three percent (33.3%) of the respondents indicated that their commercial banks had less than 10 staff members; 20.5% of the respondents indicated that their commercial banks had 21-30 ICT staff members in their organizations; 15.4% of the respondents indicated they had 11-20 ICT staff members in their commercial banks, 15% of the respondents indicated that their commercial banks had between 31-40 ICT staff members in their commercial banks and 15% of the respondents indicated that their commercial banks had more than 40 ICT staff members respectively. The results in graph 4.5.7

Graph 4.5.7: Number of ICT in Organization
4.5.8 Number of ICT Staff who have Undergone Training on Cyber Security

The study sought to find out how many of the ICT staff members had undergone through training. Forty eight point Seven percent (48.7%) of the respondents expressed that less than 10 ICT employees trained on cyber security; 25.6% of the respondents expressed that between 11-20 ICT employees had been trained on Cyber Security, 12.8% of the respondents expressed that between 31-40 employees ICT employees had been trained, 10.3% of the respondents expressed that more than 40 ICT employees trained on Cyber security and 2.6% of the respondents expressed that between 21-30 ICT employees had been trained on cyber security. Graph 4.5.8 shows the respondents expressions in a tabula format.

Graph 4.5.8: No of ICT Staff with Training on Cyber Security
4.5.9 Systems in Place Lock out Users after Several Failed Log on Attempts

The research sought to find out whether banks systems lock out users after several failed log on attempts as a way of mitigating cybercrime. Seventy Two percent (72%) of the respondents expressed that they strongly agreed that the systems in their commercial banks lock out users after several failed log on attempts, 26% of the respondents expressed that they agreed that the systems in their commercial banks lock out users after several failed log on attempts and 3% of the respondents expressed that they disagreed that the systems in their commercial banks lock out users after several failed log on attempts.
4.5.10 Exiting Employees are Removed from the System During the Exit Process
The study sought to find out whether the exiting employees were removed from the system during the exit process. Seventy one point Eight percent (71.8%) of the respondents indicated that they strongly agreed that exiting employees are removed from the system during the exit process., 25.60% of the respondents indicated that they agreed that exiting employees are removed from the system during the exit process and 2.60% of the respondents indicated that they disagreed that exiting employees are removed from the system during the exit process. Graph 4.5.10 shows the above responses diagrammatically.
4.5.11 System in Place Prevents Coping of Data by Unauthorized Personnel.

The study sought to find out whether the system in place prevented coping of data by unauthorized personnel. Sixty one percent (61%) of the respondents pinioned that they strongly agreed that in their organizations systems were in place to prevent coping of data by unauthorized personnel, 31% of the respondents pinioned that they agreed that in their organizations systems were in place to prevent coping of data by unauthorized personnel, 8% of the respondents pinioned that they disagreed that in their organizations systems were in place to prevent coping of data by unauthorized personnel.

### 4.5.12 Prior to Employment the Bank Vets Potential Employees

The study sought to find out whether prior to employment the bank vetted potential employee. Forty three point six percent (43.6%) of the respondents indicated that they strongly agreed that their organizations vet potential employees prior to employment, 41% of the respondents indicated that they agreed that their organizations vet potential employees prior to employment; 12.8% of the respondents indicated that they disagreed that their organizations vet potential employees prior to employment and 2.6% of the respondents indicated that they strongly disagreed that their organizations vet potential employees prior to employment. Graph 4.5.11 shows there representations.
Graph 4.5.11: Prior to Employment Bank Vets Potential Employees

4.5.13 The Bank Handles Disgruntled Employees well

The study sought to find out whether banks handled disgruntled employees well. The Graph 4.5.12 is a pictorial representation of the responses obtained. 53.8% of the respondents felt that their organizations handled disgruntled employees well, 25.6% of the respondents felt that their organizations did not handle disgruntled employees well while 10.3% of the respondents felt that their organizations handled disgruntled employees very well and another 10.3% of the respondents felt very negatively on how their organizations handled disgruntled employees.
Graph 4.5.12: The Bank Handles Disgruntled Employees well

<table>
<thead>
<tr>
<th></th>
<th>Response Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Agree</td>
<td>10.30%</td>
</tr>
<tr>
<td>Agree</td>
<td>53.80%</td>
</tr>
<tr>
<td>Disagree</td>
<td>25.60%</td>
</tr>
<tr>
<td>Missing</td>
<td>10.30%</td>
</tr>
</tbody>
</table>

4.5.14 Bank Employees had Been Educated to Recognize Social Engineering

The study sought to find out whether bank employees were educated to recognize social engineering. The Graph 4.5.13 tabulated the responses. 61.5% of the respondents indicated that they agreed that the institutions employees had been educated to recognise social engineering; 30.8% of the respondents indicated that they disagreed that their institutions employees had been educated to recognise social engineering, 5.1% of the respondents indicated that they strongly agreed that the institutions employees had been educated to recognise social engineering and 2.6% of the respondents indicated that they strongly disagreed that the institutions employees had been educated to recognise social engineering.
4.5.15 Bank Allows for Access to Personal Emails on Work Computers

The study sought to find out whether commercial banks allowed personnel to access personal email on work computers. Forty Eight point Six percent (48.6%) of the respondents stated that they disagreed, that their banks allow for access to personal email account on work computers, 29.7% of the respondents stated that they agreed, that their banks allow for access to personal email account on work computers, 16.2% of the respondents stated that they strongly agreed, that their banks allow for access to personal email account on work computers, while 5.4% of the respondents stated that they strongly disagreed, that their banks allow for access to personal email account on work computers.
Graph 4.5.14: Bank Allows for Access to Personal Emails on Work Computers

<table>
<thead>
<tr>
<th></th>
<th>Missing</th>
<th>Strongly Disagree</th>
<th>Disagree</th>
<th>Agree</th>
<th>Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Agree</td>
<td>16.20%</td>
<td>29.70%</td>
<td>48.60%</td>
<td>5.40%</td>
<td>9.80%</td>
</tr>
</tbody>
</table>

4.5.16 Banks Employ Sending of Authentication Messages to Mobile Devices.

The research sought to find out whether banks employed sending of authentication messages to mobile devices. Sixteen point two percent (16.2%) of the respondents said that they strongly agreed that their institutions send authentication messages to mobile devices; 29.7% of the respondents said that they agreed that their institutions send authentication messages to mobile devices 48.6% of the respondents said that they strongly disagreed that their institutions send authentication messages to mobile devices while 5.4% of the respondents said that they strongly disagreed that their institutions send authentication messages to mobile devices. The Graph 4.5.15 below depicts these responses.
The Bank Employed Sending of Authentication Messages to Mobile Devices

Graph 4.5.15: The Bank Employed Sending of Authentication Messages to Mobile Devices

4.5.17 Duration of Bank Auditing Logical Access Logs

The study sought to find out how often Kenyan commercial banks audit logical access logs. Fifty three point one percent (53.1%) of the respondents stated that their institutions audited their access logs after periods of less than 6 months, 31.3% of the respondents stated that their institutions audited their access logs after periods of between 7-12 months, and 12.5 of the respondents stated that their institutions audited their access logs after periods of more than 12 months.

Graph 4.5.16: Duration of Bank Auditing Logical Access Logs
4.5.18 Bank Communicates to the Public Using Social Media

The study sought to find out whether Kenyan commercial banks communicate to the public using social media. Thirty three point three percent (33.3%) of the respondents expressed that they strongly agreed that their institutions communicated to the public using social media and 33.3% of the respondents expressed that they agreed that their institutions communicated to the public using social media, 30.8% of the respondents expressed that they disagreed that their institutions communicated to the public using social media while 2.6% of the respondents expressed that they strongly disagreed that their institutions communicated to the public using social media. Graph 4.5.17 gives a pictorial view of these representations.

Graph 4.5.17: The Bank Communicates to the Public using Social Media

4.5.18 Bank Employed the Use of Cloud Computing
The study sought to find out whether commercial banks in Kenya employed the use of cloud computing. Fifty six point four percent (56.4%) of the respondents indicated that they agreed that their banks had employed the use of cloud computing. 25.6% of the respondents indicated that they strongly agreed that their banks had employed the use of cloud computing. 17.9% of the respondents indicated that they disagreed that their banks had employed the use of cloud computing. Graph 4.5.18 is a visual representation of the reactions.

Graph 4.5.18: Bank employed the use of Cloud Computing

![Bar Chart: Bank Employed the use of Cloud Computing](image)

<table>
<thead>
<tr>
<th></th>
<th>Response Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Agree</td>
<td>25.60%</td>
</tr>
<tr>
<td>Agree</td>
<td>56.40%</td>
</tr>
<tr>
<td>Disagree</td>
<td>17.90%</td>
</tr>
<tr>
<td>Missing</td>
<td>4.90%</td>
</tr>
</tbody>
</table>

4.5.19 The Recent Past Cyber Attacks Had Been on the Increase

The study sought to find out whether the recent past cyber-attacks had been on the increase. Fifty three point six percent (53.6%) of the respondents pinioned that they strongly agreed that in the recent past cyber-attacks had been on the increase, 32.1% of the respondents pinioned that they agreed that in the recent past cyber-attacks had been on the increase and 14.3% of the respondents pinioned that they disagreed that in the recent past cyber-attacks had been on the increase. Graph 4.5.19 shows in a tabular format the opinions of the respondents.
4.6 Chapter Summary

In summary, the study sought to find out factors contributing to occurrence of cybercrime on e-banking in commercial banks in Kenya. The results showed data was collected from 41 ICT experts. This study was targeting a sample of 30 respondents resulting in a 100% response rate.

Seventy three Percent (73%) of the respondents were aged between 25-35 years. There was representation of both gender majority being males who constituted of 68% of the total sample population. Fifty three percent (53%) of the respondents had a 1st degree, most of whom were IT experts while the lowest qualification was Professional certifications constituting 20% of the respondents. The sample comprised of ICT staff in various levels within a bank setup. This information was important for validity and authentication of the research. Of the above described respondents, Fifty Two point Six percent (52.6%) of the respondents indicated that they strongly agree that their organizations employed the use of Technology to serve their customers.
The study sought to find out the factors contributing to the occurrence of cybercrime on e-banking in commercial banks in Kenya. The study searched to find out the respondents' knowledge of what cybercrime is. The results showed that 94.4% of the respondents understood what cybercrime is all about and 87% pinned that cyber security was very important. The respondents also indicated the percentage of account holders who took advantage of E- Banking services. The percentage range as per the respondents was between 18% and 38%.

Ninety two point seven percent (92.7%) of the respondents specified that they have a network policy. Ninety two point five Percent (92.5%) of the respondents agreed to have a disaster recovery site. Ninety two point five percent (97.5%) of the commercial banks had a firewall. The respondents were also asked to indicate how often their firewall configurations were reviewed. The most frequent review was done in intervals described as very often and this response was given by 48% of the respondents while the one that was only reviewed sometimes was at 3%. The 95.1% of the respondents expressed that that Kenyan commercial banks employ the use of an antivirus. There was a significant positive relationship between biometrics used as authentication method and highest level of education $r(39) = .445$. p=004.

Of importance as well was to know the level of awareness, sensitization and education on cybercrime as if the ICT staff and the other staff in the commercial banks had been taken through the same. 14.6% stated that they strongly agreed that their ICT Staff had undergone Cyber Security training. With regards to the customers, Fifty Six Percent (56%) of the respondents indicated that they agreed that they had educated customers to protect themselves from cyber stalking. It is notable to say that Sixteen point two percent (16.2%) of the respondents said that they strongly agreed that their institutions send authentication messages to mobile devices.

There was also a representation of the various authentication methods used within the banks where the respondents pinned that the use of No authentication methods ranked highest, followed by the use of Biometrics.
As regards to the stored Data, 75.6% of the respondents pinioned that their banks store data in encrypted format and that. Twenty Nine point three percent (29.3%) of the respondents expressed that they strongly agreed that their banks employed the use of intrusion detection systems. In addition to this, 70.7% or the respondents expressed that they update/patch their software between 0-6 months.

From the opinions given by the respondents, 7% of them specified they did not have a cyber-security policy, 2.5% of the respondents indicated that they strongly disagreed that their Cyber Security policies described on how to get back from an attack strongly disagreed.2.4%,31.7% of the respondents expressed they were not aware of the proposed national cyber security policy, and 2.5% of the respondents articulated that their organizations did not use firewalls, 9.8% stated that they disagreed that their ICT Staff had undergone Cyber Security training, while 24.4% of the respondents pinioned that their banks store data in encrypted format. Fifteen point Four percent (15.4%) of the respondents expressed that they strongly agreed. Five point Seven Percent (5.7%) of the respondents pronounced that in their organizations audit the logical access logs are never audited.

The next chapter shall review and discus the results and findings of the study.
CHAPTER FIVE

5.0 DISCUSSION, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter reviews the results and findings of the study presented in the previous chapter. The purpose of the study, the research objectives and the research method used have been highlighted and explained. More exactly, the study population, the sample size, the data gathering method and the research procedure have also been discussed. A summary of the study has been presented with the three research questions aiding as assurance through which the inquiry into factors contributing to occurrence of cybercrime on e-banking in commercial banks in Kenya. This is finally followed by discussions, conclusions and recommendations for further development that have been proposed.

5.2 Summary

The purpose of the study was to investigate the factors contributing to occurrence of Cybercrime on the E-Banking Industry in Commercial Banks in Kenya. The study addressed the following objectives:

i. To determine the level of cyber security on commercial banks in Kenya.

ii. To assess the effectiveness of existing regulation on cybercrimes in Kenya.

iii. To determine how employee awareness and competence influences occurrence of cybercrimes in commercial banks in Kenya.

The research design used was descriptive. The results showed data was collected from 41 ICT experts. To select the respondents for this study, random sampling technique was used. Primary data was first edited, coded and then analyzed using Microsoft Excel and
SPSS computer packages. The interpreted data was grouped into common themes and was presented in the form of pie-charts, percentages, figures, tables and bar graphs.

The findings of the first specific objective regarding the level of cyber security on commercial banks in Kenya revealed that, 100% of the respondents indicated that they understood the importance of cyber security. Ninety two point Seven Percent (92.7%) of the respondents indicated that they had network security policies in place while 92.5% agreed to having a disaster recovery site. 75% of the respondents said that they serviced their disaster recovery site between 0-6 months, the rest had much longer periods in between the services. Ninety five point one percent (95.1%) of the respondents indicated that they use an antivirus.

The second specific objective was assessing the effectiveness of existing regulation. Sixty one point one percent (61.1%) of the respondents cited that they had not reported any cases of cybercrime. 40% of the respondents indicated that they strongly agreed that their Cyber Security policies described on how to get back from an attack. Sixty Seven point five percent (67.5%) of the respondents expressed they were aware of the proposed national cyber security policy. 76.9% of the respondents expressed that they agreed that the computers in their organizations were secure from cyber criminals.

The responses of the third specific objective on how employee awareness and competence influences occurrence of cybercrimes in commercial banks in Kenya. Seventy one point Eight percent (71.8%) of the respondents indicated that they strongly agreed that exiting employees are removed from the system during the exit process. Eighty four point six point six percent (84.6%) of the respondents indicated that they agreed that their organizations vet potential employees prior to employment. 53.8% of the respondents felt that their organizations handled disgruntled employees well.

5.3 Discussion

This section interprets the results of the findings of the study in respect to the recommended practice and the international practice. This study explores Cybercrime in relation to the three specific objectives, it highlights the gaps in the Kenyan practice and
recommends some solutions as well as other areas for further research. This study discusses how Kenyan banks are operating, the preventive measures being taken by the banks to prevent cybercrime from taking place, the detective measures they have undertaken so as to know when cybercrime is ongoing and the corrective measures to ensure that the banks are able to recover from an attack.

5.3.1 To Determine the Level of Cyber Security on Commercial Banks in Kenya.

As advised by Firewalls and Virtual Private Networks (2009), a network security policy needs to be in place. This is further backed by Tendulkar, 2013 who stated that robust cyber security and cyber resilience are important factors in mitigating impacts of cybercrime. The findings from the study are in line with the above advice where Ninety two point Seven Percent (92.7%) of the respondents indicated that they have a network security policy.

The respondents displayed knowledge of the importance of having Firewalls to protect their networks. Internal network security measures need to be set in place. Measures such as access controls and updating of software to the most current version should be regularly done, having up to date operational antivirus, regular review of firewall configuration and intrusion detection software (Siddique & Rehman, 2011). The study revealed that 97.5% of the commercial banks had a firewall and adhered to the recommendations by Siddique and Rehman. This was further supported by Limited (2011) who detailed that every request from a public network to the protected network must pass through a firewall.

The study revealed that 75% of the respondents agreed the ICT staff had been trained on cyber security. These findings were in line with Tendulkar, (2013) who asserts that Cyber-security measures could be easily side-stepped if the crime is perpetrated by an ‘insider’ Training for all staff is important and given the innovation of cybercrime, training is best executed periodically with staff being kept up-to-date on new threats and trends.

Internal network security measures need to be set in place. Measures such as access controls and updating of software to the most current version should be regularly done,
having up to date operational antivirus and intrusion detection software (Siddique & Rehman, 2011). From the survey, it was found that of the sampled commercial banks in Kenya, 95.1% of the respondents indicated that they use an antivirus and thus complied with the recommendations by Siddique & Rehman, (2011). In addition to this the sampled banks evidenced the use of various access control methods where 82.9% of the respondents indicated that they use passwords as a method of accessing a Network. Simmons (2012) supports these security enhancements as he states that it is necessary for organisations to take action to ensure that computer and physical security is well addressed. Moreover 97.6% of the sampled respondents from the banks indicated that they the use intrusion detection systems.

Bhasin (2007) eluded that in order to strengthen network security, a comprehensive approach with regards to physical, technical and administrative controls should be done. The study revealed that 75.6% of the responded indicated that banks are storing data in encrypted formats thus agreeing with Bhasin (2007) and Schulz(2006) who stated that banks are constantly transmitting Data over the networks, thus it was necessary for them to put in place measures such as Data Encryption, use of VPN’s and IPSEC protocols. Regarding the policies and procedures that addresses cybercrime, 92.7% of the respondents indicated that they have a network security policy already in place.

Siddique and Rehman (2011), advised on the use of three security preventive measures. Firstly, they stated that banks should ensure that they have a protection program that has power over cookies, which prevent internal information from being forwarded to other destinations outside the organization.

Siddique and Rehman (2011) further advice that it is important to have the latest software which is updated with the latest patches. This means that all known loopholes and bugs which have been discovered by the vendors have been patched and bugs resolved. Findings on how regularly the banking institutions patch their software indicated that that 70.7% or the respondents expressed that they update/patch their software in periods less than 6 months; this is in line with the recommendations.
Sixty five point nine percent (65.9%) of the respondents stated that their organizations had employees charged with the responsibility of media monitoring which is in line with Siddique and Rehman (2011) advice. Paula, Carol, Kevin, Martin and Barbra (2014) support Siddique and Rehman (2011) when they go ahead to explain that social media is a threat. It is a platform where disgruntled employees can engage in posting derogatory material, hate speech and cyber bullying.

5.3.2 To Assess the Effectiveness of Existing Regulation on Cybercrimes in Kenya.

The Kenya Cyber Security strategy was developed and launched in 2014. Seven point five percent (70.5%) of the respondents expressed they were aware of the existence of the policy. The respondents were asked about their priorities in implementing the main focuses, their responses were as follows; Forty point Two Percent (40.2%) of the respondents indicated that they would incorporate the Information Security Policy followed by the Management Controls and Procedures. The respondents ranked Cyber Security Systems and Access Management systems at 60.9% in their list of priorities.

Wang (2007) pronounces that new technologies open doors for new crimes and there has been an increase in the number of cybercrimes reported. However this does not seem to be the case in the Kenyan context as the 61.1% of the respondents indicated that they had not reported any cases of cybercrime.

Some of the earliest Technology adoptions were the use of ATM’s in Commercial banks in Kenya. The use of ATM is not only safe and sound but also suitable. This safety and convenience, has an evil side which is reflected in the form of “ATM FRAUD” that is an international problem (Mehta, 2011). Ninety Two point five percent (92.5%) of respondents stated that their banks employ the use of Automated teller Machines which is in agreement with Mehta (2011).

Banks have now gone a step further in enabling customers to operate their bank accounts from their mobile phones, computers and other mobile devices (Rashid, 2011). The Kenyan banks also demonstrated compliance to the same as revealed by 93.1% of the respondents indicating that their banks allow mobile banking for their customers. Hundred percent (100%) of the respondents indicated that their organizations employed
the use of Technology to serve their customers. Some other ways of using Technology included sending of authentication messages to the customer’s mobile devices. The responses from the sample on the use of this two factor authentication revealed that 94.5% of the respondents indicated said that their institutions send authentication messages to mobile devices.

According to Amaroso (2010), it is important to educate the users who are the key decision makers. It is now necessary to emphasize the importance of following the set security policy rules. Use of access codes is one such mechanism that is used to authenticate users. The study sought to find out how often access codes were changed in their commercial banks. The responses were in line with Amaroso (2010)’s assertions and were as follows, 96% of the respondents articulated that their organizations require the employees to change the access codes.

With the given access codes, the study also sought to find out whether there were policies set in place to block out several failed logon attempts. The findings were in line with Amaroso (2010), Ninety Eight percent (98%) of the respondents expressed that they strongly agreed that the systems in their commercial banks lock out users after several failed logon attempts, Amaroso (2010) however is quick to clarify that total compliance cannot be achieved and that the staff in an organization and in this case the staff in commercial banks be educated and made aware of the risks in any actions that they may take that could damage the security in the given environment.

5.3.3 Determining Employee Competence and Awareness in Influencing Cybercrime in Banks

Employees leaving organizations should be removed from the security clearance lists and organizations’ authentication platforms. Employees and former employees may also take part in Net espionage where they may obtain vital data from their own organization and provide it to a competing firm (Panel, 2006). Ninety seventy point four percent (97.4%) of the respondents indicated that exiting employees are removed from the system during the exit process.
Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance, when sending record media to another location, e.g., the off-site backup facility. India (2000) also advises on the use of digital signatures to authenticate electronic documents and the use of private and public keys to authenticate the authorize users to decrypt data. Schulz (2006) adds to the support on encryption of data saying that banks should put in place measures such as data encryption and use of VPN’s and IPSEC protocols. Ninety two percent (92%) of the respondents indicated that in their organizations systems were in place to prevent coping of data by unauthorized personnel.

The study agreed with the assertion that personnel should be well vetted, and their references checked prior to employment. These same measures should be taken when promoting staff because the staff shall have access to more vital and confidential data as they move up the corporate ladder. Rohini’s sentiments are echoed by Kris’s and Belicove (2012) work which state that making a wrong hiring decision can haunt your company, other employees and your client base. Kris in his article ‘Background Checks’, supports the importance of vetting of employees prior to employment. He says that a Society for Human Resource Management survey shows that, overall, employers are moving away from examining an applicant’s actual work history and are turning instead to credit, criminal, and character data checks before hiring. Ninety Six Point Four percent (96.4%) of the respondents indicated that they their organizations vet potential employees prior to employment.

In the Serianu report, Paula, Carol, Kevin, Martin, & Barbara, (2014) go ahead to explain how Social Media can be a threat to organization. They explain that social media is a platform where disgruntled employees can engage in posting of derogatory material, hate speech and cyber bullying. In the research conducted, the results revealed that commercial banks were acting contrary to the recommendations. The respondents indicated that 53.8% of the respondents felt that their organizations handled disgruntled employees well. These findings would further mean that the perpetrators are as defined by Verizon (2012) as the internal agents who perform internal attacks which go unreported because they are not detected.
Verizon (2012) reported that almost one third of cyber-attacks in 2012 involved social engineering. Sixty six point six (66.6%) of the respondents indicated that they agreed that the institutions employees had been educated to recognize social engineering. The numbers in this case are low considering the impact of cybercrime in commercial banks and the advice given by Youga and Singh (2013), that staff require more skill on social engineering to enable them to identify an attempted breach.

Amaroso (2010 utters that it is important to train users who are the key decision makers. Thus, In addition to training the employees, awareness creation should also be taken a step further to include the customers. In the study conducted, it was found out that Ninety three point one percent (93.1%) of the respondents indicated their banks allow mobile banking. This necessitates the training of Customers on how to recognize social engineering. Fifty Six Percent (56%) of the respondents indicated that they agreed that they had educated customers to protect themselves from cyber stalking.

Despite the presumptive legality, the law firm’s stringent network security policy has drawn less than enthusiastic reviews. Critics argue that the law firm’s “draconian” security strategy is ultimately ineffective, and that the real security risk is an untrained network user. These critics remind that malicious emails are often sent to employees’ work email accounts, and any employee who is likely to open a suspicious email or attachment will also do it on his or her work account. In support of this Internet Safety (2015) identifies that emails have become an essential tool for communicating and thus in order for the users to protect themselves, the users must learn to safely manage their emails. The findings were contrary to the recommendations above where only Forty Eight point Six percent (48.6%) of the respondents stated that they disagreed, that their banks allow for access to personal email account on work computers.

ISACA (2010) notes that business units such as research and development, marketing, human Capital, Marketing, and customer service are realizing the potential for utilizing social media tools to motivate revolution, create brand recognition, hire and retain employees, generate revenue, and improve customer satisfaction. Social media use is no longer just an option for enterprises that want to lead in today’s business environment. Sixty six percent (66.6%) of the respondents expressed that they agreed that their
institutions communicated to the public using social media to communicate with their customers thus agreement with ISACA (2010). ISACA (2010) goes ahead to advice that there is need to be aware that malicious outsiders could use the social media pages to promote targeted attacks.

Over time, as computing ease and functionality have grown, users have an ever-expanding desire for more information. Capacity utilization thus improved and cost of services came under some degree of control. So the concept of sharing or abstracting through virtualization beyond just servers grew and produced a bigger picture, known as cloud computing. (Raval, 2010). The study revealed that 82.1% of the respondents indicated that their banks had employed the use of cloud computing. (Cadregari, 2011) challenges this argument, saying that There is need to take cognisance of the potential for harm (such as the organizational data be worth to a cybercriminal and what a hacker do with the information stored on the cloud) from centralizing and sharing resources has grown to a level that can quickly exceed the business case for cloud computing.

The study agreed with notion that an environment of low awareness and transparency for example through lack of information sharing arrangements could exacerbate the impact of cyber-attacks. A lack of awareness may mean that actors are more likely to be ‘blindsided’ by a new attack and find themselves without the appropriate tools and protocols to mitigate damage. Furthermore, where there is a lack of transparency around emerging forms of cyber-crime, there could be a hidden build-up of risk. (Tendulkar, 2013). The above was supported by 85.7% of the respondents indicating that recent past cyber-attacks had been on the increase due to lack of information sharing.

5.4 Conclusions

5.4.1 To Determine the Level of Cyber Security on Commercial Banks in Kenya.

The study revealed that the necessary policies have been formulated and documented and that commercial banks understand what cybercrime is and the effect of the same in the banking industry, and that is paramount that the commercial banks guard themselves against it.
Other conclusions which can be reached are that commercial banks have set up some preventive controls such as having firewalls in place as well as having their computers protected using antivirus. In addition to this, commercial banks use access control mechanisms to authenticate users. The institutions have invested in training their ICT personnel on cyber security. However training of Non ICT staff and customers has not been done in equal measure to that of the ICT staff.

The study revealed that intrusion detection systems and storage of data in encrypted formats have not been fully adopted as ways of protecting of data from unauthorized access.

5.4.2 To Assess the Effectiveness of Existing Regulation on Cybercrimes in Kenya.

The study enumerated that commercial banks have embraced the use of technology to perform its day to day operational activities thus improving efficiency and accuracy and bring closer the services to the people the of thorough enablement of extended working hours, ATM machines and mobile banking. The study further revealed that the commercial banks were aware that there has been an increase in the cases of cybercrime. However the reporting of the same to the authorities was at a minimum. For the cases which were reported, these are subjected to the same process as theft as the Kenyan legislation is yet to establish laws which deal with these cases as they should.

The study revealed that 67% of the staff know about the Kenya Cyber Security Policy 2014. It is necessary for the government to carry out targeted publicity of this National Policy Document. Despite the increase of cybercrime in commercial banks in the international scene, majority of the respondents indicated that they had not reported any cases of cybercrime. This is however questionable as the Kenya Bankers Association in 2015 have put up a spirited campaign to create awareness to the customers on how to protect themselves from these crimes. Recently there also some cases of Kenyans having defrauded some commercial banks some money using technology as was reported in the Business Daily on the 4th June 2015.
The findings further revealed that commercial banks need to stress there is also need stress on policies which enforce the expiry and resetting of access codes after a specified period of time. Care should be taken as well to have in place policies which lock out several failed log on attempts thus reducing the probability of a hacker gaining access to the systems.

5.4.3 Determining Employee Competence and Awareness in Influencing Cybercrime in Banks

The study identified that a significant number of disgruntled employees were not handled well in the organization. The study further revealed that commercial banks vet their employees prior to employing them. The information which is verified includes among other things credit, criminal and Character history. The study goes ahead to disclose that some efforts have been put in place towards educating employees to recognize social engineering. However more efforts need to be geared towards this front

Some commercial banks are yet to fully adapt the use of social media as a communication platform; the study reveals. In using this platform the commercial banks are advised to engage some professionals to undertake media monitoring so as to be able to perform damage control or reverse resultant negative publicity. The study revealed that only a few banks had this service in place.

5.5 Recommendations for Further Study

5.5.1 Recommendation for Improvement

From the results of this study there are several proposed improvements that can be undertaken to boost cyber Security in commercial Banks in Kenya.

5.5.1.1 To Determine the Level of Cyber Security on Commercial Banks in Kenya.

Commercial banks need set up some preventive controls such as having firewalls whose configurations are frequently reviewed and updated. In addition to this, commercial banks use access control mechanisms to authenticate users. These access control mechanisms need to be used in doubles for example password and finger scanner. The basic rules of
setting up this is ‘something you are and something you have’. The institutions need to
invest in training their non ICT personnel and customers on cyber security.

Commercial banks also need to have in place intrusion detection systems and storage of
data in encrypted formats as ways of protecting of data from unauthorized access.

5.5.1.2 To Assess the Effectiveness of Existing Regulation on Cybercrimes in Kenya.

Commercial banks were aware that there has been an increase in the cases of cybercrime
over the last few years. However the reporting of the same to the authorities is at a
minimum. Commercial banks need to come out clean and report cases of cybercrime
which happen within their institutions. This shall assist the country as a whole develop
proper policies and measures to safeguard the National networks. This shall also help the
government to come up with the proper laws which can be used to deal with cases of
cybercrime.

In addition to the above, commercial banks need to stress on policies which enforce the
expiry and resetting of access codes after a specified period of time. Care should be taken
as well to have in place policies which lock out several failed log on attempts thus
reducing the probability of a hacker gaining access to the systems.

5.5.1.3 Determining Employee Competence and Awareness in Influencing
Cybercrime in Banks

Organizations should handle disgruntled employees well. They should establish groups of
employees who other employees can easily approach whenever one feels aggrieved. The
employees to be approached should have been well trained in handling grievances so as
to address the issues as well as escalate the matters for the organization to address. In
addition to this, commercial banks should continue to vet their employees prior to
employing them.

Commercial banks should invest in training all employees and customers to recognize
and protect themselves from social engineering. Commercial banks need to fully adapt
the use of social media as a communication platform as well as engage some
professionals to undertake media monitoring so as to be able to perform damage control or reverse resultant negative publicity.

5.5.2 Recommendations for Further Study

Majority of the organizations have put in place the necessary policies and educated ICT staff on cyber security. However there is need to establish the level of compliance with these documented policies and procedures. Policies and procedures can only be effective if they are practiced on a day to day basis. There is however need to improve on how regularly the patching and firewall updates are done since delay in patching and updates leaves the organizations vulnerable for the duration when the updates are undone.

Business continuity is a major concern for any organization in business. It defines the steps that the organization are to take after an attack Disaster recovery is the section in the business continuity plan that defines the steps towards recovery with a focus of the computer systems, programs and applications. It is necessary to perform a study on the level of preparation of commercial banks to recover from a disaster like cybercrime. The measures that they have established to ensure continuity of operation and service delivery to the customers and the public as a whole.

A study should be conducted to determine what the effect of inculcating cyber awareness to students while they are still in training would be. It would also be worthwhile to suggest ways in which this could be done.
REFERENCES


Belicove, M. E. (2012, 10 26). The 10 Dos and Don'ts of Conducting Employee Background Checks. Retrieved from Forbes:


Internet Safety. (2015, 02 19). Retrieved from GCFlearnfree.org:
http://www.gcflearnfree.org/internetsafety/4/print


Internet Safety. (2015, 02 19). Retrieved from GCFlearnfree.org:
http://www.gcflearnfree.org/internetsafety/4/print


APPENDICES

Appendix A: Introductory Letter

To Whom It May Concern

Dear Sir/Madam,

I am pleased to inform you that I am a graduate student at United States International University pursuing a Masters of Business Administration (IT Management). As partial fulfilment of the Master’s degree, I am conducting a research seeking to investigate the Factors Contributing to Cybercrime in Commercial Banks in Kenya. Please note that any information you give will be treated with confidentiality and at no instance will it be used for any other purpose other than for this project. Your assistance will be highly appreciated.

I look forward to your prompt response.
Yours Faithfully,

Maryanne Mwai
7th January 2015

TO WHOM IT MAY CONCERN

RE: RESEARCH PROJECT BY MARYANNE NYAMBURA MWAI: STUDENT ID 615648

The bearer of this letter is a student at United States International University-Africa pursuing Master’s Degree in Business Administration (MBA).

As part of the program, she is required to undertake a research project on “Factors contributing to occurrence of cybercrime on E-banking in commercial banks in Kenya”; which requires her to collect data and information from various relevant institutions.

Kindly assist by enabling her access data, information and contact to respondents who can complete her questionnaires. I assure you that the information provided will be treated with the utmost confidentiality.

Should you have any enquiries regarding the student research please feel free to contact me.

Yours faithfully

Dr Amos Njuguna
Associate Dean, Chandaria School of Business
Email: amnjuguna@usi.ac.ke
Tel: 020 360 6419
Appendix B: QUESTIONEIRE

PART A: GENERAL INFORMATION

1. Gender: Male [ ] Female [ ]

2. Age: Below 25 [ ] 25 to 35 [ ] 36 to 50 [ ] over 50 years [ ]

3. Status: Married [ ] Divorced [ ] Never Married [ ]

4. Highest Level of Education:
   Professional Certification [ ] 1st Degree [ ] Masters [ ] PHD [ ]

5. Position within the bank:----------------------------------------(State)

6. Average income per month:
   Below 50,000[ ] 50,001-150,000[ ] 150,001-300,000[ ] 300,001 and above [ ]

7. Has your bank computerized its operations: Yes[ ] No[ ]

8. Does your bank have e banking services: Yes [ ] No [ ]

9. How important is cyber security with reference to your e-banking services:
   Very important [ ] Important [ ] uncertain [ ] Not important [ ]

10. How many account holders does your bank have? ------------------------

11. How many account holders have subscribed to the use of E- Banking services?
   0 to 5000[ ] 5001-20,000[ ] 20,001-50,000[ ] above 50,000[ ]
PART B: FACTORS CONTRIBUTING TO THE OCCURRENCE OF CYBERCRIME ON E-BANKING IN COMMERCIAL BANKS IN KENYA

2.2 Determining the Level of Cyber Security

2.2.1 Current Practice in Prevention and Policy of Cyber Security

1. What has been the impact of using technology on customer levels?

(i) Reduced number of customers [ ]

(ii) None [ ]

(iii) Increased number of customers [ ]

In the following questions, tick YES or NO as is applicable to your organization

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Do you know what cybercrime is?</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Do you have a network security policy?</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Do you have a disaster recovery site?</td>
<td></td>
</tr>
</tbody>
</table>

5. How often is the disaster recovery site serviced?

0 Months-6 Months [ ]

12 Months to 24 Months [ ]

More than 24 months [ ]

2.2.2 Constituents of Threat Model and Prevention

6. Does your organization have a firewall?

Yes [ ]

No [ ]

7. How often does your organization review firewall configurations?
8. The ICT staff in my organization have undergone cyber security training

   Strongly Agree [ ]
   Agree [ ]
   Disagree [ ]
   Strongly Disagree [ ]

9. Does the bank employ the use of antivirus?

   Yes [ ]
   No [ ]

10. Which authentication methods does the bank use? (Multiple choices allowed)

    a) Biometric
    b) Passwords
    c) Cards
    d) None

11. Does bank have an intrusion detection system for logical intrusions?

   Strongly agree [ ]
   Agree [ ]
   Disagree [ ]
12. Does the bank store its data in encrypted format?

Yes [ ]
No [ ]

13. How often does the bank update/patch its software?

0 Months - 6 Months [ ]
12 Months to 24 Months [ ]
More than 24 months [ ]

14. Does the bank have employees charged with the responsibility of media monitoring?

Yes [ ]
No [ ]

15. The bank has a risk department which deals with risk associated with technology

Strongly Agree [ ]

Agree [ ]

Disagree [ ]

Strongly Disagree [ ]

2.3 Assessing the Effectiveness of Existing Regulation

2.3.1 Dealing with Cybercrime on The International Scene

16. Has your organization reported any cases of cybercrime?
2.3.2 Insight into Some Existing Cyber Regulation

17. How often does the bank review the firewall policies?

0 Months - 6 Months [ ]

7 Months to 24 Months [ ]

More than 24 months [ ]

18. Does your bank have a cyber-security policy?

Yes [ ]

No [ ] (If yes go to Question 7.)

If no, proceed to Question 8.[ ]

19. Does your Cyber Security policy address on how to get back from an attack?

Strongly agree [ ]

Agree [ ]

Disagree [ ]

Strongly Disagree [ ]

20. Are you aware of the proposed National Cyber Security Policy?

Yes [ ]

No [ ]

21. The cyber security policy in Kenya serves the banking industry adequately
22. The computers in my organization are secure from cyber criminals.

   Strongly agree [ ]
   Agree [ ]
   Disagree [ ]
   Strongly disagree [ ]

2.3.3 Cybercrime in the Existing Industry in Kenya

23. Has your bank employed the use of automated teller machines?

   Yes [ ]
   No [ ]

24. My bank has employed the use of Technology to serve its customers

   Strongly agree [ ]
   Agree [ ]
   Disagree [ ]
   Strongly disagree [ ]

25. Which aspects of the proposed National Cyber Security Policy would you incorporate into your banks cyber security policy? (Multiple choices allowed)

   i. information security
ii. management controls and procedures,

iii. cyber security systems,

iv. identity management systems

v. Access management systems.

26. The bank has educated its customers to protect themselves from cyber stalking

   Strongly Agree [ ]

   Agree [ ]

   Disagree [ ]

   Strongly disagree [ ]

27. Electronic banking Guidelines are sufficient to provide a good banking environment

   Strongly agree [ ]

   Agree [ ]

   Disagree [ ]

   Strongly disagree [ ]

2.4 Determining Employee Competence and Awareness in Influencing Cybercrime in Banks

2.4.1 Effect of Staff on Cybercrime

<table>
<thead>
<tr>
<th>Tick the most applicable to your organization</th>
<th>0-200</th>
<th>201-400</th>
<th>401-600</th>
<th>601-800</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
28. How many non ICT staff do you have in your whole organization

29. How many staff in your organization use the computer as a tool?

30. How many of these Non Ict staff have been trained on cyber security?

| 2.4.2 Effect of Social Engineering on Cybercrime |
|---|---|---|---|---|
| Tick the most applicable to your organization |
| 0-6 Months | 7-24 Months | More than 24 months | Never |

31. How often are employees required to change their access codes?

32. How often does the bank audit logical access logs?

33. Does the bank allow mobile baking for its customers? Yes [ ] No [ ]

| 2.4.3 Mitigation Options Available |
|---|---|---|---|---|
| Tick the most applicable to your organization |
| <10 | 11-20 | 21-30 | 31-40 | >40 |

34. How many ICT staff do you have in your organization
35. How many of your ICT staff have undergone training on cyber security? |   |   |   |

36. The systems in place lock out users after several failed log on attempts | Strongly agree | Agree | disagree | Strongly disagree |

37. Exiting employees are removed from the system during the exit process |   |   |   |

38. The systems in place prevent copying of data by unauthorized personnel |   |   |   |

39. Prior to employment the bank vets potential employees |   |   |   |

40. The bank handles disgruntled employees well |   |   |   |
<table>
<thead>
<tr>
<th></th>
<th>Tick the most applicable to your organization</th>
<th>Strongly agree</th>
<th>Agree</th>
<th>disagree</th>
<th>Strongly disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>41.</td>
<td>The bank employees have been educated to recognize social engineering</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>42.</td>
<td>The bank allows for access to personal emails on work computers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>43.</td>
<td>The bank employed sending of authentication messages to mobile devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>44.</td>
<td>How often does the bank audit logical access logs?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;6 Months[ ]</td>
<td>7-12 Months[ ]</td>
<td>&gt;12 Months[ ]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>45.</td>
<td>The bank communicates to the public using social media</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>46.</td>
<td>The bank has employed the use of cloud computing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the recent past cyber attacks have been on the increase</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>