

**AN EVALUATION OF THE PERCEIVED EFFECTIVENESS OF
PROACTIVE AND REACTIVE STRATEGIES IN MITIGATING
CYBERCRIME AGAINST BANKS IN KENYA**

TOO DENNIS KIPKORIR

**Submitted in partial fulfilment of the requirements for the Degree of Master of
Commerce at Strathmore University.**

School of Management and Commerce

Strathmore University

Nairobi, Kenya.

JUNE, 2016

**This thesis is available for library use on the understanding that it is copyright material and
that no quotation from the thesis may be published without proper acknowledgement.**

DECLARATION

I declare that this thesis has not been previously submitted for approval by this or any other University. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

© No part of this thesis may be reproduced without the permission of the author and Strathmore University

Too Dennis Kipkorir

Signed:

Date:

Approval

The thesis of Too Dennis Kipkorir was reviewed and approved by the following:

Dr. David Wang'ombe (supervisor)

Senior Lecturer, School of Management and Commerce
Strathmore University

Dr. David Wang'ombe

Dean, School of Management and Commerce
Strathmore University

Prof. Ruth Kiraka

Dean, School of Graduate Studies
Strathmore University

Abstract

The increase in reported losses from cybercrime in the banking industry as a result of the shift to e-banking underscores the importance of finding an effective strategy to mitigate cybercrime. This research set out to identify an effective solution to cybercrime in the banking industry by identifying a set of variables that if controlled will provide managers with a means to abate cybercrime. The objective was achieved by establishing the relationship between the frequency of cyber-attacks and the strategies employed by Kenyan banks to mitigate cybercrime. Questionnaires and interviews were administered to the managers of the IT and internal audit departments of the banks operating in Kenya as at December 2014. A Likert scale was used to capture the frequency of cyber-attacks from the managers and the strategies adopted to mitigate cybercrime. Simple and multiple regressions were then applied to the mean responses to establish the relationship between the frequency of cyber-attacks and the strategies employed. Findings indicate that all 14 previously identified cyber-attack methods were present with varying degrees of frequency. The research established that attacks by viruses, spamming, phishing, adware, worms, spyware and Trojans were experienced on a daily basis by some banks. The highest occurrence of ATM card fraud and DOS was weekly while attacks by Vishing, SMSishing, botnets and hacking occurred most frequently on a monthly basis. Key loggers had the least frequency of occurrence with most of the banks not attacked. The study found all the banks in Kenya are at different stages of implementing both proactive and reactive strategies as measures against cybercrime. The responses indicated a partiality towards proactive strategies with less than 4% having not implemented any of the previously identified proactive strategies. Regression analyses established both strategies have a negative relationship with the frequency of cyber-attacks. Further, the paper determined reactive strategies to have a higher negative relationship to frequency of cyber-attacks than proactive strategies. The size of the bank was established to have a positive relationship to frequency of attack. This was achieved despite the effort curtailed by less than 100% response rate. The study provides a basis for future research into cybercrime in the banking industry especially on the effectiveness of strategies employed. Further, the research offers impetus for a study on threats from the insider and a view of cybercrime from the customer's perspective.

Table of Contents

DECLARATION	ii
Abstract	iii
List of Tables.....	viii
List of figures	ix
Abbreviations	x
Acknowledgement.....	xi
Dedication	xii
CHAPTER 1: INTRODUCTION	1
1.0 Background	1
1.1 Problem statement	2
1.2 Research objectives and questions	4
1.3 Significance of the study	5
1.3.1 Banks and other financial institutions.....	5
1.3.2 Customers	5
1.3.3 Regulators	5
1.3.4 Software vendors	6
1.3.5 Government and law makers	6
1.3.6 Researchers	6
1.4 Scope of the study	6
1.5 Chapter summary	6
1.6 Organization of the thesis.....	6
CHAPTER 2: LITERATURE REVIEW	8
2.0 Introduction	8
2.1 Adoption of E-banking.....	8
2.2 Cybercrime in the banking industry	9
2.3 Measuring the cost of cybercrime.	11
2.4 Cyber-attack methods.....	12
2.5 Theoretical framework of understanding the approaches banks employ	16
2.5.1 Legitimacy theory	16
2.5.2 Institutional theory	17
2.6 Strategies employed by banks to mitigate cybercrime	18
2.7 Establishing the relationship between the approach the management of Kenyan banks take against cybercrime and the frequency of cyber-attack.	22

2.8 Control Variable	23
2.8.1 Size of the bank.....	23
2.9 Conceptual framework (dependent variable- frequency of Cyber attack)	24
Figure 2.1 Conceptual framework.....	24
2.10 Chapter summary	24
CHAPTER 3: METHODOLOGY	25
3.0 Introduction	25
3.1 Research design.....	25
3.2 Population and sampling	25
3.3 Data collection methods	26
3.4 Data analysis.....	26
3.4.1 Operationalization of Variables	28
3.4.1.1 Dependent Variable.....	28
3.4.1.2 Independent Variables.....	29
3.4.1.3 Control variables	29
3.4.2 Data presentation	29
3.5 Research quality	29
3.5.1 Objectivity	29
3.5.2 Generalizability.....	30
3.5.3 Validity	30
3.5.4 Reliability.....	30
3.6 Ethical considerations.....	30
3.7 Chapter summary	31
CHAPTER 4: FINDINGS.....	32
4.1 Introduction	32
4.2 Establishing the frequency of cyber-attacks in the banking industry in Kenya.	32
4.2.1 Test for reliability	33
4.2.2 Frequency of occurrence of cyber-attacks.	33
4.2.3 Summary of the findings on the frequency of cyber-attacks against banks in Kenya.....	40
4.3 Strategies employed by banks in Kenya to abate cybercrime	41
4.3.1 Extent of adoption of Proactive strategies by Kenyan banks against cybercrime	41

4.3.3 Perceived effectiveness of proactive strategies adopted by Kenyan banks to mitigate cybercrime	43
4.3.4 Extent of adoption of Reactive strategy by Kenyan banks to mitigate cybercrime	44
4.3.5 Perceived effectiveness of reactive strategy adopted by Kenyan banks to mitigate cybercrime	46
4.3.6 Summary of strategies employed by banks in Kenya to mitigate cybercrime	47
4.4 Regression analysis to determine the relationship between the strategies employed by banks in Kenya to abate cybercrime and frequency of cyber-attack	47
4.4.1 Normalization of the data collected on each variable in the regression model	49
4.4.2 Univariate analysis to establish the relationship between each independent variable and the dependent variable.....	49
4.4.3 Multivariate regression analysis to establish the relationship between the frequency of cyber-attacks against banks in Kenya and the strategies they employed to mitigate cybercrime	50
4.5 Chapter Summary	53
CHAPTER 5: CONCLUSION.....	55
5.1 Introduction	55
5.2 Summary of study objectives and methods	55
5.3 Summary of findings	55
5.3.1 Frequency of cyber-attacks in the banking industry in Kenya	55
5.3.2 Strategies employed by banks to mitigate cybercrime	58
5.3.3 Relationship between the strategies implemented and frequency of cyber-attacks	60
5.4 Research implications and recommendations	61
5.4.1 Banks	61
5.4.2 The government and law makers	63
5.4.3 Regulators	63
5.4.4 Software vendors	64
5.5 Limitations.....	64
5.6 Suggestions for further research.....	64
REFERENCES.....	65
APPENDIX I: Questionnaire	74
APPENDIX II: List of banks	77

APPENDIX III: Definitions of identified types of cyber-attack..... 78

APPENDIX IV: Definitions of identified strategies against cybercrime..... 81

List of Tables

Table 4.1 Cronbach's alpha test for reliability	33
Table 4.2 Summary of the mean occurrence and frequency of cyber-attacks against banks in Kenya.....	34
Table 4.3 Extent of adoption of proactive strategies.....	41
Table 4.4 Perceived effectiveness of proactive strategy	44
Table 4.5 Extent of adoption of Reactive strategy	45
Table 4.6 Perceived effectiveness of the reactive strategies	46
Table 4.7 Test for normality.....	49
Table 4.8 Simple regression analysis output.....	50
Table 4.9 Regression output for the model	50
Table 4.10 Coefficients of the Regression	51
Table 4.11 Comparison between Multivariate and Univariate output	52
Table 12 List of banks and total assets.....	77
Table 13 Definitions of cyber-attacks	78
Table 14 Definitions of identified strategies against cybercrime.....	81

List of figures

Figure 2.1: Conceptual framework.....	24
---------------------------------------	----

Abbreviations

ACH	Automated Clearing House
ATM	Automated Teller machine
CEO	Chief Executive Officer
CF	Credit Card fraud
CNP	card-not-present
DDOS	Distributed Denial of service
DOS	Denial of Service
H	Hacking
ICT	Information and Communications technology
ID	Identity
IFMIS	Integrated Financial Management System
IPRS	Integrated Procurement Management System
KEPSS	Kenya Electronic Payment and Settlement System
K	Key loggers
P	Phishing
PA _{st}	Pro-active strategy
PR _{st}	Pro-active and Reactive strategy
RA _{st}	Reactive strategy
S	Spyware
SQL	Structured query language
T	Trojans
V	Viruses
W	Worms
CNP	Card-Not-Present

Acknowledgement

This research has been accomplished with the encouragement, support and contribution from several people to whom I will forever be indebted.

My utmost gratitude goes to my supervisor Dr.Wang'ombe for the advice, guidance and useful suggestions towards the advancement of this thesis.

I appreciate my family, friends, classmates and lecturers who supported and believed in me to undertake this research and gave me words of encouragement when the task seemed daunting.

Above all, I thank the Almighty God for seeing me through every step of the MCOM program up to its culmination in this research thesis.

Dedication

This thesis is dedicated to my family, thank you for the support.

CHAPTER 1: INTRODUCTION

1.0 Background

The development of Information and Communication Technology infrastructure has led to the proliferation of electronic-based banking products as an alternative channel for steering banking services to customers. Its adoption in Kenya has been supported by the rapid diffusion of the internet in the country due to lowering of bandwidth and connectivity costs (Narteh, 2012; C.A, 2014). The digitization of economic activities with an emphasis on banking has led to cybercrime gaining momentum in developing countries while increasing in sophistication and frequency (Kshetri, 2010; Osborn Quarshie & Martin- Odoom, 2012). This paradigm shift from the traditional brick-and-mortar to an up -grade towards e-banking has given cybercriminals an opportunity to use different means to steal personal and bank information and ultimately money while destroying the bank's reputation (Choo, 2011; R. Yazdanifard Yazdanifard, WanYusoff, & Sade, 2011). Global estimates from digital crime are reported to have cost between US\$ 375B to US\$ 445B in 2014 with 75% of financial sector CEOs saying cyber threats are risks to the growth outlook of their organizations (EY Megatrends, 2014; Mcfee, 2014).

Cybercrime defined as “criminal acts committed using electronic communications networks and information systems or against such networks and systems” (European Commission, 2007) is a social construct defined by the intention of the actors in relation to norms laid down by law with technology being only a means to an end (Lagazio, Sherif, & Cushman, 2014). It is also defined as criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or on-line data, or sabotage of equipment and data (European Commission, 2007; NCSC report, 2013; Saini, Rao, & Panda, 2012). These crimes have been defined using different classification methods by authors depending on the approach with which they view the crime. Using the technological approach the criminals employ, Bamrara, Chouhan, Bhatt, et al, (2012) group the crimes into Buffer overflow, Spoofing, Brute force, remote file inclusion, Cross-site scripting and SQL injection vulnerability groups. Cybercrime has also been identified according to how digital opportunities and technological innovations have transformed traditional crimes into cybercrime (Wall, 2007) as quoted in

Lagazio et al., (2014) . Lagazio et al., (2014) then build on Wall's model to take a broader approach of including all cyber activities that support crime in any aspect while emphasizing how the internet has transformed traditional crimes and projected them to a much larger scale. Using this approach they propose four categories for identifying cybercrime: traditional crimes that are conducted online e.g. fraud; hybrid cybercrimes which are traditional crimes whose effectiveness, nature and modus operandi have significantly changed as a result of opportunities provided by the internet e.g. ID theft; true cybercrime involving opportunities created purely by the internet and only carried out in cyberspace e.g. denial of service and lastly cyber platform crimes e.g. use of botnets to facilitate other crimes rather than being used to carry out the criminal activity itself. Cybercrimes can also be grouped according to the victims (Gaikwad & Jadhav, 2015a) into crimes against individuals, organizations or the society at large.

Researchers agree that levels of cybercrime are increasing (Ponemon Institute, 2013; EY Megatrends, 2015; Pwc Financial focus, 2015) and are viewed as risks to the growth outlook of organizations (PWC report, 2015). Two schools of thought exist that disagree on the appropriate methods of abating cybercrime. Some researchers propose reactive strategies which entail catching and punishing perpetrators through vigorous policing as the most suitable method (Anderson et al., 2013;Guitton, 2012;Cassim, 2011). Contrary, other researchers advocate for deterrence including a robust security system for detection and prevention as the most viable security concept (Van der Putten, Meijnders, & Rood, 2015;Kanyaru & Kyalo, 2015;Fick, 2009). There is need for organizations to rethink cyber security and adopt an Integrated Approach to fighting cybercrime through defining cyber security processes, developing better intelligence and continuously monitoring their networks. There is also need for the private sector and the government to work together to understand emerging threats and develop proactive security solutions to safeguard the Internet and physical infrastructure that relies on it (Kenya cyber security report-Serianu,2014).

1.1 Problem statement

The losses incurred as a result of cybercrime continue to rise with the banking sector in Kenya reported to have lost Ksh 4 billion in 2014 from cybercrime (Serianu,

2015). The high figures place banks as the second high-value target to cybercriminals after the government (Ponemon Institute, 2013; Pwc, 2014; EY Megatrends, 2015; Pwc Financial focus, 2015; Ochieng' 2015; Serianu, 2015). Global estimates of losses from digital crime are reported to have cost between US\$ 375B to US\$ 445B in 2014 (EY Megatrends, 2014; Mcfee, 2014) with Kaspersky lab products detecting 22.9 million attacks utilizing financial malware that targeted 2.7 million users. Studies done in Kenya show 70% of Kenyan businesses are vulnerable to cybercrime with the annual cost being Ksh15 billion (Kibet, 2015).Cybercrime exists both in the public and private sector. The government being the highest value target in Kenya is reported to have lost Ksh 5 billion in 2014 following the adoption of technology and automation processes including IFMIS, E-procurement, ITax and IPRS as seen in the ongoing case of Ksh 791 million lost at the NYS through suspicious online payments (Kenya cyber security report, 2015;Wafula, 2015; Ochieng', 2015).

Research has found that the losses incurred from cybercrime are lower than the expenditure by companies on system's protection (Bernik, 2014). Further, measures taken by companies to mitigate cybercrime are not driven by the number of cybercrime incidents experienced by financial companies which sometimes are fictitious but rather by the way these companies choose to protect their business interests and market positioning in the presence of cybercrime (Lagazio et al., 2014; Bernik, (2014).

Based on differences in research methods, researchers disagree on the best strategy of dealing with cybercrime with conclusions offering different and often conflicting strategies (Lagazio et al., 2014). Suggestions have been made for victims of cybercrime to spend less in defence and anticipation of cybercrime and more on catching and punishing perpetrators (Anderson et al., 2013). This is particularly true for developing countries with inadequate domestic solutions and limited finances to maintain security and preventive measures (Cassim, 2011). Other researchers on the other hand advocate for the relevance of deterrence as a viable security concept especially when tailored to a specific area of threat, group or actors (Van der Putten, Meijnders, & Rood, 2015; Fick, 2009). This resonates with suggestions by Kanyaru & Kyalo, (2015) who in cognisance of the inadequacy of traditional techniques of

authenticating individuals via passwords and usernames conclude that the best practice in Kenya to prevent online transaction fraud includes robust security systems for detection and prevention of fraud related attacks, continuous detection and conventional protection measures. There is need to establish the effectiveness of both proactive and reactive strategies against cybercrime in the banking industry in Kenya and offer suggestions to banks of the most effective strategy to pursue.

The thesis set out to identify the relationship between the frequency of cyber-attacks and the strategies employed to mitigate cybercrime in the banking industry. The objective was achieved by first establishing the frequency of cyber-attacks facing banks in Kenya. The study then identified the approaches the banks have adopted in dealing with cybercrime. Consequently, through analysis of the relationship between the frequency of attacks and strategies adopted, the research sought to identify a suitable method of fighting cybercrime in the banking industry.

1.2 Research objectives and questions

The main objective of this research was to establish an effective solution to cybercrime in the banking industry by identifying a set of variables that if controlled will provide managers with a means of abating cybercrime.

The study specifically set out to:

1. Establish the frequency of identified types of cyber-attacks in the banking industry in Kenya.
2. Identify the strategies managers of Kenyan banks adopt in response to cybercrime.
3. Determine the relationship between the strategies used by the banks and the frequency of cyber-attacks.

The study was guided by the following questions:

1. What is the frequency of cyber-attacks in the Kenyan banking industry?
2. Which strategies do banks in Kenya employ to abate cybercrime?
3. What is the relationship between proactive and reactive strategies and the frequency of cyber-attacks?

1.3 Significance of the study

The principal motivation for this study is the reported increase in levels of cybercrime in the banking industry as a result of the rapid adoption of the internet as a platform for doing business. Unlike in developed countries where the shift occurred much earlier hence the availability of quality research on cybercrime, Kenya as a developing country is new to these developments and the CEOs of banking institutions are playing catch up instead of taking a more aggressive approach to cyber threats. According to cybercrime statistics released by Fred Matiangi, the former Kenyan cabinet secretary for information and communication technology (ICT), the banking industry is the most affected by cybercrime. Kenya lost US\$ 23 million in 2013 through cybercrime with the figures increasing by 108% to reach 5.4 million cyber-attacks in 2014 up from 2.6 million in 2013 (Serianu, 2014). Further, government statistics indicate that on a daily basis, close to 1,000 Kenyans fall victim to Internet fraud. There is an urgent need to study these trends and find solutions to mitigate cybercrime in developing countries. Findings of this research will benefit the following;

1.3.1 Banks and other financial institutions

By establishing suitable methods of dealing with cybercrime, the research will guide managers on the best strategies to adopt. The research achieved this by relating the frequency of cyber-attacks against the strategies the managers employed in the year 2014.

1.3.2 Customers

Through this research, bank account holders and users of online financial transactions will be able to learn of the different cyber-attack methods and take necessary precautions to safe guard vital information and their finances.

1.3.3 Regulators

The research will inform regulators of the banking industry including the Central Bank on the trends regarding the security and integrity of the IT infrastructure supporting banking operations. The knowledge will enable them set minimum standards to be adhered to by all players in the sector.

1.3.4 Software vendors

Software vendors stand to gain from the knowledge on cybercrime in the banking industry which will facilitate customization of their products for the particular needs of this sector.

1.3.5 Government and law makers

With regards to attribution as a strategy, the research illuminates the effectiveness of the existing laws as a deterrent against cybercrime thereby guiding the government and law makers on any existing legislative gaps.

1.3.6 Researchers

The study further contributes to existing literature by providing empirical evidence on the suitability of either proactive or reactionary techniques of dealing with cyber crime. The study provide impetus for further research in tackling cybercrime in the banking industry.

1.4 Scope of the study

The research focused on the 42 commercial banks operating in Kenya as at 31 December 2014 (CBK, 2015) exploring the strategies they employed in mitigating cybercrime in relation to the frequency of cyber-attacks they experienced for the financial year ending 31 December 2014. One year was chosen for this study because of the rapidly evolving nature of cybercrime (Kenya Cyber security report, 2015; Kaspersky, 2015).

1.5 Chapter summary

Chapter 1 gives an introduction to the research through highlighting the background of the adoption of e-banking and the emergence of cybercrime in the banking industry. Further, the chapter has highlighted the disagreement among researchers on the best strategies of dealing with this emerging threat. The chapter offers three objectives that will guide this inquiry into identifying a suitable method of abating cybercrime and the scope of the study.

1.6 Organization of the thesis

The thesis is organised into five chapters, chapter 1 gives a background to the paper, states the research problem and outlines the objectives that will guide the research.

Chapter 2 presents a literature review of the studies carried out on the prevalent cyber-attack methods and the proactive and reactive strategies of dealing with cybercrime. The chapter also presents the theoretical and conceptual framework adopted for this study, the hypotheses to be tested and the control variables.

Chapter 3 presents the research methodology. It identifies both quantitative and qualitative research techniques as the approaches used in this study. The data set, sources and collection methods are highlighted. Regression analysis is chosen as the techniques used to test the hypotheses on the relationship between the strategies Kenyan banks take against cybercrime as the independent variables and its impact on the frequency of identified cyber-attack methods. Size as a control variable identified from the literature review is included as a moderator.

Chapter 4 presents the results and discussions obtained from the research and analysis.

Chapter 5 presents the conclusions, recommendations, limitations of the study and suggests areas for further research.

CHAPTER 2: LITERATURE REVIEW

2.0 Introduction

Chapter 2 presents the theoretical framework for this research. Through analysis of prior studies, the chapter highlights the different methods of cybercrime used to attack banks and the two differing approaches of defence and offence as strategies employed by bank managers to mitigate cyber-attacks. The chapter further defines the hypotheses to be tested.

2.1 Adoption of E-banking

Kenya has experienced a rapid diffusion of the internet attributed to massive investment by mobile operators and internet service providers into base stations and the last mile fibre optic transmission links to support the increasing bandwidth demand in the country (CA, 2014). Coupled with mobile phone penetration standing at 82.6 percent as at December 2014 and data/internet subscription reaching 16.4 million in the same period, the developments have seen most banks shift their products to the e-platform.

Adoption of online transactions by companies transforms the market place by changing the manner of doing business through fostering closer relationships with customers, increased interactivity within the economy and providing a catalytic effect of accelerating changes already taking place. Further, information and communications technology (ICT) positively influences banking operations globally by transforming them from paper based to computer and internet oriented operations (OECD, 2013; Al-Jabri & Sohail, 2012). ICT has been credited for the introduction of many platforms through which transactions can be done with ease allowing 24 hour access to bank accounts through ATMs, online and mobile banking services. The innovations increase bank performance, profitability and returns on asset by making banking transactions easier through bringing services closer to its customers (Vrancianu, Popa, et al., 2010; Aduda & Kingoo, 2012). Since its introduction in mid-2005, the adoption of internet banking has been slow due to impaired or unavailability of infrastructure and lack of supportive legislation for internet banking. Its uptake has accelerated as a result of observed advantages like enhanced performance in the banking industry due to increased efficiency, effectiveness and productivity (Nyangosi & Arora, 2009; Okiro & Ndungu, 2013). The prevalent internet banking services include customers seeking product rate information and the

use of online credit cards (Bamrara, Chouhan, Bhatt, et al., 2012b). Other services offered that improve the banks performance include viewing of account information, downloading and printing bank account statements and proof of payments, funds transfer to different accounts, linking bank accounts, performing foreign exchange transactions, paying utility bills, purchase of air time and mobile money transactions, query foreign exchange and interest rates and email communication with the bank. Competition, minimal bank reserves, operational costs, operational risk, capital requirements, customer base/reach, regulatory requirements, customer relations, profitability and customer trust in internet banking are some of the factors that adversely affect their financial performance (Mutevu, 2015). The Kenyan payment system architecture through innovation has developed into four inclusive areas; Kenya Electronic Payment and Settlement System (KEPSS), Automated Clearing House (ACH), Payment card infrastructure and Mobile payment platform (Nduati et al., CBK paper, 2015).

2.2 Cybercrime in the banking industry

The disruption caused by technology in the banking industry fuelled by the convergence of social, mobile, cloud, big data and growing demand for anytime anywhere access to information provides opportunities for enterprises to take advantage of the “internet of things” to capture vast amounts of information, enter new markets, transform existing products and introduce new products and delivery models. However, this paradigm shift from the traditional brick and mortar to an upgrade towards e-banking has given cybercriminals an opportunity to use different means to steal personal and bank information and ultimately money (Choo, 2011; EY Mega trends, 2015).

This digitization of the world and rising connectivity of people, devices and organizations provides new vulnerabilities for criminals to exploit with 75% of financial sector CEOs saying cyber threats are risks to the growth outlook of their organizations. Global estimates from digital crime are reported to cost between US\$ 375B to US\$ 445B in 2014 (EY Megatrends, 2014; Mcfee, 2014). In 2014, Kaspersky lab products detected 22.9 million attacks utilizing financial malware that targeted 2.7 million users. Of these attacks against banks, 50.51% were targeting 13 of the biggest and most well-known international financial organizations and the

remaining 49.49% were distributed between the more than 1000 banking brands. The banking sector in Kenya is ranked the second high-value target to cybercrime after the government because they have money and due to their increasing reliance on technology and third parties to perform and enhance their management and transfer of money. (Kenya cyber security report, 2015).

There is no universally accepted definition of cybercrime (Kshetri, 2010; Menon & Guan Siew, 2012; Leukfeldt, Veenstra, & Stol, 2013) but it is generally agreed that the definition depends on its final purpose, means and classification (Leukfeldt et al., 2013). This research adopts an encompassing definition as “criminal acts committed using electronic communication networks and information systems or against such networks and systems”. It is criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or on-line data, or sabotage of equipment and data (European commission, 2007; NCSC report, 2013; Saini, Rao, & Panda, 2012). Cybercrime can be distinguished according to; the transformation of traditional crime into cybercrime because they are conducted online through digital opportunities and technological innovations such as tax fraud; transitional crimes whose modus operandi has changed with the shift to online transactions such as credit card fraud; new crimes arising from the existence of the internet; and platform crimes like botnets which facilitate other crimes (Wall, 2007; Anderson et al., 2013) . Similarly Gaikwad & Jadhav, (2015) give cybercrime two definitions: any criminal activity e.g. fraud that uses the computer either as an instrumentality, target or means for perpetrating crimes further or any activity in which computers or networks are a tool, a target or place of criminal activity e.g. phishing.

The study of cybercrime has been characterized by many controversies arising from the complexity of understanding the subject from either an economic perspective or a social perspective. Research done on the subject also provides statistics that is insufficient and fragmented suffering from under- or over-reporting depending on who collected them (Lagazio et al., 2014; Anderson et al., 2013). The reports also contain errors which could be intentional as the case of vendors and security agencies playing up the threats or unintentional due to response effects or sampling bias.

2.3 Measuring the cost of cybercrime.

Different researchers have strived to quantify as accurately as possible the costs incurred as a result of cybercrime in the banking industry. These efforts have been curtailed by the lack of reliable data due to the competitive nature of the industry and under-reporting to protect reputation and market share (Ponemon, 2013;Lagazio et al., 2014).

Studies have been done using field-based research involving interviewing senior-level personnel in an attempt to capture the total cost spent on detection, investigation, incident response, containment, recovery and ex-post response. This method faces challenges on the integrity of confidential responses received from companies due to the respondents not providing truthful responses (Ponemon, 2013; Lagazio et al., 2014). These setbacks can be overcome by using a qualitative approach combining insights from survey followed by in-depth interviews.

A causal model relating different types of cybercrime to their impact on the economy can be used to measure the cost of cybercrime. The method is achieved through decomposing costs into various components by reviewing data drawn from information in the public domain that is not classified or commercially sensitive. The information is supplemented with knowledge from experts in cyber-security, business, law enforcement and economics. Constraints to this model include lack of a reliable database or information that is not up to date and the use of a particular year as a baseline to predict future impact gives a snapshot of the economic situation while the dynamics also matter (Detica, 2011;Anderson et al., 2013).

Exploratory studies into police files and government departments to establish cybercrime costs from investigations, prosecutions and census offer the same challenge of missing valuable information (Leukfeldt et al., 2013; NCSC, 2013). Information from the media cannot also be relied on because they could be blowing cybercrime out of proportion since they “feed” and “feed off” the public’s desire for shocking information by blurring predictions about what could happen with reality. Sensationalism of the media causes a disproportionate impact upon public beliefs and attitudes raising levels of cyber-fear (Wall*, 2008).

A more robust method suggested by researchers is to adopt a qualitative approach through use of a survey to investigate the opinion of the heads of internal audit and

computer departments of banks to establish the perceived security threat from cybercrime. They are asked to indicate the frequency of occurrence of each security threat and the research further uses unstructured interviews to explore the respondents' opinion regarding the type and adequacy of implemented security controls (Abu-Musa, 2006; Lagazio et al., 2014; Bamrara, Singh & Bhat, 2013).

2.4 Cyber-attack methods

Cybercrime can either be perpetrated by individuals or groups (Broadhurst, Grabosky, Alazab, Bouhours, & Chon, 2013). Little empirical evidence exists to ascertain if it is now dominated by groups (Lusthaus, 2013) though Kshetri, (2010) had asserted that most cybercrimes are committed by organized groups. Cybercrime is increasingly being committed using malicious software that is more profit driven, stealthy, targeted and continuously evolving to pose a serious threat to banking customers. This is achieved using the internet as a platform in three basic ways: it can serve as the instrument of the crime; the target of the crime; or it can be used incidentally in furtherance of criminal activity (Broadhurst et al., 2013; Etaher & Weir, 2014). Financial gain through fraud is the main motivation for cyber attacks in the banking sector and usually takes many forms that include:

ATM/credit card fraud: the misuse of a credit card to make purchases without authorization or counterfeiting credit cards or the card details of victims used to purchase goods or services (Detica, 2011). It is a shift of traditional crime to cyberspace where the perpetrators' method of operation changed with the introduction of the internet and IT. Compromised cards and accounts are the most common cybercrime incidents bringing maximum financial losses to companies (Lagazio, et al., 2014; Anderson, et al., 2014). Malicious software could be used to steal bank card data directly from the merchant's point of sale terminal or stealing of on-line banking and credit card information by replacing the authentication fields of mobile banking app stores on the infected device (Kaspersky, 2014). Although less than 10% of credit card transactions occur in the online environment, they account for nearly 70% of fraud associated with credit cards (Schneider, 2011). Card fraud includes Card-not Present (CNP) fraud which involves transactions conducted remotely (i.e. on the internet, by telephone or mail order) where neither the cardholder nor card are present. The Card could have been lost or stolen offline and used fraudulently online as part of CNP (Mcquire & Dowling, 2013).

Phishing/Spear phishing: criminals attempting to fraudulently acquire sensitive information like the user's ID, passwords, contacts and credit card information by masquerading as a trustworthy person or business in an electronic communication (Wale, Jadhav, Kale & Gupta, 2014). The cyber criminals obtain financial or other valuable information by tricking individuals through scams such as purchase frauds and bogus money-transfer requests from foreign countries to many e-mail accounts. Spear phishing is highly personalised bogus e-mail targeted at a single individual. Victims of phishing scams are tricked into revealing passwords, PIN numbers and other sensitive information that the criminals can sell or exploit (Detica, 2011). Reports indicate financial phishing attacks against banks, payment systems and e-shops accounted for 28.73% of all phishing attacks with banking phishing accounting for 16.27% of all the attacks (Kaspersky lab report, 2014).

Denial of service/Distributed denial of service: an attack with the purpose of preventing legitimate users from using a specified network resource. DDos is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems (Chauhan & Prasad, 2015). Criminals could hold a company ransom by flooding the company server with erroneous internet traffic leading to loss of business for companies with a high reliance on the internet (Detica, 2011). It is intended to harm victims by halting the operations of computer systems, specifically online banking servers that provide internet access to bank transactions and data (Singleton, Singleton & Gottlieb, 2006). Distributed denial of service is a modified DoS where multiple attacks are launched simultaneously from various innocent client computers to a single target. Their impact on financial institutions are less devastating than the other forms of attack (Singleton, Singleton & Gottlieb, 2006).

Worms: self-contained computer programs or algorithms which perform destructive actions by invading computers in a network and are self-replicating by executing its own code independent of any other program. They perform the infection and malicious action without human intervention which may include using up the computer's resources and possibly shutting down the system. Worms don't need a host to cause harm and are spread via network connections with the goal of infecting as many computers as possible (Idika & Mathur, 2007; Etaher & Weir, 2014).

Trojans: an apparently harmless computer program that may appear useful and functional but contains harmful components that will insert themselves into a machine and install an illicit or malicious action. They do not self-replicate but are embedded by the designer and have the ability to “sit” on a system and capture keyboard strokes and send them back to the perpetrator. Trojans have the potential ability to steal passwords and Ids especially in online banking (Singleton, Singleton & Gottlieb, 2006; Idika & Mathur, 2007; Etaher & Weir, 2014). Trojan-SMS and Trojan-Banker accounted for 48.15% of attacks on users of Android-based devices that were blocked by Kaspersky in 2014 (Kaspersky Lab report, 2014). The most common banking Trojan is Zeus.

Viruses: self-replicating programs that modify the contents of files by hiding within other inoffensive programs in order to perform malicious acts. They spread through media e.g. USB cables and across networks. It is a code that replicates itself by inserting itself into other programs called hosts (Idika & Mathur, 2007; Etaher & Weir, 2014).

Hacking: unauthorised access made by a person to cracking the system or an attempt to bypass the security mechanism by penetrating the bank sites or customer accounts. If the system is not configured properly or the updated patches are not installed then hackers may crack the system using a security hole (Bamrara, Singh & Bhatt, 2012). Hackers are usually motivated to explore others’ computer system for education, financial gain, out of curiosity or to earn respect from peers (Saini, Rao, & Panda, 2012).

Key loggers: malware whose goal is to secretly collect critical information such as passwords, logins and other credentials manually entered from the client server device and transmit it to the source of the infection (Etaher & Weir, 2014). Its use has decreased because of the falling demand for standalone key logging malware and increased preference for complicated all-in-one malware (e.g. Trojans) which have the ability to log key board strokes (Kaspersky, 2014).

Spyware: entails assault against the integrity of network access mechanisms through installing programs on a computer in order to transmit, track and report information regarding the activities of an internet user. Its evolution from simple cookies to sophisticated user-tracking systems poses a threat through disclosure of business

information and risks privacy, confidentiality, integrity and system availability. They achieve these by tracking e-mail, instant messaging usage and keystrokes in stealth mode. Some could perform screen captures, scan PCs and corrupt data (Wall, 2007; Etaher & weir, 2014; Gordon, 2005).

Adware: software that installs to provide advertisers with information regarding the browsing habits of the users. It monitors web browsing habits or preferences and transmits that information to third parties who use it for target advertising. The most prevalent adware appears as internet pop-up windows or bars that track web browsing habits or preferences (Etaher & Weir, 2014; Gordon, 2005).

Botnet: a network of computers coordinated by a single control mechanism, often programmed to complete a set of repetitive tasks. It signifies a network of zombie (compromised) computers used without the owner's knowledge or permission. Most have centralised command and control architecture though peer-to-peer structured botnets have gradually emerged as the new advanced threat due to the distributive nature of peer-to-peer networks (Lerner, 2014; Wang, Wu, Aslam, & Zou, 2015).

Vishing: a social engineering phishing technique using a phone number owned by the criminals which when dialled, prompts the user to enter the account number and PIN. It uses fake caller ID to give the appearance that the call originates from a trusted organization. Vishing is facilitated by a Voice over Internet Protocol where the user is asked to make a phone call that will trigger a Voice response system that could then ask for confidential information like credit card numbers (Pasricha & Mehrota, 2014; Shah, 2015).

SMSishing: phishing using short messaging service giving the appearance of originating from a trusted organization. The attacker takes advantage of the target's fear of losing or excitement of gain. This technique requires good social engineering skills and after increased awareness, it becomes ineffective (Pasricha & Mehrota, 2014; Shah, 2015).

Spamming: unsolicited bulk e-mail. The recipient has not requested for it and is sent as part of a larger package of messages with substantially the same content (IEEEEC,2015; Kozak Iefremova, & Hartley, 2015). A summary of the definitions of the identified types of cyber-attack is provided in Appendix 3, Table 13.

The literature survey done is global in nature and this research seeks to investigate the Kenyan banking scene in order to build on local cyber intelligence capabilities that will enhance the visibility of threats facing the organizations (Serianu, 2015). This will be achieved by establishing from the managers the cybercrime threat landscape in the Kenyan banking industry by identifying the prevalent modes of cyber-attack and their frequency.

2.5 Theoretical framework of understanding the approaches banks employ

The epistemology (theory of knowledge) of this research is founded on the subjective nature of the approaches banks take to mitigate cybercrime. As a social construct, cybercrime is defined by the intentions of the actors in relation to norms laid down by law with technology being only a means to an end (Lagazio et al., 2014). Studies have found that the strategies employed by managers to counter these cyber-attacks are not driven by levels of cyber-attack but by market positioning in relation to competitors (Lagazio et al., 2014). This approach by managers can be explained using systems oriented theories particularly legitimacy, stakeholder and institutional theories derived from the political economy theory which describes the interaction of actors within a pluralistic society (Williams, 1999). This research is based on the following theories:

2.5.1 Legitimacy theory

Metcalf's law underscores the importance of more people using a typical network, thus making it more valuable (Anderson, 2001). The quest by banks to achieve this by getting more customers to join the e-platform leads to information asymmetry existing on cybercrime with the different actors involved often unable or unwilling to share their knowledge for fear of negative consequences (Lagazio, sherif, & Cushman, 2014). Consumers expect banks, on-line payment systems and on-line stores to protect their computers and mobile devices from financial fraud and any negative information will erode their confidence (Locke, 2014). Other indirect losses to banks include lost trust in online banking, leading to reduced revenue from transaction fees, and higher costs of maintaining branch staff and cheque clearing activities; missed business opportunity for banks to communicate with their customers by e-mail; indirect losses arising from reduced commercial exploitation of IP and opportunity costs through weakened competitiveness. An ICT survey in 2010 by Eurostat found that 14% of UK consumers stated that they refrained from buying

goods or services online because of security concerns (Ponemon, 2012; Anderson et al., 2013).

The under-reporting of cybercrime incidents by managers and overspending on defence measures as a means of protecting business interests and market positioning (Lagazio et al., 2014) is a legitimating process. Anderson et al., (2013) highlights this discrepancy in Costs vs. Losses by mentioning the gains from a third of the botnets attack through spam in 2010 earning the criminals \$2.7 million while worldwide expenditure on spam prevention probably exceeding a billion dollars. Legitimacy theory rests on the idea that a social contract exists between a company and the society in which it operates (O'Donovan, 2002). Attention is focussed on the nexus between the organization and its operating environment and whether the value system of an organization is congruent with the value system of the society and its objectives meet social expectations (Suchman, 1995). The theory is based on the idea that in order to continue operating successfully, corporations must act within the bounds of what society identifies as socially acceptable behaviour (O'Donovan, 2002). Banks need to operate within the bounds of societal expectations since defence measure taken in the fight against cybercrime can be ineffective without the citizens', society's and industry's engagement and may be considered illegitimate through negatively impacting societal utility and hindering fundamental rights (Schneier, 2010; Lagazio et al., 2014).

2.5.2 Institutional theory

The isomorphism within the banking sector on approaches to tackling cybercrime can be coercive as a result of national and international legislation (Cassim, 2011; Menon & Guan Siew, 2012) or mimetic where banks ape each other for competitive advantage and to reduce uncertainty (DiMaggio & Powell, 1983). This falls under Institutional theory which explains why organizations within a particular field tend to take on similar characteristics and form (Scott, 1987). Isomorphism as a dimension of this theory explains the constraining process that forces one unit in a population to resemble other units facing similar environmental conditions (DiMaggio & Powell, 1983).

Banks are expected to operate within defined laws covering cybercrime. In the UK, organisations are accountable to the Information Commissioner's office for data

breaches and can be levied substantial fines when negligent. The UK's data protection act safeguards consumers' data though it does not require organisations to make any formal disclosure in the event of a data breach. In Kenya, The Kenya Information and Communication Act (Part VI A) provides the legal recognition to electronic transactions and sets out specific key areas that need to be adhered to. This includes the need to facilitate electronic transactions by ensuring the use of reliable electronic records, promotion of public confidence in the integrity and reliability of electronic records and transactions and development of a sound framework to minimize the incidence of forged electronic records and fraud in electronic commerce and other electronic transactions. Other bills and regulations covering cybercrime include the Data Protection Bill and the Cybercrime and Computer Related Crimes Bill. The country also recognises certain International standard setting Bodies governing the integrity of electronic transactions. This includes Bank of International settlement-committee on Payments and Settlement Systems, International Organisation of Standards and Financial Action Task force (Nduati, 2015) . These laws and guidelines create a uniformity in the banking sector on ways of maintaining information system's integrity either through coercion or mimicry.

2.6 Strategies employed by banks to mitigate cybercrime

Bank managers can use two approaches to mitigate cybercrime; defence in expectation of attack or spend less in defence and anticipation of cybercrime and more on catching and punishing perpetrators. By highlighting different cost calculation models, Bernik, (2014) finds that most of the huge financial losses from cybercrime reported in different studies are fictitious and that the largest share of costs is generated by investments into protection which however is not always successful. He advocates for increasing awareness among personnel as a much more efficient and inexpensive method for protection against cybercrime. His study reviewed various cost determination models including the cost decomposing model used by Anderson et al., (2013), the causal cost estimation model used by Detica, (2011) and the Ponemon, (2013) cost estimation model based on confidential diagnostic interviews with key respondents within benchmarked organizations. Through decomposing the costs of cybercrime into defence costs, indirect costs and direct losses including criminal revenue, Anderson et al., (2013) and Lagazio et al., (2014) identified shifts in financial companies' strategic priorities, the need to protect

customer trust and loyalty and considerations for market positioning in relation to competitors as the key drivers in determining the cost of cybercrime. This was after analysis of what is known about the actual losses from cybercrime coupled with estimation and concluding that the cost of defence against new cyber-frauds was much higher than the earnings the cyber-criminals made. They advocate for spending less in anticipation of cybercrime but more on catching and punishing perpetrators through vigorous policing.

Contrary to the above studies, other authors advocate for defence as an effective strategy against cybercrime. Focus should be on prevention rather than prosecution of cybercriminals using the Defence in Depth strategy by shifting the paradigm from a reactive to a proactive approach with emphasis on deterrence (Anderson, 2001; Fick, 2009). This poses benefits in terms of saving cost, time, resources and organisational reputation through sharing information on threats and attacks. Robust security systems for detection and prevention of fraud related attacks, continuous detection and conventional protection measures, incident management plans and regular security assessment coupled with consumer education in collaboration with government and private agencies are viewed as the best strategy against cybercrime (Bamrara, Chouhan, Bhatt, et al., 2012c; Kanyaru & Kyalo, 2015).

There exists a difference in research methodology between the authors advocating for offensive measures against cyber criminals and studies that suggest defensive mechanisms which could explain the inconsistency in findings. Proponents of proactive strategy including Fick, (2009); R. Y. Yazdanifard, Yusoff, & Sade, (2011); Kanyaru & Kyalo, (2015) and Van der Putten et al., (2015) did not carry out cost ascertainment comparison between the costs of defence in relation to losses from cybercrime but relied on literature survey. Guitton, (2012); Anderson et al., (2013) and Lagazio et al., (2014) did a quantitative analysis of the costs of cybercrime and advocate for a reactive strategy. Use of a different methodology is bound to give different possibilities of findings and a combination of research methods in the same instance should be used to find whether there is inconsistency in the conclusions.

The prevalent proactive strategies include the following: know your enemy- Banks are accustomed to the threat of fraud and theft from intrusion with threat from the

insider being the hardest to detect. Though rare, this comes from an individual who has access to security and transaction systems. Banks are increasingly implementing behaviour analysis tools to flag anomalies in the network activity of employees and issue alerts in real time coupled with multiple levels of approval for every transaction to reduce the threat from rogue employees. Banks also monitor transactions by creating and analysing full reports on all transactions to spot anomalies and suspicious activity from both the insider and outsider threats (Symantec, 2014;Kaspersky, 2014;Citi, 2014).

Training: banks train customers and employees on the common phishing techniques by raising their awareness against anyone claiming to be from the bank and asking for passwords and private information or accepting email invitations and clicking on shortened URLs. Staff must be trained in such a way that their soft and hard skills are ICT enhanced (Osborn Quarshie& Martin- Odoom, 2012; Machogu & Okiko, 2012); Shah, 2013; Symantec, 2014; Kaspersky, 2014; Citi, 2014).

IT Discipline: discipline and vigilance by IT staff and end-users enhances cyber security. This entails using the latest anti-virus/malware software and regularly updating browsers and operating systems of both the company IT infrastructure and personal devices that can access the company platform especially for employees in companies encouraging BYOD-bring your own device (Shah, 2013;Symantec, 2014; Kaspersky, 2014; Citi, 2014).

Channel protection: this blocks unauthorised access into the platform through strong log-in credentials for authentication using techniques like “challenge” and/or “response” tokens, use of digital certificates and encryption of all data exchanged with clients to enhance data privacy and the use of chip and pin to enhance card security. A near perfect solution to security breaches is the use of biometric technology though it faces social, ethical and managerial challenges due to close association to human, physical and behavioural aspects (Venkatraman & Delpachitra, 2008;Symantec, 2014;Kaspersky, 2014;Citi, 2014).

Defence-in-depth: these are multiple, overlapping and mutually supportive defence systems to back up all other methods. This strategy involves understanding your

organization, define roles and responsibilities, clearly state policies and procedures, regular assessment, research and adopt new developments and involve both public and private partners. (Fick, 2009; Symantec, 2014; Citi, 2014).

Identified reactionary strategies include: use of the cyber-kill-chain methodology which enables the victim to collect and tag information in order to identify an attack at the earliest stages when the attacker is still looking for vulnerabilities and counter it. Malware detection relies on two approaches (Etaher & Weir, 2014) that include signature based techniques which use a series of commands designed for the malware which produces its signature that can be captured by researchers. This method aims to replicate the malicious behaviour and use it in detection. The second is the behaviour based technique which involves analysing the behaviour of recognised malicious software including the basis and addresses of the malware (Mathur et al., 2013; Elhadi et al., 2012; Idika et al., 2007).

Attribution as deterrence against cybercrime: knowledge about attribution plays a significant role in deterrence of certain types of cybercriminals but not all. Challenges to implementing this method arise from the transnational nature of cybercrime which poses significant implications on legislation, investigative and prosecutorial capacity of governments (Guitton's, 2012; Commonwealth Secretariat, 2014) as seen in the arrest of 77 Chinese nationals in Kenya accused of cybercrime (Omuya, 2014). Prosecution may involve multiple offenders, victims and evidence from many countries creating resource and logistical challenges to prosecution. Coupled with differences in legislation, emphasis is on the need for collaboration across jurisdictions to harmonise laws against cybercrime. This identified jurisdictional arbitrage provides opportunities for criminals to take advantage by launching crimes from countries with inadequate cyber laws especially African nations and suggests the need for regional partnerships with full government support (Cassim, 2011; Saini et al., 2012; Kshetri, 2010). Forensic accountants engaged to identify fraudulent digital information and conduct digital investigation to identify the party guilty of a cyber-attack will increase the probability of identifying the attackers and have a deterrent effect (Venuti, 1998 ; van der Putten et al., 2015).

2.7 Establishing the relationship between the approach the management of Kenyan banks take against cybercrime and the frequency of cyber-attack.

Different authors advocate for deterrence as the best strategy against cybercrime with focus on prevention rather than prosecution of cybercriminals. The strategy can be achieved through implementation of a robust security system for detection and prevention, continuous detection and conventional protection measures, incident management plans and regular security assessment (Fick, 2009; Kanyaru & Kyalo, 2015). The research determined the effectiveness of this approach through testing the following hypothesis:

H1₁: A significant negative relationship exists between proactive strategies employed against cybercrime and the frequency of cyber-attacks on Kenyan banks.

However research by Anderson et al., (2013); Bernik, (2014) and Lagazio et al., (2014) find spending less in anticipation of cybercrime but more on catching and punishing perpetrators through vigorous policing as the best strategy against cybercrime. The study determined the effectiveness of the reactive strategy through testing the following hypothesis:

H2₁: A significant negative relationship exists between reactive strategies employed against cybercrime and the frequency of cyber-attacks on Kenyan banks.

A point of note is the strategies are not mutually exclusive. A combination of design and operation principles that include both proactive and reactive strategies can be employed against cybercrime. This is achieved through use of offensive tools together with implementing prevention techniques, tools and policies to enhance cyber-security (Singleton, Singleton & Gottlieb, 2006; Amoroso, 2011).

2.8 Control Variable

2.8.1 Size of the bank

The size of the bank can be described using the following parameters: Assets- high profile banks are targeted by hackers leading to increased levels of cyber-attack highlighting the positive relationship between organizational size and cost of cybercrime (Ponemon, 2012; Raghavan & Parthiban, 2014). Nevertheless these large companies in the financial sector over-spend on security to protect their reputation not necessarily as a result of increased cyber-risk but this ultimately improves the security (Lagazio et al., 2014).

Customers: as an increasing number of customers use the internet, they become subject to increased malware threats (Etaher & Weir, 2014) however Pwc's Current Fraud trends report, (2015) contrasts an observed increase in card transactions between 2008 to 2014 by 51% with total value spent increasing by 33 % yet in the same period overall card fraud losses decreased by 21%.

Products: digitization of banking activities has led to an increase in cybercrime. However this transition to the e-platform increases the productivity gain for the company, boosts revenue and increases profits leading to affordability of high-end security measures and better security infrastructure (Kshetri, 2010;Lagazio et al., 2014).

Employees: financial institutions can suffer security breaches as a result of insider attacks from employees authorised to access the system exploiting vulnerabilities in the e-commerce platform (Detica,2011;Shah, 2013) or criminals stealing access keys from them. Conversely, the employees could also be a critical success factor against cybercrime by training on fraud prevention in e-banking.

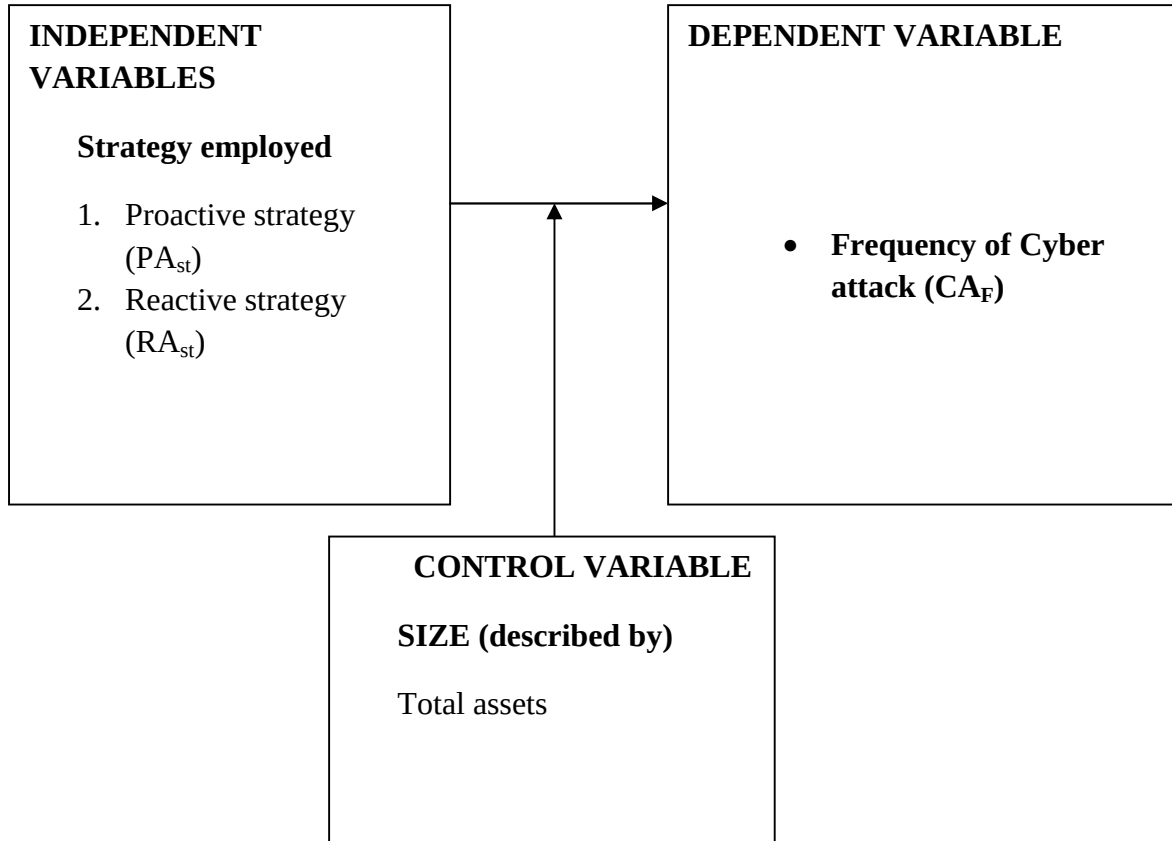
The research adopted total assets of the bank as an indicator of bank size which was used to represent the rest of the indicators of bank size. Its effect on the frequency of cyber-attacks was determined through testing the following hypothesis:

H3₁ : A significant positive relationship exists between the size of the bank and the frequency of cyber-attacks on Kenyan banks.

2.9 Conceptual framework (dependent variable- frequency of Cyber attack)

The conceptual framework for this research is derived from the literature review. The dependent variable is the frequency of cyber-attacks which the model conceptualizes can be explained by the strategy the bank adopts against the threat of cybercrime. The control variable size depicted by total assets is the moderator.

Figure 2.1 Conceptual framework



2.10 Chapter summary

This chapter has presented a literature review of the studies carried out on the prevalent cyber-attack methods, the proactive strategies and the reactive strategies of dealing with cybercrime. The chapter also presents the theoretical and conceptual framework adopted for this study explaining the relationship between the dependent and the independent variables and the control variable. Further, the chapter has introduced the hypotheses to be tested.

CHAPTER 3: METHODOLOGY

3.0 Introduction

Chapter three presents the methodology used by the study to achieve the objectives guiding the research. The study first identifies the frequency of the different types of cyber-attack against banks in Kenya, then investigates the strategies employed by the banks against cybercrime, and finally determines the relationship between the two.

3.1 Research design

The study adopted the sequential procedures of the mixed methods approach to research by expanding the findings of one method with another (Creswell, 2003). The research began by identifying the frequency of cyber-attacks against banks in Kenya in 2014. A qualitative analysis of the strategies banks take to mitigate cybercrime was then done. Through quantitative analysis of the results, the relationship between the strategies and the frequency of cyber-attacks was established.

In seeking to identify an effective method of controlling cybercrime in the banking industry in Kenya, the study assumed a reductionist nature by identifying variables that influence the frequency of cyber-attacks in the banking sector in the country. To achieve this, the research took a postpositive ontological (knowledge) claim reflecting a deterministic philosophy in which causes probably determine effects and outcomes (Creswell, 2003). The quantitative research approach envisaged in this position was employed in determining the relationship between the strategies managers take and the frequency of cyber-attacks through relationship analysis. Postpositivism was identified for this research since the study satisfies the following key assumptions highlighted by Phillips and Burbles, (2000) of this knowledge claim as quoted in (Creswell, 2003): relativism hence the use of hypotheses –leading to a reject or failure to reject and not proving; the research is a process of making claims then refining or abandoning through test of a theory; data, evidence and rational considerations shape knowledge; the research sought to explain the situation of concern and describe causal relationships; the study is objective and examines methods and conclusions for bias.

3.2 Population and sampling

The data used in this study was obtained from the 42 banks operating in Kenya in 2014 (CBK, 2015). One year was chosen for the study because of the rapidly

evolving nature of cybercrime (Kenya Cyber Security report, 2015; Kaspersky, 2015). The population was chosen for the research because of the small number of banks operating in Kenya hence no need for sampling. This enhanced accuracy and generalizability of the results.

3.3 Data collection methods

The research used primary data obtained from the 42 banks operating in Kenya through use of a questionnaire filled by both the bank IT and audit managers and interviews conducted for further clarification. Selecting one industry offered the advantage of the respondents working in similar environments and having similar skills and backgrounds thus promoting homogeneity of the data (Abu-Musa, 2006). The methods were adopted because of the flexibility of interviews and the efficiency of questionnaires (Sekaran & Bougie, 2009). The questionnaire was prepared based on the literature review using the specific variables to be tested as guidelines. It was delivered physically and via e-mail after initial contact through a visit or a phone call to increase the response rate and enable a follow up on the progress. The control variables were obtained from the annual reports for the financial year 2014 sourced from the company website.

3.4 Data analysis

A five point Likert scale was used to capture the strategies banks employ to mitigate cybercrime, the extent of adoption and the perceived effectiveness of these strategies. It was also used to identify the prevalent cyber-attack methods and their frequency. The scale was chosen for its suitability in measuring attitudes and feelings in organizational research (Sekaran & Bougie, 2009). To establish the frequency of cyber-attacks as envisaged in objective 1, the Likert scale in Part II of the questionnaire captured the frequency in a five point scale. Descriptive analysis of the data collected was then done to determine the mean that was used for ranking and the mode to highlight the frequency of occurrence of each cyber-attack method. The mean and the mode are measures of central tendency. Objective 2 was similarly achieved using the Likert scale in Part III, section B and D of the questionnaire which captured from the bank's IT and internal audit managers the extent of adopting the strategies identified in the literature review. The scale was also able to capture the manager's perception of the effectiveness of these strategies in Part III, section C and E of the questionnaire. Descriptive analysis was then done to establish the percentage

of banks that had implemented each strategy to specified levels and the manager's perception of their effectiveness.

To determine the relationship between the frequency of cyber-attacks and the strategies implemented against cybercrime as highlighted in object 3, a simple regression analysis was done. The β coefficients were used to establish the strength and direction of the linear relationship between the frequency of cyber-attacks and each strategy implemented to mitigate cybercrime. Further, a multiple regression analysis was done to determine the effect of each independent variable on the dependent variable in the presence of other independent variables. The R^2 obtained was used to explain the percentage of variance in the dependent variable explained by variation in the independent variables (Hamad, Manan, Shabiralyani & Iqbal, 2015). Multiple Regression was chosen as an effective means of objectively assessing the degree and the character of the relationship between the independent and the dependent variables (Sekaran & Bougie, 2009). Establishing the relationship involved test of significance, p-value determined at 5% level of significance and the R^2 measure considered to test the strength of the model. The β coefficients were used to establish the strength of causality and direction of the relationship between the independent variables and the dependent variable.

Examination of the data for the existence of multicollinearity was performed to check whether two or more predictors in the regression model were moderately or highly correlated (Mansfield & Helms, 1982; Sekaran & Bougie, 2009). The test was achieved by examining the tolerance value and the Variance Inflation Factor (VIF) which quantifies how much the variance of the estimated coefficients are inflated by multicollinearity. A VIF exceeding 10 indicates a high degree of multicollinearity which requires correction.

Based on the conceptual framework, the relationship between the variables can be expressed in the form of a function as follows:

$$CA_F = f(PA_{st}, RA_{st}, CS_z)$$

Where:

CA_F = Frequency of Cyber attacks (measured by the mean of the total number of identified cyber-attack incidences).

PA_{st} = Pro-active strategy (measured by the mean extent of implementing proactive strategies).

RA_{st} = Reactive strategy (measured by the mean extent of implementing reactive strategies).

CS_z : Control representing size of the company. The research will use total assets to depict the size of the bank.

The resultant equation which is a modification of Hamad, et al.'s, (2015) research is as follows:

$$CA_F = \beta_0 + \beta_1 PA_{st} + \beta_2 RA_{st} + \beta_3 CS_z + \epsilon$$

Hamad, et al., (2015) used regression analysis to determine the effect of cyber-attacks on the adoption of e-business by the business community in Southern Punjab. The resultant equation was as follows:

$$Y_i = \beta_0 + \beta_i x_i + \epsilon$$

Where:

Y_i represents the adoption of e-business

X_i represents the frequency of cyber-attacks

3.4.1 Operationalization of Variables

This is the process of defining the variables as measurable factors.

3.4.1.1 Dependent Variable

Cyber criminals could use the internet in three basic ways: it can serve as the instrument of the crime; the target of the crime; or it can be used incidentally in furtherance of criminal activity (Broadhurst et al., 2013). Through literature survey, the present study identified the following cyber-attack methods preferred by criminals: Credit card/ATM fraud (CF); Hacking (H); Trojans (T); DOS Attack (DOS); Phishing/Vishing/SMSishing (P); Key loggers (K); Worms(W); Viruses (V), Spyware (S), Botnets, Adware and Spamming. The research will use the mean occurrence of the identified cyber-attack methods to depict the frequency of cyber-attacks in the Kenyan banking industry.

3.4.1.2 Independent Variables

Proactive strategy: these are defence strategies put in place in anticipation of cybercrime (Fick, 2009). The strategies include; robust security systems for detection and prevention (Kanyaru & Kyalo, 2015); training (Machogu & Okiko, 2012); channel protection through restricted access using strong log-in credentials and biometrics (Venkatraman & Delpachitra, 2008) and IT discipline. The research established the extent of Kenyan banks implementing a particular strategy through use of a Likert scale that allowed the managers to highlight the extent of adoption. The mean of the responses was used to create a super variable.

Reactive strategy: the approach advocates for spending less in anticipation of cybercrime and more on catching and punishing perpetrators through vigorous policing (Anderson et al., 2013). The strategy includes attribution after digital forensic investigation (Venuti, 1998; Guitton, 2012) and cyber-kill chain methodology through signature based and behaviour based techniques of spotting attacks (Etaher & Weir, 2014). The research sought to capture the extent of use of this approach by banks in Kenya and their perceived effectiveness through a Likert scale that allowed the managers to highlight the extent of adoption. The mean of the responses was used to create a super variable.

3.4.1.3 Control variables

High profile banks are targeted more by hackers leading to increased levels of cyber-attacks highlighting the positive relationship between organizational size and cost of cybercrime (Ponemon, 2011; Raghavan & Parthiban, 2014). The size of the bank was described using total assets.

3.4.2 Data presentation

Results from the descriptive analysis of the frequency of cyber-attacks and the extent of implementing the strategies were presented in tabular form. Results from the regression analysis done was presented as generated while presentation of the β coefficients were summarised in tabular form.

3.5 Research quality

3.5.1 Objectivity

Results from the data analysis were based on findings obtained from the actual data and free from the researchers bias in order to achieve a scientific investigation. The

research also strived to be free from any ethical-moral values held by the researcher (Ackoff, 1979).

3.5.2 Generalizability

The research findings will be applicable to financial institutions with an emphasis on the banking industry. To achieve this, the research obtained data from all the banks in Kenya as opposed to sampling and meticulously adhering to the data-collection methods (Sekaran & Bougie, 2009).

3.5.3 Validity

Through survey of literature, the researcher was able to identify the most appropriate instruments and processes used to capture and measure the variables for the study. Further, the research identified appropriate techniques that will give empirical evidence and theoretical rationale supporting the adequacy and appropriateness of inferences based on test scores and other modes of assessment (Messick, 1989 as quoted in Rogelberg, 2002).

3.5.4 Reliability

The research instruments chosen are unbiased with stability and consistency over time. The study if replicated using the same tools and under the same circumstances will yield the same results at a different time (Weiner, 2007). Reliability and consistency was tested using Cronbach's α with internal consistency increasing as the α approached 1.

3.6 Ethical considerations

The research was guided by Strathmore University's code of ethics. Particular attention was paid to the anonymity of the banks and their employees as the main ethical issue under consideration. Participants were informed via a letter of introduction explaining the anonymity of their participation and that the information provided will be kept confidential. In regards to telephone interviews, the conditions as stipulated in the letter of introduction were mentioned in advance and the participant asked for permission to record the interview. To ensure the privacy of participants, their names were replaced with numbers, and contact information maintained privately by the researcher in case further clarification was needed. Protection of financial privacy was maintained by the researcher not seeking financial information unavailable in public records.

3.7 Chapter summary

Chapter 3 presents the research design. It identifies both quantitative and qualitative research techniques as the approaches used in the study. The data set, sources and collection methods are highlighted. Simple and multiple regression analyses are identified as the techniques used to test the hypotheses. Tenets guiding the research quality are outlined and adherence to ethical practice assured.

CHAPTER 4: FINDINGS

4.1 Introduction

Chapter 4 presents an analysis and interpretation of the data collected from the respondents. The Chapter is organised into 4 main sections. Section 4.1 gives an introduction of the main objective of the research and how it was achieved. Section 4.2 summarizes the findings of the inquiry into the prevalent types of cyber-attack against banks in Kenya. Section 4.3 outlines a summary of the strategies employed by Kenyan banks to mitigate cybercrime and their perceived effectiveness. Section 4.4 presents the established relationship between the strategies employed against cybercrime and the frequency of cyber-attacks.

The main objective of the research was to identify an effective solution to cybercrime in the banking industry. The study achieved this objective by identifying a set of variables that if controlled will provide managers with a means to abate cybercrime. Chapter 4 presents results from the research in narrative and tabulated form. First, the study identifies the frequency of the different types of cyber-attack facing banks in Kenya. Second, the research establishes the strategies employed by banks to mitigate cybercrime and their perceived effectiveness. Ultimately through regression analysis, the relationship between the frequency of cyber-attacks and the methods employed to mitigate cybercrime is established. To capture the data, 84 questionnaires were distributed to the 42 banks operating in Kenya as at 31 December 2014. Two questionnaires were given to each bank to be filled by the managers of the internal audit and the IT departments. Fifty four questionnaires were returned, two were discarded because the responses indicated no cyber-attacks occurred in 2014 and fifty two picked for analysis representing 61.9% of the total target population. The research noted that some of the questionnaires given to the audit department had been forwarded to the risk department and the security department. Further research on this topic should perhaps incorporate managers of those departments as target respondents.

4.2 Establishing the frequency of cyber-attacks in the banking industry in Kenya.

Objective one of this study was to establish the frequency of cyber-attacks in the banking industry in Kenya. The study set out to identify the frequency from the

managers of the IT and audit departments of the banks through a questionnaire. The research gave a scale to the respondents in order to capture the frequency of the different types of cyber-attacks on banks as established by the literature review. The filled questionnaires were subjected to a reliability test to determine internal consistency.

4.2.1 Test for reliability

To check for reliability of the scale in capturing the frequency of cyber-attacks and the strategies employed by banks in Kenya to mitigate cybercrime, a Cronbach's alpha analysis was done. The test is used to determine the internal efficiency in the use of different items in a scale (Cortina, 1993).

Table 4.1 Cronbach's alpha test for reliability

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.835	.827	14
.774	.779	5

A Cronbach's alpha of 0.835 for 14 items indicates a high level of internal consistency of the scale in capturing the frequency of cyber-attacks. In capturing the strategies employed, the scale had a Cronbach's alpha of 0.774 indicating a high level of internal consistency (Cortina, 1993).

4.2.2 Frequency of occurrence of cyber-attacks.

To identify the frequency of cyber-attacks, a descriptive analysis of the data collected was done to determine the mean frequency and the mode. The mean occurrence of each type of attack out of the 52 responses was established based on the scale provided to help in ranking. The mode as a measure of central tendency was also determined. Table 4.2 presents a summary of the frequency of occurrence of the cyber-attacks across the banks in the study. The banks are attacked either daily, weekly, monthly, yearly or never. The mean occurrence of each type of attack is also presented in the table.

Table 4.2 Summary of the mean occurrence and frequency of cyber-attacks against banks in Kenya

Cyber-attacks (Ranked from highest to lowest based on mean of occurrence)	Mean	% Frequency of occurrence				
		Never 1	Yearly 2	Monthly 3	Weekly 4	Daily 5
1.Viruses	3.31	7.7	11.5	46.2	11.5	23.1
2.Spamming	2.98	7.7	36.9	26.5	17.3	11.6
3.Phishing	2.94	3.8	42.7	32.3	7.7	13.5
4.Adware	2.92	7.2	58.3	12.9	12.4	9.2
5.ATM fraud	2.88	-	50.7	30.1	19.2	0
6.Worms	2.85	7.7	45.3	23.9	3.8	19.3
7.Spy ware	2.73	11.5	50.8	18.5	11.5	7.7
8.Trojans	2.56	7.7	55.8	21.2	3.8	11.5
9.Vishing	2.35	3.8	57.7	38.5	0	0
10.Denial of service	2.25	21.2	44.2	23.1	11.5	0
11.SMSishing	1.88	50.0	39.8	10.2	0	0
12.Botnet	1.69	50.2	30.8	19.0	0	0
13.Hacking	1.60	52.9	43.2	3.9	0	0
14.Key Loggers	1.52	51.85	48.15	0	0	0

Responses indicating daily, weekly and monthly attacks make up the upper quadrant and were treated as a significant cause for concern. Whereas banks that were never attacked or the attacks occurred on a yearly basis were treated as not significant. The researcher offers caution in the treatment of these classes because of the possibility that the frequency of attack might not reflect the financial losses incurred. Financial loss was beyond the scope of this study with the researcher not privy to this information.

Findings of this survey indicate that viruses are the biggest threat to the banking industry in Kenya. The rank is supported by the tabulated results which shows the highest percentage of responses (80.8%-representing a total of responses indicating attacks that occurred monthly, weekly and daily) are in the upper quadrant reporting attacks ranging from attacks on a daily basis to monthly. Key loggers posed the least threat among the identified cyber-attacks with a majority of the banks (51.85%) never attacked while the rest (48.15%) were attacked on a yearly basis. The questionnaire gave the respondents an opportunity to highlight any other cyber-attack methods but none was indicated. Reluctance to volunteer information might be due to the secretive disposition of financial institutions driven by the competitive nature

of the industry and protection of reputation. Similar studies faced the same challenge. Ponemon's (2013) study in the USA, had a target of 560 companies and received 60 responses while Lagazio et al., (2014) study in the UK got 6 responses out of 59. The higher response rate in this study is attributed to the research avoiding to ask for financial information unlike the previous research. An analysis of each cyber-attack is outlined next;

Viruses are self-replicating programs that modify the contents of files by hiding within other inoffensive programs in order to perform malicious acts. It was expected from prior literature to find high levels of virus attack. The study identified viruses as the biggest threat to the banking industry in Kenya with 80.8% of the responses in the upper quadrant of occurrence more than once a month. Similarly, surveys done by Ponemon institute on benchmarked companies in USA for the years 2012 and 2013 consistently found that all the companies had been attacked every month by viruses. While both studies used primary data from the respondents, the similarity in findings indicates that viruses occur with the same frequency across different geographical regions. Contrary to these findings, Serianu's Kenya cyber security reports of 2014 and 2015 do not mention figures relating to viruses specifically. On inquiry, the researcher was informed that resource constraints curtailed analysis and inclusion of these data in their reports though virus attacks are extensive in the country.

Spamming involves attack by unsolicited bulk e-mail that clogs a company network. Results of this research show that a majority of the attacks were in the upper quadrant with 55.4% of the attacks occurring more than once a month. The results reflect the observations by Trend Micro's (2014) smart protection network that monitors systems worldwide. Trend Micro identified between 4.0 billion to 5.1 billion spam sending IP addresses in the second quarter of 2014 highlighting the gravity of this threat. Overall country statistics from previous research indicates that spamming accounted for 15.83% of all malicious activity and attacks across all sectors in Kenya in 2013 (Serianu, 2014). The high occurrence of spam can be attributed to the fact that spam can be used as a vehicle for spreading other malicious software.

Phishing involves criminals fraudulently acquiring sensitive information including user's ID, passwords, contacts and credit card information by masquerading as a

trustworthy person or business in an electronic communication. The responses indicate a significant number of banks (53.5%) were attacked by phishing more than once a month with 13.5% of these attacked on a daily basis. These results are comparable to findings by Ponemon institute, (2014) in the US on 56 benchmarked companies. They identified an increase in attacks from 38% in the year 2012 to 42% on 60 benchmarked companies in 2013 across a one month period. Contrary, figures from this research which indicate all banks were attacked by phishing are comparably higher than the survey done by Serianu, (2014) who report that only 49% of all firms in Kenya were attacked by phishing in 2014. The findings lead the research to conclude that perhaps the banking sector is targeted more than the other sectors. The phishing attacks involved use of social engineering techniques to fool the users and steal sensitive information and bank account credentials. This is achieved through emails that request victims to click on links which go to websites that replicate a bank's website where they will be requested to submit sensitive information such as passwords, card numbers and account details.

Adware is software that installs on computers without permission and provides advertisers with information regarding the browsing habits of the users. It monitors web browsing habits or preferences and transmits that information to third parties who use it for targeted advertising. The research offered mixed results on the frequency of adware attacks. While it was found that a significant percentage of the banks (58.3%) were attacked by adware once a year, it was also observed that 34% of the banks were attacked more than once a month. Previous studies yielded lower results and found adware coupled with denial of service and spyware were responsible for 23% of all malware attacks in Kenya in 2014 (Serianu, 2014). With the increased adoption of e-commerce in Kenya, unethical enterprises may perhaps use adware to facilitate targeted advertising to the increasing number of card holders (Gordon, 2005; Etaher& Weir, 2014). This might explain the higher frequency of occurrence in the banking sector. The high frequency of adware attacks might also suggest third parties handling customer information could be selling this information to vendors or their sites are compromised.

ATM/Card fraud entails the misuse of a credit card to make purchases without authorization. It also involves counterfeiting credit cards or the card details of victims and make purchases or withdraw money from ATMs. ATM and card fraud is

a major cybercrime in the banking industry (Raghavan & Parthiban, 2014). A significant percentage of the banks in this research (49.3%) experienced card fraud either weekly or on a monthly basis. Similarly, Kaspersky, (2014) notes an increase in attacks on Visa cards from 6.36% in 2013 to 31.02% in 2014 worldwide. Studies done by Serianu, (2014) in Kenya find that card skimming has been on the increase in the country. The increased frequency of card fraud is probably explained by the increased number of cards in circulation. At the beginning of 2014, over 10 million cards were in circulation in Kenya transacting billions every month. A shift to the more secure chip and pin based technology from magnetic strip cards in June 2014 led to a reduction in ATM/Card fraud by the year 2015 (Serianu, 2014; 2015). With the enhanced card security, cybercriminals shifted to card skimming. Companies serving large customers increasingly became targets of malicious software that can steal bank card data directly from merchant Point Of Sale terminals.

Worms are self-replicating computer programs or algorithms that perform malicious action without human intervention. They are spread via network connections and use up computer resources and possibly shut down the system. Previous studies place it at varying threat levels. The current study similarly found varying results across banks in Kenya with some never attacked while others were attacked on a daily basis. Ponemon's survey of 2012 and 2013 found all the companies in the survey had been attacked by worms every month. Contrary to this high figure, The Kenya cyber security report of 2014 by Serianu, (2014) observed worms being responsible for only 0.24% of all the attacks by malicious software in Kenya and the subsequent report of 2015 does not mention worms. The discrepancy in findings on the levels of attack across banks can be attributed to the difference in size of the bank networks. A further explanation could be the varying number of products banks have in the e-platform offering different levels of exposure across banks.

Spyware entails assault against the integrity of network access mechanisms through installing programs on a computer in order to track, transmit and report information regarding the activities of an internet user. Most banks in this research experienced spyware once a year with the overall results spreading from never to attacks on a daily basis. Previous research identified spyware in Kenya and together with denial of service and adware were responsible for 23% of all malware attacks in the country in 2014 (Serianu, 2015). As a means of tracking and transmitting activities of internet

users, the attacks emanate from criminals intent on acquiring financial information about the banks and customers.

Trojans are apparently harmless computer program that may appear useful and functional but have the ability to “sit” on a system and capture keyboard strokes and send them back to the perpetrator. They have the ability to steal passwords and IDs especially in online banking. Results of this research on the banking sector in Kenya found a low occurrence of attack by Trojans with 63.5% of the responses in the lower quadrant. It should be noted though that some banks were attacked on a daily basis. Previous research identifies Trojans occupying the top 10 malware families commonly used in 2014 to attack online banking users. The top malware previously observed in Kenya being the Pushdo Trojan taking 90% of the malware observed followed by the Kelihos Trojan at 8.6% (Serianu, 2014; Kaspersky statistics, 2015). Difference in target population might explain this incongruence in findings. While, Serianu and Kaspersky did a survey on online banking users, this study was on the banks themselves. Further, Kaspersky’s threat report of 2014 notices a decline in Trojan attacks towards the end of the year and attributes it to a US Department of justice crackdown on Zeus-malware responsible for 90% of global banking fraud (Etaher & Weir, 2014).

Vishing is a social engineering phishing technique using a phone number owned by the criminals which when dialled, prompts the user to enter the account number and PIN. Reported cases of voice phishing have been on the increase with criminals using fake caller ID to give the appearance that the call came from a trusted source (Angira, 2014; Pasricha and Mehrotra, 2014). Contrary to expectation of a high occurrence, in the year 2014 most banks in Kenya were attacked by Vishing once a year though a significant number experienced it once a month. Increased media attention on Vishing cases raises customer awareness on social engineering and may perhaps explain the low cases reported.

Denial of service is an attack with the purpose of preventing legitimate users from using a specified network resource. Distributed Denial of service is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems. Denial of

service is not a significant threat to banks in Kenya. A majority of the responses were in the lower quadrant with 44.2% of the attacks occurring yearly while 21.2% reporting the attacks never occurred. These results are comparably much lower than global statistics. Ponemon's study of 2012 found 32% of the 56 benchmarked companies in the USA with a global reach experienced cyber-attacks from denial of service every month. The figure increased to 50% of 60 benchmarked companies in the USA with a global reach in the year 2013 over the same period. The lower figures are perhaps the result of most Kenyan banks not having a global reach thus reduced exposure to cyber criminals. Denial of service usually attacks very high profile servers for ransom or hacktivism.

SMSishing is a phishing technique that uses short messaging services giving the appearance of originating from a trusted organization. The attacker takes advantage of the target's fear of losing or excitement of gain. The research noted a low occurrence of SMSishing with 69.8% of the responses in the lower quadrant. Most banks never experienced SMSishing while 39.8% experienced it yearly. Contrary, media reports indicate phishing using SMS' has been increasing in Kenya across all telecommunication service providers (Angira, 2012). The high cases reported in the media could be because of sensationalism or the low figures found in this research could be because of raised customer awareness from media reports.

Botnets signify a network of zombie computers used without the owner's knowledge or permission. They were found to exist to a low degree in the banking industry in Kenya. In the year 2014, results of this survey indicate attacks were on the lower quadrant with a majority of banks (50.2%) never experiencing botnet attacks. These results are consistent with studies done by Wang, Wu, Aslam, & Zou, (2015) who find that bank networks are not vulnerable to botnets. However, these observations are in contrast with overall country statistics which place botnets as the highest malicious activity at 57.59% of all cyber-attacks in Kenya (Serianu, 2014). The difference in findings between Serianu's (2014) study and this research can be attributed to banks relying on a central server. Serianu's study was on all sectors and included Peer to Peer networks without a central server in their research. Networks without a central coordination by servers or stable hosts are the most vulnerable to botnet attacks.

Hacking entails unauthorised access made by a person to cracking a system or an attempt to bypass the security mechanism by penetrating the bank sites or customer accounts. Hacking is not a major threat to banks in Kenya with 96.1% of the responses in the lower quadrant including 52.9% of the banks not attacked. Contrary, global figures indicate hacking accounted for 34% of data breaches globally in 2014 causing huge financial losses(Symantec, 2014).The low frequency of occurrence in the banking industry can be attributed to hackers shifting from hacking the organization to hacking the person (Serianu, 2015).

Key loggers are malware whose goal is to secretly collect critical information such as passwords, logins and other credentials manually entered from the client server device and transmit it to the source of the infection. Results from this study place key loggers at the lowest threat level. All the respondents indicated occurrence in the lower quadrant with a majority of the banks not attacked. Similar results were noted by Kaspersky, (2014) on financial threats covering 2013 and 2014. Their two year survey found a decrease in key logger attacks from 4.18% in 2013 to 4.01% in 2014.The low threat levels are attributed to a reduced demand for standalone malware with key logging functionality in preference for complicated all-in-one malware like Trojans which includes the capability for key logging.

4.2.3 Summary of the findings on the frequency of cyber-attacks against banks in Kenya

Objective 1 of the research set out to establish the frequency of cyber-attacks in the banking industry in Kenya. Results of the study indicate that all the 14 different types of cyber-attack identified from the literature review exist in the banking industry in Kenya. The findings are contrary to conclusions drawn by Bernik, (2014) and Lagazio et al., (2014) who were of the opinion that the reported losses from cybercrime and the incidences of cyber-attacks are fictitious. The study established that attacks by viruses, spamming, phishing, adware, worms, spyware and Trojans were experienced on a daily basis by some banks. The highest occurrence of ATM card fraud and denial of service was on a weekly basis with the responses showing all the banks experienced ATM card fraud. Attacks by Vishing, SMSishing, botnets and hacking occurred most frequently on a monthly basis. A majority of the banks never experienced hacking, botnets and SMSishing. Key loggers had the least frequency of occurrence with a majority of the banks not experiencing it while the

rest were attacked on a yearly basis. Although the study gave the respondents an opportunity to highlight any other types of cyber-attack, none was indicated.

4.3 Strategies employed by banks in Kenya to abate cybercrime

Objective 2 of this research was to find out the strategies employed by banks in Kenya to mitigate cybercrime. The questionnaire set out to capture this information by giving a scale to the respondents to indicate the extent of adoption of each strategy. The strategies in the scale had been identified from the literature review and while the research gave room for the respondents to indicate any other proactive strategies, none was indicated.

4.3.1 Extent of adoption of Proactive strategies by Kenyan banks against cybercrime

To capture the extent of adopting the proactive strategies identified from the literature review, the research gave a scale to the respondents indicating three distinct levels of implementation. Banks can either have fully implemented the strategy, in the process of implementing the strategy (partial implementation) or have not implemented it completely.

Responses to the questionnaire which set out to capture the extent of adoption of the strategies are summarised in tabular form. The responses are presented as percentages of the number of banks that have adopted each strategy to specified levels.

Table 4.3 Extent of adoption of proactive strategies

Strategy	Extent of Adoption (% of banks)		
	Not implemented 1	Partially implemented 2	Fully implemented 3
Know-your-Enemy	3.8	69.3	26.9
Training	2.5	27.0	70.5
IT discipline	1.7	28.8	69.5
Channel Protection	-	42.3	57.7
Defence-in-depth	3.6	71.2	25.2

Continuous knowledge of evolving trends in cybercrime provides an advantage to managers in developing defence mechanisms. The knowledge is extended through researching on the behaviour of malware to enable its detection (Idika & Mathur, 2007; Citi, 2014; Symantec, 2014). Clearly from the responses it can be seen that managers appreciate this strategy and have implemented it. While 26.9% have fully

adopted the know-your-enemy strategy, a majority of the banks in Kenya (69.3%) are pursuing it while still in the implementation stage. Full implementation is probably curtailed by the fact that this strategy entails a considerable shift from their core banking mandate.

Training aims to increase awareness on cybercrime among key stakeholders, administrators and users who use/maintain and have access to company information. The responses indicate massive adoption of training at 70% within the banking sector in Kenya. A point of concern is the respondents highlighted concentration of training on employees while excluding customers. Previous research by Kaspersky (2014) indicates a fall in the number of banking attacks from 2013 to 2014 due to countermeasures implemented that include educational campaigns among clients. Similar to the results of this research, the KPMG, (2014) crime survey of India among 170 companies with more than 1000 employees found 72% of the respondents pursued awareness training.

General defence mechanisms that form part of IT discipline include use of updated browsers and plugins, Anti-virus software and Sandbox for running un trusted programs (Chang et al., 2012). The study observed most respondents had implemented this strategy with 69.5% having fully implemented it. Likewise, a survey by KPMG, (2014) on 170 participants across all sectors in India found 81% of the respondents believed firewalls protected their organizations, 83% believed in anti-viruses while 69% used anti-spam filters. The high adoption of this strategy can be explained by the fact that most banks have standard operating procedures and User Access Management policies. These documents give guidelines on appropriate measures of enhancing the security of the bank's electronic infrastructure. Further, most software updates automatically once connected to the internet with minimal input from the users. Banks are also connected through a central server with all software updated from a central point.

Channel protection entails protecting the network from unauthorised access. While the Kenyan government has not defined a clear strategy on the protection of critical infrastructure including the telecoms and financial services. Efforts have been made by the Kenya Bankers Association who imposed a mandatory shift to the more secure chip-based technology for credit and debit cards from the magnetic strip cards

(Serianu, 2014). From this survey, all banks in Kenya have either fully implemented channel protection at 57.7% or have implemented it to some degree at 42.3%. Contrary to findings of this survey, Serianu, (2014) found that only 2 banking portals out of a sample of 33 banks in Kenya had adequate online security deployed through encryption. Their observations reflect the lack of appreciation for encryption as a viable form of channel protection or its adoption is limited by resources. Biometrics have also not been implemented by banks in Kenya. Integration of biometrics as a near perfect solution to secure identification and personal verification faces legal, social and ethical challenges associated with privacy. Contrary, the KPMG (2014) crime survey of India found 25% of the respondents had adopted Biometrics, smart cards and tokens as a means of channel protection. They also encrypted their files for further security of electronic communication.

Cybercrime from different types of attack require organizations to have a multi-layered response to counter these threats. The adoption of increased prevention techniques has seen most organizations embracing this multi-pronged approach (Fick, 2009; Citi, 2014). A majority of banks in Kenya pursue this strategy but have not fully implemented it. The observation is congruent with results from adoption of the previous strategies which show that a majority of the banks have adopted all the strategies.

4.3.3 Perceived effectiveness of proactive strategies adopted by Kenyan banks to mitigate cybercrime

The questionnaire set out to establish from the managers their perception of the effectiveness of the proactive strategies adopted. The inquiry was done in order to compare this perception to the level of adoption of each strategy. A scale was given to the respondents indicating 5 levels of effectiveness ranging from not effective to fully effective. The responses are summarised into Table 4.5 which shows the perceived effectiveness of each strategy across the banks in the study.

Table 4.4 Perceived effectiveness of proactive strategy

Strategy	Perceived effectiveness (% of banks)				
	Not effective 1	Partially ineffective 2	Neutral 3	Partially effective 4	Fully Effective 5
Know-your-enemy	3.2	7.7	9.6	51.7	27.8
Training	0	0	0	55.8	44.2
IT discipline	0	0	0	50.0	50.0
Channel Protection	0	0	0	57.7	42.3
Defence-in-depth	0	0	0	80.8	19.2

The adoption of all the above proactive strategies is relatively in tandem with the perception of the managers as to their effectiveness. Other than the Know-your-enemy strategy, the other proactive strategies identified from the literature review including Training, IT discipline, Channel protection and defence-in-depth were found by the managers to be effective. This leads the research to postulate that perhaps choice of adoption of a strategy is biased by the perception of the managers as to their effectiveness subject to resource constraints. Contrary, reliance on these strategies due to reasons beyond their choice including bank policy might positively influence their perception as to their effectiveness.

4.3.4 Extent of adoption of Reactive strategy by Kenyan banks to mitigate cybercrime

To capture the extent of adopting the reactive strategies identified from the literature review, the research gave a scale to the respondents indicating three distinct levels of implementation. Banks can either have fully implemented the strategy, in the process of implementing the strategy (partial implementation) or have not implemented it completely.

The questionnaire set out to capture the extent of adoption of reactive strategies including cyber-kill-chain methods and attribution by providing a scale to the managers to indicate the level of implementation. The responses are presented as percentages of banks that had adopted each strategy to specified levels. The research gave the respondents an opportunity to indicate any other reactive strategies but none was indicated.

Table 4.5 Extent of adoption of Reactive strategy

Strategy	Extent of adoption (% of banks)		
	Not implemented 1	Partially implemented 2	Fully implemented 3
Cyber-kill-chain-method	19.2	71.2	9.6
Attribution	11.5	55.8	32.7

Cyber-kill-chain method entails acting quickly against cybercrime and is essential to reducing losses. The strategy is achieved through tagging information immediately an attack is identified and countering it before it fully develops. Information gathered is then stored and used for spotting future threats (Citi, 2014). The approach detects existing attacks which can then be researched on to discover new exploitation techniques and zero-day vulnerabilities used by attackers. A majority of banks in Kenya are still in the implementation stage of this strategy while 19.2% have not implemented it completely. Similarly, Serianu's survey of 2014 found that 90% of Kenyan organizations have no real-time insight on cyber risks. They lack the ability, budget and skills to combat rising cybercrime with a majority of these organizations unable to detect cyber-attacks using the existing systems and processes. Likewise, the KPMG, (2014) survey of India found only 44% of the respondents had adopted Intrusion Detection systems in their organizations for early detection of cyber threats. The full adoption of this strategy is curtailed by the need to have a dedicated in house team with enough resources for continuous monitoring and tagging of attacks.

Attribution involves conducting a digital investigation, apprehending the cybercriminals and successful prosecution. Experiments done by Guitton, (2012) found mixed results on the effectiveness of attribution as a deterrent against cybercrime based on three types of cybercriminals. Those who know about attribution but still act, those who know about attribution and this knowledge is sufficient to dissuade them from acting and the third group who lack understanding of the technical or legal systems enabling attribution. Guitton's research concludes that enhancing attribution can only work as a deterrent against the first category. While 32.7% of the responses in this study indicate full pursuit of the strategy, a majority partially pursue it while a significant number do not pursue it at all. The reluctance to pursue this strategy might emanate from the high profile nature of cybercrime cases involving banks which might negatively affect reputation and

ultimately profitability. Further, judicial arbitrage due to the universal nature of cybercrime might curtail the pursuit of this strategy.

4.3.5 Perceived effectiveness of reactive strategy adopted by Kenyan banks to mitigate cybercrime

The questionnaire administered sought to capture the perception of the managers as to the effectiveness of the reactive strategies. This was done in order to compare their perception of effectiveness to the level of implementation of the reactive strategy and find any congruence. A scale was given to the respondents indicating 5 levels of effectiveness ranging from not effective to fully effective.

Table 4.6 Perceived effectiveness of the reactive strategies

Strategy	Perceived effectiveness (% of banks)				
	Not effective	Partially ineffective	Neutral	Partially effective	Fully effective
Cyber-kill-chain method	11.5	3.8	0	69.3	15.4
Attribution	11.6	13.4	1.9	48.1	25.0

The responses show the level of adoption of the reactive strategies is synonymous with the perceived effectiveness of these strategies. While a significant percentage of the managers find cyber-kill chain methodology partially effective, some managers find this strategy not effective. The perception can be explained by the fact that it is probably because they do not pursue the strategy in the first place. Further, previous studies done by Bamrara, (2013) gave mixed results on the effectiveness of this strategy. The research found systems monitoring very effective as a strategy against particular types of cyber-attack including malicious software and phishing while it did not have any effect on denial of service attacks and ATM frauds. The inconsistency in effectiveness might also explain the perception of the managers as to the effectiveness of these strategy.

A considerable percentage of the responses also found attribution ineffective against cyber-attacks. The transnational nature of cybercrime and jurisdictional arbitrage poses significant challenges to legislation, investigation and prosecution of cybercrime. The challenges might explain the negative perception of the managers on the effectiveness of this strategy. Further, the negative publicity of such cases might contribute to the perception of the managers about attribution.

4.3.6 Summary of strategies employed by banks in Kenya to mitigate cybercrime

Objective 2 of the study set out to identify the strategies employed by Kenyan banks to mitigate cybercrime. The findings indicate most of the banks in the study have adopted to varying degrees both the proactive and reactive strategies previously identified from the literature review. The responses indicate a partiality towards proactive strategies with less than 4% of the banks having not implemented any of the previously identified proactive strategies. The research noted that 70% of the respondents indicated full implementation of training and IT discipline. This is in contrast to partial implementation by the majority of continuous research on cyber-attacks and defence-in-depth. Responses on the implementation of reactive strategies indicate very few banks had fully adopted these strategies. The research found a majority of the banks partially implemented cyber-kill-chain methods and also found it partially effective with even lower figures fully pursuing attribution as a strategy against cybercrime.

4.4 Regression analysis to determine the relationship between the strategies employed by banks in Kenya to abate cybercrime and frequency of cyber-attack

Objective 3 of the research set out to establish the relationship between the strategies used by the banks to mitigate cybercrime and the frequency of cyber attack. The study was able to achieve this through testing 3 hypotheses. The research sought to identify the individual relationships between the independent variables that include proactive strategy, reactive strategy and total assets and the frequency of cyber-attacks as the dependent variable. The hypotheses were tested using regression analysis which establishes the direction, strength and causality of the independent variables against the dependent variable. The size of the bank depicted using total assets acts as a moderator to the model. The regression equation to be tested is shown next;

$$CA_F = \beta_0 + \beta_1 PA_{st} + \beta_2 RA_{st} + \beta_3 CS_z + \epsilon$$

Where:

CA_F : Frequency of Cyber attack.

PA_{st} : Proactive strategy.

RA_{st} : Reactive strategy.

CS_z : Control representing size of the company.

The variables were measured as explained in Section 3.4.1 (Operationalization of variables).

The hypotheses to be tested are;

H1₁: A significant negative relationship exists between proactive strategies employed against cybercrime and the frequency of cyber-attacks on Kenyan banks.

H2₁: A significant negative relationship exists between reactive strategies employed against cybercrime and the frequency of cyber-attacks on Kenyan banks.

H3₁ : A significant positive relationship exists between the size of the bank and the frequency of cyber-attacks on Kenyan banks.

4.4.1 Normalization of the data collected on each variable in the regression model

Before the regression analysis was done, the data was normalised using the 2-step method and tests of normality yielded the following results;

Table 4.7 Test for normality

	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Cyber-attacks	.086	52	.200*	.985	52	.742
Proactive strategy	.066	52	.200*	.983	52	.682
Reactive strategy	.089	52	.200*	.974	52	.305
Total assets	.048	52	.200*	.988	52	.892

The Kolmogorov-Smirnov significance test for normality indicated the p-values for all the variables were greater than 0.05 proving the distributions were normal (Templeton, 2011; Sekaran & Bougie, 2009).

4.4.2 Univariate analysis to establish the relationship between each independent variable and the dependent variable.

A simple linear regression analysis was done between the frequency of cyber-attacks and each of the independent variables including proactive strategy, reactive strategy and total assets. The regression was done to determine the relationship between each independent variable and the dependent variable. The output is summarised next;

Table 4.8 Simple regression analysis output

Hypothesis	Variable	Regression Coefficients				
		Unstandardized Coefficients		t	Sig.	Test
		β	Std. Error			
H ₁	Proactive	-0.428	0.130	-3.281	0.002	Fail to reject
H ₂	Reactive	-.770	0.094	-8.149	0.000	Fail to reject
H ₃	Size	0.168	0.139	1.209	0.233	Reject

Output from the regression indicates that both proactive and reactive strategies have a negative effect on the frequency of cyber-attacks. Whereas adoption of both strategies reduces the frequency of attacks, reactive strategies have a stronger negative effect. Size with a p-value $0.233 > 0.05$ has been found to have an insignificant relationship with the frequency of cyber-attacks. Further tests using multiple regression were conducted to determine the relationships when all the independent variables were introduced to the model.

4.4.3 Multivariate regression analysis to establish the relationship between the frequency of cyber-attacks against banks in Kenya and the strategies they employed to mitigate cybercrime

The mean frequency of cyber-attacks against the banks was regressed against the extent of adopting each of the strategies with size of the bank depicted by total assets acting as a moderator. The findings are outlined next;

Table 4.9 Regression output for the model

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	F	Sig.
1	.809 ^a	.655	.633	.60158	30.366	.000

Results from the regression show an $F(3,48)=30.366$ and $p=0.000<0.05$ indicating the regression model is a good fit for the data. At 95% confidence, the model is valid and shows a strong relationship between the independent variable and the dependent variables (Williams, 2015). The R-squared of the model is 0.655 interpreted that 65.5% of the variance in cyber-attacks is explained by the linear regression. A significant F change of $0.000<0.05$ indicates variables added to the model improved the prediction.

Table 4.10 Coefficients of the Regression

Hypothesis	Variable	Unstandardized Coefficients		t	Sig.	Collinearity Statistics		Hypothesis test
		β	Std. Error			Tolerance	VIF	
H ₁	Proactive	-0.259	.092	-2.816	.007	.879	1.138	Fail to reject
H ₂	Reactive	-0.691	.091	-7.616	.000	.907	1.103	Fail to reject
H ₃	Assets	0.210	.086	2.444	.018	.965	1.036	Fail to reject

Results from the multiple regression indicate that all the independent variables are important in explaining the dependent variable. The predictors are significant at 95% confidence level and the VIFs which measure the degree of multicollinearity are less than 10 indicating inconsequential multicollinearity (O'brien, 2007).

Reactive strategies with a β coefficient of -0.691, significant at 95% level of confidence with $p=0.000<0.05$ indicates a significant negative relationship exists between adoption of reactive strategies and frequency of cyber-attacks. Adoption of this strategy reduces cybercrime by 69.1% making the greatest contribution to reducing frequency of cybercrime.

The regression results indicate Proactive strategies, significant at 95% level of confidence with $p=0.007<0.05$ also have a significant negative relationship to the frequency of cyber-attacks. The β coefficient of -0.259 indicates a reduction in frequency of cyber-attacks by 25.9% with a unit adoption of this strategy.

Total assets were used to depict the size of the firms and were introduced as a moderator to the regression model. With a β coefficient of 0.210 and $p=0.018<0.05$, it shows there exists a significant positive relationship with frequency of cyber-attacks. Interpreted it means there will be an increase in frequency of cyber-attacks by 21% with a unit increase in assets as identified in the literature review.

These results are synonymous with the findings of Guitton, (2012); Anderson et al., (2013) and Lagazio et al., (2014) who used different research methods from the one used in this study. Using cost decomposition models, Anderson et al., (2013) and Lagazio et al., (2014) advocate for increased reliance on reactive strategies. They find reactive strategies a better method of mitigating cybercrime than continued emphasis on Proactive strategies as suggested by Fick, (2009); Yazdanifard, et al., (2011); Kanyaru&Kyalo, (2015) and Van der Putten et al., (2015). Proponents of proactive strategies as better strategies did not use methods that established the relationship between implemented strategies and frequency of cyber-attacks or losses incurred.

The study further did a comparison of the relationships between the independent variables and the dependent variable both individually and when all were introduced to the model.

Table 4.11 Comparison between Multivariate and Univariate output

Variable	Unstandardized Coefficients		Sig.	Multivariate Hypothesis test	Univariate Hypothesis test		
	β	Std. Error			β	Sig	
Proactive	-0.259	.092	.007	Fail to reject	-0.428	0.002	Fail to reject
Reactive	-0.691	.091	.000	Fail to reject	-0.770	0.000	Fail to reject
Assets	0.210	.086	.018	Fail to reject	0.168	0.233	Reject

A comparison was done between the output of the simple and multiple regression analyses. The regression was done to establish the relationship between the frequency of cyber-attacks against banks in Kenya and the independent variables including the proactive strategy, the reactive strategy and the total assets of the

banks. There is a consistency in the significance and direction of the relationship between the frequency of cyber-attacks and both the proactive and reactive strategies employed to mitigate cybercrime.

An analysis of the effect of total assets on the frequency of cyber-attacks identifies a change in results in the Univariate and multivariate analyses. Total assets develop a significant positive relationship on the frequency of cyber-attacks with the introduction of both proactive and reactive strategies into the model. While the VIFs indicate inconsequential multicollinearity, this change in significance warrants further research.

4.5 Chapter Summary

Chapter 4 presents the findings of the research in narrative and tabulated form. The study set out to capture data for analysis from the IT and Audit managers through use of a questionnaire. Objective 1 sought to identify the frequency of cyber-attacks in the banking industry in Kenya in 2014. From the findings, it is unanimous that the different types of cyber-attack previously identified from the literature review exist in the banking industry in Kenya with varying degrees across banks. Attacks by viruses, spamming, phishing, adware, worms, spyware and Trojans are experienced on a daily basis by some banks. It should be noted that some banks indicated never experiencing these attacks. The highest occurrence of ATM card fraud and denial of service was on a weekly basis with the responses showing all the banks experienced ATM card fraud. While the highest frequency of occurrence of Vishing, SMSishing, botnets and hacking was monthly, a majority of the banks never experienced hacking, botnets and SMSishing. Key loggers had the least frequency of occurrence with a majority of the banks not experiencing it while the rest were attacked on a yearly basis.

Objective 2 of the research set out to identify the strategies the banks implemented to abate cybercrime. From the responses, it was clear that both proactive and reactive strategies have been adopted by the banks to varying degrees. An analysis of the adoption of proactive strategies highlights the fact that less than 4% of the banks have not implemented any of the previously identified proactive strategies. The research noted that 70% of the respondents indicated full implementation of training and IT discipline. This is in contrast to partial adoption by the majority of continuous

research on cyber-attacks and defence-in-depth. An analysis of the managers' perception of the effectiveness of these strategies indicated a general congruence in the perceptions to the levels of implementation. Contrary, training exhibited a divergence. While a majority indicated full implementation, only 44% found it effective. This was attributed to training only offered to employees without enough effort put on training customers. An analysis of the implementation of reactive strategies indicated very few banks had fully adopted these strategies. The research found a majority of the banks partially implemented cyber-kill-chain methods and also found it partially effective with even lower figures fully pursuing attribution as a strategy against cybercrime. Generally, the research noticed a partiality towards proactive strategies as opposed to reactive strategies based on levels of implementation and perceived effectiveness of the strategies.

With a view to identify the most effective solution to cybercrime, objective 3 sought to establish the relationship between the adopted strategies and the frequency of cyber-attacks. Regression analysis was chosen for its suitability in identifying causality, strength and direction of relationships. The β coefficients of the regression outputs from both the Univariate and Multivariate analyses indicated reactive strategies are superior to proactive strategies in mitigating cybercrime. The research was able to show through the regression analysis that reactive strategies have a stronger negative relationship with cyber-attacks than proactive strategies. This is in contrast to the view of the bank managers who are partial to proactive strategies.

CHAPTER 5: CONCLUSION

5.1 Introduction

Chapter 5 presents a summary of the research. First, it highlights the objectives of the study and methods of analysis. Next, the chapter offers discussions on the findings, conclusions drawn and implications of the research. Ultimately, it highlights limitations to the study and offers suggestions for further research.

5.2 Summary of study objectives and methods

The research set out to identify an effective solution to cybercrime in the banking industry by identifying a set of variables that if controlled will provide managers with a means to abate this crime. To achieve this objective, the study first sought through a questionnaire to identify the frequency of cyber-attacks against banks in Kenya from the IT and internal audit managers of the banks. The research then embarked on identifying the strategies the banks employed against cybercrime. Finally, the research identified the relationship between the frequency of cyber-attacks and the strategies employed. Analysis of the strength and direction of the relationships was investigated using regression analysis.

5.3 Summary of findings

5.3.1 Frequency of cyber-attacks in the banking industry in Kenya

Results of this research confirmed the existence to varying degrees of the 14 types of cyber-attack methods identified from the literature review. Attack by viruses ranked the highest while key loggers ranked lowest based on the mean and mode of occurrence of each attack. Further, the research established that viruses, spamming, phishing, adware, worms, spyware and Trojans were the most frequent attacks with some banks attacked on a daily basis. The highest frequency of occurrence of Vishing, SMSishing, botnets and hacking was monthly though of these types, a majority of the banks never experienced hacking, botnets and SMSishing. Key loggers had the least frequency of occurrence with a majority of the banks not experiencing it while the rest were attacked on a yearly basis.

The findings highlight the discrepancy in the frequency of cyber-attacks across banks. Some banks were attacked by specific types of malware on a daily basis while others were never attacked. The inconsistency probably reflects the varying degrees of adoption of the different strategies employed to mitigate cybercrime coupled with

other factors like size which determine the degree of exposure and the financial incentive to the criminals.

The research found that all the banks view ATM/card fraud as a threat. While no bank was attacked on a daily basis, it is important to note that all the banks were attacked with a majority of attacks occurring on a yearly basis. The findings contradict Serianu's (2014; 2015) observations that enhanced card security with the shift to chip and pin technology reduced ATM/card fraud. The existence of this threat can be attributed to criminals shifting to card skimming at merchant point of sale terminals.

Denial of service was identified as a threat to the banking industry in Kenya though on a much lower scale than the findings of Ponemon, (2014) in the USA. While the highest frequency was weekly attacks, a majority of the banks were attacked on a yearly basis with 21% not attacked. The low frequency of occurrence can be attributed to Kenyan banks not having a global reach.

Botnets were observed not to pose a serious threat to banks in Kenya. Half the banks were not attacked with the highest frequency observed being monthly against 19% of the banks. The research attributes this to reliance on a central server which offers protection to the banks. The findings are in conflict with studies done by Serianu, (2014; 2015) who using sensors deployed in Kenya, surveys and interviews found that botnets are the highest malicious activity in the country. The difference can be attributed to Serianu's (2014) study being all encompassing and included peer-to-peer networks without a central server which are more vulnerable to botnet attacks (Wang, Wu, Aslam, & Zou, 2015). This study offers a more reliable analysis of the banking industry which relies on a central server.

Spamming is a major threat to banks in Kenya. Though 7.7% were not attacked, 11.6% were attacked on a daily basis. Overall results indicate 55.4% of the attacks occurred more than once a month. These findings are synonymous with country statistics from previous research which indicates that spamming accounted for 15.83% of all malicious activity and attacks across all sectors in Kenya in 2013 (Serianu, 2014). These unsolicited email usually contains malware that is activated once downloaded and opened. The high occurrence of spam can be attributed to the fact that spam can be used as a vehicle for spreading other malicious software.

A significant number of banks (53.5%) were attacked by phishing more than once a month with 13.5% of these attacked on a daily basis. The observations echo worldwide trends reported by Ponemon, (2013); Detica, (2011) and Kaspersky, (2014) who indicate that financial phishing attacks against banks, payment systems and e-shops account for a great percentage of all phishing attacks. The research contradicts media reports which claim that variants of phishing that include voice phishing and SMS phishing are increasing in Kenya (Angira, 2014). Findings indicate most banks were attacked once during the year. The inconsistency could be attributed to the tendency of the media to sensationalise issues as observed by wall, (2008). Contrary, the media can be given credit for increasing awareness thus reducing this type of cyber-attack.

The study established that banks suffered from attacks by Trojans with frequency ranging from some experiencing it on a daily basis while most of the respondents indicated attacks on a yearly basis. Overall findings indicate 63.5% of the responses were in the lower quadrant with 7.7% not attacked. As established by findings of Serianu, (2014) and Kaspersky, (2015), preference for Trojans will increase because of their key logging capability leading to a decrease in standalone key loggers.

Instances of attacks from adware were also observed. Results of this research found a significant percentage of the banks (58.3%) were attacked by adware once a year though 34% of the attacks were in the upper quadrant of more than once a month. Adware monitors the browsing habits and preferences of users and transmits this information to third parties. The results reflect a need for targeted advertising on card holders with the increased adoption of e-commerce and the use of cards for purchases (Gordon, 2005; Etaher& Weir, 2014).

Hacking is not a major threat to banks in Kenya. 96.1% of the responses were in the lower quadrant with 52.9% of the banks not attacked. Contrary, Serianu's reports of 2014 and 2015 do not give figures for virus attacks. A call to inquire indicated a lack of enough resources to analyse the huge amounts of data available on virus attacks. The research attributed the low frequency of hacking attacks on banks to criminals shifting from hacking the organization to hacking the person.

5.3.2 Strategies employed by banks to mitigate cybercrime

Objective 2 of the research was to establish the strategies employed by banks to mitigate cybercrime. An analysis of the responses indicate all banks had adopted both proactive and reactive strategies to varying degrees.

The proactive strategies implemented include training. The study established that a majority of the banks in Kenya (70%) were found to have fully adopted training as a defence against cybercrime. An inconsistency was noticed between the level of adoption of this strategy and its perceived effectiveness. Only 44% found it fully effective. On further inquiry, it was discovered that banks offer training to employees with little attention to customers. The oversight might explain the low perception managers have of the effectiveness of this strategy. Quarshie & Odoom, (2012), Machogu & Okiko, (2012), Shah, (2013), Symantec, (2014), Kaspersky, (2014) and Citi, (2014) advocate for training of both customers and employees. The training aims at raising awareness on common methods of cyber-attack as an effective means of controlling cybercrime. It is imperative that the training manuals should be up to date with emerging threats and the banks should provide annual refresher courses.

Managers need to stay up to date on emerging trends in cybercrime in order to develop effective defence mechanisms. A majority of the banks in Kenya at 96% have adopted the strategy of knowing-your-enemy to varying degrees. The study noted that only 26.9% had fully implemented this strategy while 3.8% had not implemented it at all. A survey into the managers' perception of the effectiveness of this strategy established a majority of them found it partially effective. Contrary, conclusions from observations by Citi, (2014) and Symantec, (2014) find it fully effective. Full implementation is probably curtailed by the fact that this strategy involves a considerable shift from their core banking mandate.

IT discipline involves vigilance by IT staff and end users. The strategy entails updating browsers and the operating systems and the use of anti-viruses in both the company network and private devices. The research identified that a majority of banks at 69.5% have fully implemented this measure though only half of them find it fully effective. The results contrast the findings by Citi, (2014); Serianu, (2014); KPMG, (2014) and Chang, (2013) who deem the strategy an effective and simple preventive measure. The incongruence in the level of implementation and perception

of effectiveness reflects the fact that though banks have full control of their networks, they cannot control the private devices of their employees or customers.

Contradictions were noted between findings of this study and the observations of Serianu, (2014) in regards to channel protection as a defence strategy. Results from the survey of this study indicate that all banks in Kenya have implemented this strategy to some degree with 57.7% having fully implemented it. Serianu identified only 2 banks out of 33 had secured their networks through encryption. Difference in research methods was noted with Serianu reviewing the online banking sites while this study relied on survey through a questionnaire. Discrepancy in the findings can also be explained by the fact that while this study sought to investigate all forms of channel protection under one umbrella, Serianu picked a facet of channel protection.

The diverse nature of cyber-attacks require organizations to simultaneously implement a wide array of mechanisms to effectively deal with different forms of cybercrime. Most banks representing 71.2% partially pursue this defence-in-depth strategy while few have fully implemented it. All the respondents find it effective though only 19.2% find it fully effective. The success of this strategy depends on continuously sharing information across banks to identify new threats and effective solutions. Information sharing creates a challenge due to the secretive nature of the banking industry (Ponemon, 2013; Lagazio et al., 2014).

The study of banks in Kenya identified the implementation to varying degrees of the two reactive strategies identified in the literature review. The observations echo the conclusions by Detica, (2011); Anderson et al., (2013); Ponemon, (2013) and Bernik, (2014) who using different cost determination models laid emphasis on the adoption of reactive strategies as opposed to continued spending on proactive strategies.

A Majority of banks have partially implemented measures for early malware detection and countering through cyber-kill-chain methods. While only 9.6% have fully implemented this strategy, 19.2% do not pursue it completely. The method relies on early malware detection through use of signature based and behaviour based techniques. Of note is that this degree of adoption is a general trend across all sectors. Serianu's (2014) survey of all sectors found that 90% of Kenyan organizations had no real-time insight into cyber-risks. The low implementation

levels probably reflect a lack of the necessary skills and enough resources to keep track of the continuously evolving cyber-threats.

Most banks in Kenya partially pursue attribution as a strategy against cybercrime. Despite analysis by the office of the director of public prosecutions observing that the procedural safeguards to investigate and prosecute cybercrime in the country are adequate (Article 19, 2014). The research found only 32% fully pursue it while 11.5% do not pursue it completely. Lack of enthusiasm for prosecution stems from the high profile nature of the cases involving cybercrime in the banking industry which impacts negatively on reputation and ultimately financial performance. The transnational nature of cybercrime and jurisdictional arbitrage further pose significant challenges to legislation, investigation and prosecution of cybercrime. Studies by Kshetri, (2010); Cassim, (2011); Saini et al., (2012); Guitton, (2012) and the Commonwealth Secretariat, (2014) advocate for attribution as an effective strategy against cybercrime and whose success depends on regional partnerships with full government support. Its success entails engaging forensic experts to investigate and identify fraudulent digital information and prosecute. The low level of adoption and implementation of this strategy could also be because of the inadequacy of the existing laws on cybercrime.

5.3.3 Relationship between the strategies implemented and frequency of cyber-attacks

An analysis of the effects of proactive and reactive strategies on the frequency of cyber-attacks against banks in Kenya identified the adoption of both proactive and reactive strategies negatively influenced the frequency of cyber-attacks. Conclusions of the research refute the findings by Anderson et al., (2013), Bernik, (2014) and Lagazio et al., (2014). They were of the different opinion that legitimating processes are the key drivers of adoption of strategies against cybercrime. Further, the research has identified reactive strategies which include early detection and countering of attacks coupled with investigation and prosecution have a higher negative effect on the frequency of cyber-attacks than proactive strategies which emphasise prevention and defence techniques. These findings echo the conclusions of Detica, (2011); Anderson et al., (2013) and Ponemon, (2013) who used a different research method which entailed comparison of the costs of implementing the strategies against cybercrime and the losses incurred from cybercrime.

Conclusions from the regression analysis in this research do not reflect the prevailing practise in the banking industry. An analysis of the extent of adoption of the strategies shows that proactive strategies have been implemented to a greater extent than reactive strategies. Training, IT discipline and channel protection have been fully implemented by a majority of the banks. Contrary, results indicate reactive strategies have been fully implemented by fewer banks. Similar to suggestions by Fick, (2009); Yazdanifard, Yusoff & Sade, (2011); Kanyaru & Kyalo, (2015) and Van der Putten et al., (2015) banks in Kenya lay more emphasis on proactive strategies with the managers having a higher perception of their effectiveness than reactive strategies.

Results of this study through analysis of the effect of total assets as a representation of size identify that the bigger the bank, the higher the frequency of cyber-attacks. Big banks have increased exposure and offer higher financial incentives to the criminals. Similar to this observation, Lagazio, (2014) and Shah, (2013) conclude that high profile banks in terms of more assets, more customers, higher number of products in the e-platform and having the most employees are more exposed to cyber-attacks than smaller banks.

5.4 Research implications and recommendations

The research has established the existence of cybercrime in the banking industry from a variety of cyber-attack methods. The findings contradict the view of Bernik, (2014) and Lagazio, et al., (2014) who were of the opinion that most reported losses from cybercrime are fictitious. The frequency of these cyber-attacks is bound to increase as more customers embrace e-banking, more products are introduced into the e-platform and banks expand into other regions. It is imperative that all stakeholders take necessary precautions to safeguard information and monetary assets of both the customers and the banks.

5.4.1 Banks

Through analysis of the relationship between both proactive and reactive strategies and the frequency of cyber-attacks, the research has established the superiority of reactive techniques in the fight against cybercrime. The study has shown the reactive strategies have a higher negative effect on the frequency of cyber-attacks than proactive strategies. Contrary, the prevailing practise in the banking industry as seen

from the literature review and supported by findings of this research is the reliance by banks on proactive strategies implemented to stop cyber-attacks. The thesis has determined Cyber-kill-chain methods which entail systems monitoring to identify and stop cyber-attacks at the earliest possible moment coupled with investigation, collecting evidence and successfully prosecuting cyber-criminals have a higher effect of reducing cyber-attacks. Banks need to shift their continued focus on proactive strategies and pursue reactive strategies more. Specialised units should be created that in conjunction with law enforcement will investigate, gather evidence and prosecute cybercriminals. Attribution and prosecution can only be achieved through cross border judicial cooperation using a common platform with coordinated efforts involving governments, the banking industry and security agencies.

It is important that banks should implement real time systems monitoring to identify cyber-attacks at the earliest stage. Systems monitoring enables the bank to collect and tag information in order to identify an attack at the earliest stages when the attacker is still looking for vulnerabilities and counter it.

Banks need to further implement the know your enemy strategy by staying up to date on emerging trends in cybercrime in order to develop effective defence mechanisms. The strategy entails continued research on the behaviour of malware to enable early detection and stopping of attacks. To achieve this, banks need to institute a dedicated in-house research team to avoid relying on software vendors interested in sales and consultants eager to stay relevant.

It is imperative that banks enhance channel protection through adoption of stronger online security measures. The banks electronic networks need enhanced information assurance that ensures confidentiality, integrity, authentication and availability of information in storage, processing or in transit. An effective means of achieving this is through integrating biometrics as a near perfect solution to secure identification and personal verification. Facial recognition, fingerprint, iris and palm biometrics should be introduced at ATMs and other identification points. The legal, social and ethical challenges associated with privacy and the feared effects of infrared light on health will have to be addressed. Banks should also consider encryption enabled terminals and encryption of connections between data centres for enhanced information security.

Banks and their partners including Telcos need to undertake a security skills gap assessment among customers and develop a training program to sensitize customers on emerging cyber-threats. The awareness training should not be limited to employees but in coordination with a relevant body like the Kenya Bankers Association, the banks should pull resources and provide training programs through the mainstream media and the social media.

5.4.2 The government and law makers

The government and law makers should enact laws to hold banks accountable for breach of system security where customers are found not negligent. The prospect of prosecution will give banks the impetus to increase security of their electronic infrastructure.

Adequate legislation covering cybercrime also needs to be enacted. The laws should harmonize the legal framework concerning cybercrime across regions and jurisdictions to facilitate investigation and prosecution of criminals to avoid the need for extradition of foreign cybercriminals.

The legislature should continue refining the laws governing cybercrime building on the initiative of the office of the director of public prosecution which seeks to equip law enforcement agencies with the necessary legal and forensic tools to tackle cybercrime. The various stakeholders: law enforcement, legislators, anticrime commissions and researchers should come together and share common knowledge to enact laws and policies compatible with international and comparative standards to provide a sufficient and effective legal framework against cybercrime. Effective laws will improve the effectiveness of attribution and prosecution as a strategy against cybercrime.

5.4.3 Regulators

The Central Bank of Kenya in agreement with The Kenya Bankers Association and the banks need to set minimum thresholds that enhance infrastructure security like it did with the shift to chip and PIN. They should enforce encryption of all data transmission and data in storage as standard practice. Biometrics should also be introduced at all identification points including ATMs. Enhanced security will encourage more customers to join the electronic banking network making it more valuable as envisaged in Metcalfe's law.

5.4.4 Software vendors

It is imperative that software developers customize their solutions to cybercrime with the needs of the banking industry in Kenya. Weaknesses that can be exploited by the identified cyber-attacks should be patched and bespoke security solutions offered to the banking industry.

5.5 Limitations

The sensitive nature of information regarding cybercrime in the banking industry curtailed 100% response rate which goes against the overall view that the fight against cybercrime is a collective effort whose success depends on sharing information.

The research focussed on threats from the outsider without considering threats from the insider. These might not paint the full picture of the gravity of cybercrime in the banking industry.

The research considered attacks over a one year period which might not reflect the rapidly evolving nature of cybercrime.

5.6 Suggestions for further research

Further research should be done from the customers' side to identify the frequency of cyber-attacks in the course of conducting e-banking.

Research also needs to be done on the cyber-threat from the insiders who are privy to the defences and the weaknesses of the banks.

Research should be done over shorter time periods e.g. weekly or monthly to capture the rapidly changing nature of cybercrime.

REFERENCES

- Abu-Musa, A. A. (2006). Perceived security threats of computerized accounting information systems in the Egyptian banking industry. *Journal of Information systems*, 20(1), 187–203.
- Ackoff, R.L. (1979). The Future of Operational Research is Past. *The Journal of the Operational Research Society*, 30(2), 93-104.
- Aduda, J., & Kingoo, N. (2012). The relationship between electronic banking and financial performance among commercial banks in Kenya. *Journal of Finance and Investment Analysis*, 1(3), 99–118.
- Al-Jabri, I. M., & Sohail, M. S. (2012). Mobile banking adoption: Application of diffusion of innovation theory. *Journal of Electronic Commerce Research*, 13(4), 379–391.
- Amoroso, E. G. (2011). *Cyber attacks: protecting national infrastructure*. Burlington, MA: Butterworth-Heinemann.
- Anderson, R. (2001). *Security engineering: a guide to building dependable distributed systems*. New York: Wiley.
- Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265–300). Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-39498-0_12
- Angira, Z. (2012, Jan 18). How crooks lure mobile phone users through fake calls and text messages. *Daily Nation*. Accessed from www.nation.co.ke
- Aransiola, J. O., & Asindemade, S. O. (2011). Understanding Cybercrime Perpetrators and the Strategies They Employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, 14(12), 759–763. <http://doi.org/10.1089/cyber.2010.0307>
- Article 19. (2014). Kenya: cybercrime and Computer related crimes bill. Legal Analysis. retrieved from www.article19.org
- Balan, L., & Popescu, M. (2011). Credit card fraud. *The USV Annals of Economics and Public Administration*, 11(1), 81–85.
- Bamrara, D., Chouhan, G. S., Bhatt, M., & others. (2012a). An explorative study of satisfaction level of cyber-crime victims with respect to e-services of banks. *Journal of Internet Banking and Commerce*, 17(3). Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2236575
- Bamrara, A., Singh, G., & Bhatt, M. (2013). Cyber Attacks and Defence Strategies in India: An Empirical Assessment of Banking Sector. *International journal of cyber criminology* 7(1). Retrieved from www.internationaljournalofcriminology.com

- Bernik, I. (2014). Cybercrime: The Cost of Investments into Protection. *Varstvoslovje: Journal of Criminal Justice & Security*, 16(2). Retrieved from http://www.fvv.um.si/rV/arhiv/2014-2/01_Bernik.pdf
- Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. K. (2013). Crime in Cyberspace: Offenders and the Role of Organized Crime Groups. *SSRN Electronic Journal*. <http://doi.org/10.2139/ssrn.2211842>
- CA. (2014). Sector Statistics Report Q2 2014-2015. Retrieved from www.ca.go.ke
- Cassim, F. (2011). Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players. *Comparative and International Law Journal of Southern Africa*, 44(1), 123–138.
- Central Bank of Kenya (2015). 3rd Quarter report. Retrieved from www.cbk.go.ke
- Chauhan, K., & Prasad, V. (2015). Distributed Denial of Service (DDoS) Attack Techniques and Prevention on Cloud Environment. Retrieved from <http://academicscience.co.in/admin/resources/project/paper/f201509251443166942.pdf>
- Chang, Y.C. (2012). *Cybercrime in the Greater China Region: Regulatory responses and crime prevention Across the Taiwan strait*. Cheltenham, UK: Edward Elgar publishing.
- Choo, K.K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8), 719-731.
- Citi. (2014). Fighting cyber-crime together. retrieved from www.citibank.com
- Commonwealth Secretariat. (2014). Report of the Commonwealth Working Group of Experts on Cybercrime. *Commonwealth Law Bulletin*, 40(3), 502–561. <http://doi.org/10.1080/03050718.2014.937068>
- Cortina, J. M. (1993). What is coefficient alpha? An examination of theory and applications. *Journal of Applied Psychology*, 78(1), 98.
- Creswell, J. W. (2003). *Research design: qualitative, quantitative, and mixed method approaches* (2nd ed). Thousand Oaks, Calif: Sage Publications.
- Detica. (2011). The Cost of Cybercrime. retrieved from www.detica.com
- Dimaggio, P.J., & Powell, W.W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociology Review* 48(2). Retrieved from <http://links.jstor.org>
- Elhadi, A.A., Maarof, M.A., & Osman, A.H. (2012). Malware detection based on Hybrid Signature Behaviour Application Programming Interface call Graph. *American journal of Applied Sciences*, 9(3), 283

- Etaher, N., & Weir, G. (2014). Understanding the threat of banking malware. In *Cyberforensics 2014-International Conference on Cybercrime, Security & Digital Forensics* (pp. 73–80). Retrieved from <http://strathprints.strath.ac.uk/48856/>
- European Commission. (2007). The commission communication “towards a general policy on the fight against cybercrime”. Retrieved from <http://www.ec.europa.eu/commission>
- EY. (2015). Megatrends 2015: Making sense of a world in motion. Retrieved from www.ey.com
- Faqir, R. S. (2013). Cyber Crimes in Jordan: A Legal Assessment on the Effectiveness of Information System Crimes Law No (30) of 2010. *International Journal of Cyber Criminology*, 7(1), 81.
- Fick, J. (2009). Prevention is Better than Prosecution: Deepening the Defence against Cyber Crime. *Journal of Digital Forensics, Security and Law*, 4(4), 51–72.
- Gaikwad, B. P., & Jadhav, M. E. (2015a). Cyber Crime Intensification in the World. *Advances in Computational Research*, 7(1), 179.
- Gentzoglanis, A., & Levin, A. (2014). Fraud and Privacy Violation Risks in the Financial Aggregation Industry. Retrieved from http://www.ryerson.ca/content/dam/tedrogersschool/privacy/AODAforms/OPC_Financial_Aggregators_FinalReport_April_2014.pdf
- Gordon, S. (2005). Fighting Spyware and Adware in the Enterprise. *Information Systems security*, 14(3), 14–17.
- Guitton, C. (2012). Criminals and cyber attacks: The missing link between attribution and deterrence. *International Journal of Cyber Criminology*, 6(2), 1030–1043.
- Hamad, N., Manan, A., Shabiralyani, G. & Iqbal, N. (2015). A Quantitative Approach to cybercrimes Impact on Society in Pakistan Case Study: Business Community of Southern Punjab. *Journal of Information Engineering and Applications*, 5(5), 50–55.
- Harris, A. (2013). The Invisible [cyber attacks on critical infrastructure]. *Engineering & Technology*, 8(10), 40–42.
- Idika, N., & Mathur, A.P (2007). A survey of malware detection techniques. *Purdue University*, 48. Retrieved from <http://cyberunited.com/wp->
- Institute of Electrical and Electronics Engineering, & Communications Society (Eds.). (2015). *2015 17th International Conference on Advanced Communications Technology (ICACT 2015): Phoenix park, PyeongChang, South Korea, 1-3 July 2015*. Piscataway, NJ:IEEE.

- Kanyaru, P. M., & Kyalo, J. K. (2015). Factors Affecting the Online Transactions in the Developing Countries: A Case of E-Commerce Businesses in Nairobi County, Kenya. *Journal of educational policy and entrepreneurial research*, 2(3), 1–7.
- Kaspersky. (2014). Kaspersky Lab Report: Financial cyber threats in 2014. Retrieved from www.kaspersky.com
- Kaspersky. (2015). Kaspersky Security Bulletin 2015 Overall statistics for 2015. retrieved from www.kaspersky.com
- Kesharwani, A., & Radhakrishna, G. (2013). Drivers and Inhibitors of Internet Banking Adoption in India. *Journal of Internet Banking and Commerce*, 18(3), 1–18.
- Kibet, L. (2015, OCT 28). Cybercrime cost Kenyan companies Sh 15 billion. *The Standard*. Accessed from www.standardmedia.co.ke
- Kozak, M., Iefremova, O., & Hartley, J. (2015). Spamming in scholarly publishing: A case study. *Journal of the Association for Information Science and Technology*, n/a–n/a. <http://doi.org/10.1002/asi.23521>
- KPMG. (2014). Cybercrime survey report 2014. retrieved from kpmg.com/in
- Kshetri, N. (2010). Diffusion and Effects of Cyber-Crime in Developing Economies. *Third World Quarterly*, 31(7), 1057–1079. <http://doi.org/10.1080/01436597.2010.518752>
- Laeven, M. L., Ratnovski, L., & Tong, H. (2014). *Bank size and systemic risk*. International Monetary Fund.
- Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, 45, 58–74. <http://doi.org/10.1016/j.cose.2014.05.006>
- Lerner, Z. (2014). Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets. *Harv. J. Law & Tec*, 28, 237–325.
- Leukfeldt, R., Veenstra, S., & Stol, W. (2013). High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands. *International Journal of Cyber Criminology*, 7(1), 1–17.
- Locke, C. (2014). *The Financial Services industry must set a higher security standard in the fight against cybercrime*. Intelligent environments'. Retrieved from www.intelligentenvironments.com
- Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime*, 14(1), 52–60. <http://doi.org/10.1080/17440572.2012.759508>
- Machogu, A. M., & Okiko, L. (2012). The Perception of Bank Employees towards Cost of Adoption, Risk of Innovation, and Staff Training's Influence on The

Adoption of Information and Communication Technology in The Rwandan Commercial Banks. *Journal of Internet Banking & Commerce*, 17(2), 1–15.

Mansfield, E.R., & Helms, B.P., (1982). Detecting Multicollinearity. *The American Statistician*, 36(3), 156-160.

Mcfee. (2014). Mcfee Labs Threat Report. Retrieved from www.mcfee.com

McGuire, M., & Dowling, S. (2013). Cyber-enabled crimes-fraud and theft *Cybercrime: A review of the evidence Home office*.

Menon, S., & Guan Siew, T. (2012). Key challenges in tackling economic and cyber crimes: Creating a multilateral platform for international co-operation. *Journal of Money Laundering Control*, 15(3), 243–256.
<http://doi.org/10.1108/13685201211238016>

Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. *The Journal of Economic Perspectives*, 23(3), 3–20.

Mutevu, R. M. (2015). Effects of technological innovations on financial performance of commercial banks in kenya: a case of equity bank of kenya. *Strategic Journal of Business & Change Management*, 2(1). Retrieved from
<http://strategicjournals.com/index.php/journal/article/view/74>

Narteh, B. (2012). Challenges of Marketing E-banking Services in a Developing Country: The Case of Ghana. *Journal of Internet Banking and Commerce*, 17(2), 2–21.

NCSC. (2013). Cyber Security Assessment Netherlands. Retrieved from www.ncsc.nl

Nduati, S.M. (2015). Cyber laws and regulations for enhancing e-commerce including case studies and lessons learned. Retrieved from www.centralbank.go.ke

Nicholas, J. (1990). *Introduction to descriptive statistics*. Mathematics Learning Centre, University of Sydney. Retrieved from
http://www.sportsunion.usyd.edu.au/stuserv/documents/maths_learning_centre/descstats.pdf

Nyangosi, R., & Arora, J. S. (2009). Emergence of Information Technology in the Kenyan banking Sector: An empirical study. *International Journal of Electronic Finance*, 3(2), 6–12.

O'brien, R. M. (2007). A Caution Regarding Rules of Thumb for Variance Inflation Factors. *Quality & Quantity*, 41(5), 673–690. <http://doi.org/10.1007/s11135-006-9018-6>

- O'Donovan, G. (2002). Environmental disclosures in the annual report: Extending the applicability and predictive power of legitimacy theory. *Accounting, Auditing & Accountability Journal*, 15(3), 344–371. <http://doi.org/10.1108/09513570210435870>
- OECD. (2013). *Electronic and Mobile Commerce* (OECD Digital Economy Papers No. 228). Retrieved from http://www.oecd-ilibrary.org/science-and-technology/electronic-and-mobile-commerce_5k437p2gxw6g-en
- Okiro, K., & Ndungu, J. (2013). The impact of mobile and internet banking on performance of financial institutions in Kenya. *European Scientific Journal*, 9(13). Retrieved from <http://www.eujournal.org/index.php/esj/article/view/1046>
- Omuya, A. (2014, Dec 3). 77 Chinese held in cyber bust. *Daily Nation*. Accessed from www.nation.co.ke
- Onyango, P. O. (2014). Examining 'Electronic Fraud' in Kenya and the Impact on Commercial Justice.
- Osborn Quarshie, H., & Martin- Odoom, A. (2012). Fighting Cybercrime in Africa. *Computer Science and Engineering*, 2(6), 98–100. <http://doi.org/10.5923/j.computer.20120206.03>
- Pasricha, P., & Mehrotra, S. (2014). Electronic crime in Indian banking. *Sai Om Journal of Commerce & Management: A Peer Reviewed National Journal (Online ISSN 2347-7563)*, 1(11), 7–14.
- Ponemon Institute. (2012). 2012 Cost of Cybercrime Study: United States. retrieved from www.ponemon.org
- Ponemon Institute. (2013). 2013 Cost of Cyber crime Study: United states. retrieved from www.ponemon.org
- Pwc. (2015). Current fraud trends in the financial sector. retrieved from www.pwc.in
- Pwc. (2014). Financial Service sector analysis of PwC's 2014 Global Economic Crime Survey. Retrieved from www.pwc.com/crimesurvey
- Pwc. (2014). Global Economic Crime Survey: Kenya Report. Retrieved from www.pwc.com/ke/crime-survey
- Raghavan, A. R., & Parthiban, L. (2014). The effect of cybercrime on a Bank's finances. Retrieved from <http://www.ijcrar.com/vol-2-2/A.R.%20Raghavan%20and%20Latha%20Parthiban.pdf>
- Rao, G. N., Giridhar, T. V. N., & Kiran, K. V. D. (2015). Effects of Cyber Crime and their Access Controls. Retrieved from <http://ijrest.net/downloads/volume-2/issue-4/pid-ijrest-24201503.pdf>

- Rogelberg, S.G. (Ed.). (2002). *Handbook of research methods in industrial and organizational psychology*. Malden, Mass: Blackwell Publishers.
- Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, 2, 202–209.
- Sekaran, U., & Bougie, R. (2009). *Research methods for business*. Chichester, West Sussex. John Wiley & Sons.
- Schneider, G.P. (2011). *E-business* (9. Ed., internat. Ed). S.I.: Course Technology Cengage Learning.
- Scott, W. R. (1987). The Adolescence of Institutional Theory. *Administrative Science Quarterly*, 32(4), 493. <http://doi.org/10.2307/2392880>
- Sedighi, R., & Ghahremani, M. (2015). Investigating and Identifying the Cybercrimes Relevant to Banking Network and the Quality of Prevention (the case study of Mahabad banks). Retrieved from http://www.irjabs.com/files_site/paperlist/r_2528_150304011514.pdf
- Serianu. (2014). Kenya Cyber Security Report 2014. Retrieved from www.serianu.com
- Serianu. (2015). Kenya Cyber Security Report 2015. Retrieved from www.serianu.com
- Shah, K. (2015). Phishing: An Evolving Threat. *International Journal of Students' Research in Technology & Management*, 3(1), 216-222.
- Shah, M. H. (2013). Critical success factors for preventing e-banking fraud. *Journal of Internet Banking and Commerce*, 18(2). Retrieved from <http://www.arraydev.com/commerce/JIBC/2013-08/Usmanv01.pdf>
- Singleton, T., Singleton, A., & Gottlieb, G. (2006). Cyber threats facing the banking industry. *Bank Accounting & finance* .
- Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review*, 20(3), 571–610.
- Symantec. (2014). Internet Security Threat Report. retrieved from www.symantec.com
- Templeton, G.F. (2011). A two-Step Approach for Transforming Continuous Variables to Normal: Implications and Recommendations for IS Research. *Communications of the Association for Information System*. retrieved from <http://aisel.aisnet.org/cais>

- Trend Micro, (2014). Turning the tables on Cyber Attacks: responding to Evolving tactics. retrieved from www.trendmicro.com
- Van der Putten, F.-P., Meijnders, M., & Rood, J. (2015). Deterrence as a security concept against non-traditional threats. Retrieved from http://www.clingendael.nl/sites/default/files/deterrence_as_a_security_concept_against_non_traditional_threats.pdf
- Venkatraman, S., & Delpachitra, I. (2008). Biometrics in banking security: a case study. *Information Management & Computer Security*, 16(4), 415–430. <http://doi.org/10.1108/09685220810908813>
- Venuti, L. (1998). *The scandals of translation: Towards an ethics of difference*. Taylor & Francis US.
- Vrancianu, M., Popa, L. A., & others. (2010). Considerations regarding the security and protection of e-banking services consumers' interests. *The Amfiteatru Economic Journal*, 12(28), 388–403.
- Wada, F., & Odulaja, G. O. (2012). Electronic Banking and Cyber Crime In Nigeria- A Theoretical Policy Perspective on Causation. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.411.2862&rep=rep1&type=pdf>
- Wafula, C. (2015, Sept 11). 21 govt officials named in NYS scandal report. *Daily Nation*. Accessed from www.nation.co.ke
- Wale, M. S., Jadhav, A., Kale, B., & Gupta, A. (2014). Anti phishing using (t, n) Visual Cryptography Scheme For Commerce Bank. Retrieved from http://www.ermt.net/docs/papers/Volume_4/2_February2015/V4N1-136.pdf
- Wall, D. (2005). *Cybercrime: the transformation of crime in the information age*. Cambridge: Polity.
- Wall, D. (2007). *Cybercrime: the transformation of crime in the information age*. Cambridge: Polity.
- Wall*, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime 1. *International Review of Law Computers & Technology*, 22(1-2), 45–63.
- Wang, P., Wu, L., Aslam, B., & Zou, C.C. (2015). Analysis of Peer-to-Peer Botnet Attacks and Defences. In *Propagating Phenomena in Real World Networks* (pp. 183–214). Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-3-319-15916-8_8
- Warner, J. (2011). Understanding cyber-crime in Ghana: A view from below. *The International Journal of Cyber Criminology*, 5, 736–749.

Weiner, J. (2007). Measurement: reliability and validity measures. *Bloomberg School of Public Health, Johns Hopkins University, Mimeo (power point presentation) OxfordJournals.org*. Retrieved from http://ocw.jhsph.edu/courses/hsre/PDFs/HSRE_lect7_weiner.pdf

Williams, R. (2015). Review of Multiple Regression. University of Notre Dame, <http://www3.nd.edu/~rwilliam/>

Williams, S. M. (1999). Voluntary environmental and social accounting disclosure practices in the Asia-Pacific region: An international empirical test of political economy theory. *The International Journal of Accounting*, 34(2), 209–238.

Yazdanifard, R. Y., Yusoff, W. F. W., & Sade, A. C. B. A. B. S. (2011). Electronic Banking Fraud; The Need To Enhance Security And Customer Trust In Online Banking. *International journal on Advances in Information Sciences and Service Sciences*, 3(10), 505–509. <http://doi.org/10.4156/aiss.vol3.issue10.61>

APPENDIX I: Questionnaire

Part I: General Information

Position held in the organization.....

Department.....

Part II: Establishing the cyber attack frequency in the banking industry in Kenya.

A. Please indicate the frequency of each threat by ticking appropriately

Cyber-attack types	Never 1	Yearly 2	Monthly 3	Weekly 4	Daily 5
ATM/Card fraud					
Denial of service/distributed denial					
Botnet					
Spamming					
Phishing					
Viruses					
Worms					
Trojan horse					
Spy ware					
Adware					
Key loggers					
Hacking					
Vishing					
SMSishing					
Please indicate any other types					

Part III: Establishing the strategies employed by banks to mitigate cybercrime.

B. Please indicate the extent of adopting the following **Proactive** strategies

Strategy	Not implemented 1	Partially implemented 2	Fully implemented 3
Know-your-enemy			
Training			
IT discipline			
Channel protection			
Defence-in-depth			
Please indicate any other strategy			

KEY

- 1 Not pursued**
- 2 Pursued but still in implementation**
- 3 Documented evidence of full implementation**

C. Please indicate the perceived effectiveness of these strategies.

Strategy	Not effective 1	Partially ineffective 2	Neutral 3	Partially effective 4	Fully effective 5
Know-your-enemy					
Training					
IT discipline					
Channel protection					
Defence-in-depth					
Please indicate any other strategy					

D. Please indicate the extent of adopting the following **Reactive** strategies

Strategy	Not implemented 1	Partially implemented 2	Fully implemented 3
Cyber-kill chain methodology			
Attribution			
Please indicate any other strategy			

KEY

- 1 Not pursued**
- 2 Pursued but still in Implementation**
- 3 Documented evidence of full implementation**

E. Please indicate the perceived effectiveness of these strategies.

Strategy	Not effective 1	Partially ineffective 2	Neutral 3	Partially effective 4	Fully effective 5
Cyber-kill chain methodology					
Attribution					
Please indicate any other strategies					

Thank you for taking the time to answer all the questions to the best of your ability. Your assistance is highly appreciated.

APPENDIX II: List of banks

Table 12 List of banks and total assets

BANK	TOTAL ASSETS (Ksh '000')
1. ABC BANK	21,438,729.00
2. AFRICAN DEVELOPMENT BANK	16,954,227.00
3. BANK OF INDIA	34,370,422.00
4. BANK OF AFRICA KENYA LIMITED	62,211,641.00
5. BARCLAYS BANK	226,118,124.00
6. BANK OF BARODA (KENYA) LTD	61,944,650.00
7. CFC STANBIC	171,347,152.00
8. CHASE BANK (KENYA) LTD	107,112,469.00
9. CITIBANK NA KENYA	79,397,808.00
10. COMMERCIAL BANK OF AFRICA	197,463,704.00
11. CONSOLIDATED BANK	15,077,051.00
12. COOPERATIVE BANK	285,396,067.00
13. CREDIT BANK LTD	8,864,537.00
14. DEVELOPMENT BANK	16,954,227.00
15. DIAMOND TRUST BANK	211,539,412.00
16. ECOBANK KENYA LTD	45,934,458.00
17. EQUITY BANK	344,572,000.00
18. EQUATORIAL BANK	16,589,359.00
19. FAMILY BANK	61,812,663.00
20. FIDELITY BANK	16,515,404.00
21. FIRST COMMUNITY	15,278,026.00
22. GIRO COMMERCIAL BANK	15,082,199.00
23. GUARANTY TRUST BANK	32,991,926.00
24. GUARDIAN BANK LTD	14,572,873.00
25. GULFAFRICAN BANK	19,753,647.00
26. HABIB BANK	9,449,365.00
27. HABIB A.G ZURICH	12,147,286.00
28. HOUSING FINANCE CO.	60,961,680.00
29. I &M BANK	137,196,446.00
30. JAMII BORA BANK	13,117,892.00
31. KCB	490,338,324.00
32. K-REP BANK (SIDIAN)	15,798,777.00
33. MIDDLE EAST BANK	5,936,601.00
34. NATIONAL BANK	122,864,886.00
35. NIC BANK	137,087,464.00
36. ORIENTAL COMMERCIAL BANK	7,857,515.00
37. PARAMOUNT UNIVERSAL	10,402,326.00
38. PRIME BANK	54,917,674.00
39. STANCHART	222,635,993.00
40. TRANS NATIONAL BANK	10,239,922.00
41. UBA KENYA LTD	4,755,787.00
42. VICTORIA COMMERCIAL BANK	17,244,092.00

APPENDIX III: Definitions of identified types of cyber-attack

Table 13 Definitions of cyber-attacks

Cyber-attack type	Author	definition
ATM/Credit card fraud	(Balan &Popescu, 2011); Detica, (2011)	The misuse of a credit card to make purchases without authorization or counterfeiting a credit card.
Denial of service/ distributed denial of service (DDoS)	(Chauhan & Prasad, 2015);Singleton, Singleton & Gottlieb, (2006); Detica, (2011)	An attack with the purpose of preventing legitimate users from using a specified network resource. DDoS is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems.
Botnet	(Lerner, 2014); Wang, Wu, Aslam, & Zou, 2015).	A network of computers coordinated by a single control mechanism, often programmed to complete a set of repetitive tasks. It signifies a network of zombies-compromised computers used without the owner's knowledge or permission.
Spamming	(Kozak, Iefremova, & Hartley, 2015); IEEE, (2015)	Unsolicited bulk e-mail- the recipient has not requested the message and the message is sent as part of a larger package of messages with substantially the same content.
Phishing	(Wale, Jadhav, Kale, & Gupta, 2014); (Pasricha & Mehrotra, 2014)	Criminals attempt to fraudulently acquire sensitive information like user's id, passwords, contacts and credit card info by masquerading as trustworthy person or business in an electronic communication.

Viruses	(Etaher & Weir, 2014); Idika&Mathur, (2007)	Self replicating programs that modify the contents of files by hiding within other inoffensive programs in order to perform malicious acts. Spreads through media e.g. USB cable.
Worms	(Etaher & Weir, 2014); Idika&Mathur, 2007	Self replicating, self contained computer programs which perform destructive actions by invading computers in a network. Perform infection action without human intervention.
Trojan horses	(Etaher & Weir, 2014); Kaspersky, (2014); , Singleton & Gottlieb, 2006	Apparently harmless computer programs that may appear useful and functional but contain harmful components that will insert themselves into a machine and install an illicit or malicious action. Require human assistance to spread and cannot self-replicate.
Spyware	(Etaher & Weir, 2014);Wall, (2007); Gordon, (2005).	Program installed on a computer in order to transmit, track and report information regarding the activities of an internet user without their consent.
Adware	(Etaher & Weir, 2014); Gordon, (2005)	Software that installs to provide advertisers with information about the browsing habits of the users.
Key loggers	Etaher & Weir, (2014); Kaspersky, (2014)	Malware whose goal is to secretly collect critical information such as passwords, logins and other credentials manually entered from client server device and transmit it to the source of the infection.
Hacking	(Rathore&Marwaha, 2015); Bamrara, Singh & Bhatt, (2012)	Unauthorised access made by a person to cracking the system or an attempt to bypass the security mechanism by penetrating the bank sites/ customer a/cs.

Vishing	(Pasricha & Mehrotra, 2014); shah, (2015)	Phishing using a phone number owned by the criminals which when dialled, prompts the user to enter the account number and PIN. Uses fake caller id to give the appearance that the call originates from a trusted organization.
SMSishing	(Pasricha & Mehrotra, 2014); Shah, (2015)	Phishing using short messaging service giving the appearance of originating from a trusted organization.

APPENDIX IV: Definitions of identified strategies against cybercrime

Table 14 Definitions of identified strategies against cybercrime

Strategy	Authors	Definition
Know-your-enemy	Citi, (2014); Symantec,(2014); Kaspersky, (2014)	Behaviour analysis to flag anomalies in transactions and network activity and issue warnings
Training	KPMG, (2014); Citi, (2014); Shah, (2013); Kaspersky, (2014)	Raising the awareness of customers and employees on cybercrime
IT discipline	Shah, (2013); Symantec,(2014); Kaspersky, (2014); KPMG, (2014).	Vigilance by IT staff through updating Anti-viruses/malware, Browsers, Operating systems
Channel protection	Venkatram&Delpachitra, (2008); KPMG, (2014); Citi, (2014); Kaspersky, (2014)	Blocking unauthorised access through strong log in credentials, Biometrics, Encryption, Chip and Pin
Defence-in-depth	Fick, (2009); Symantec, (2014); Citi, (2014)	Multiple, overlapping and mutually supportive defence systems; Clear policies and procedures; involve both public and private partners.
Cyber-kill-chain method	Mathur, et al., (2013); Elhadi, et al., (2012); Idika, et al., (2007)	Victim collects and tags information in order to identify threats at the earliest stage and counter it. Achieved through continuous systems monitoring.
Attribution	Guitton, (2012); Cassim, (2011); saini, et al., (2012); Kshetri, (2010)	Digital investigation to identify the criminal and gather evidence and successful prosecution