EFFECT OF CYBER CRIME RELATED COSTS ON DEVELOPMENT OF FINANCIAL INNOVATION PRODUCTS AND SERVICES;

A Case Study of NIC bank of Kenya

ELIZABETH WAMBUI NJOROGE

Research Project Submitted to the Department of Business and Social Science in Partial Fulfillment of the Requirements Award of Master of Business Administration of Jomo Kenyatta University of Agriculture and Technology

May, 2017.

DECLARATION

This research proposal is my own original work and has not been presented for award of any degree in any other university or institution of higher learning.

Signed ……. Date……

ELIZABETH WAMBUI

HD333-C002-4062/2014

This Proposal has been submitted for examination with my approval as University Supervisor

Signed…… Date …….

Dr. AGNES NJERU

ACKNOWLEDGEMENT

I would like to acknowledge the efforts of all those individuals whose contribution and assistance made the completion of this research proposal possible.

First, I acknowledge the almighty God, who makes all things possible within time.

I would also like to acknowledge and appreciate the invaluable assistance of my university supervisor Dr. Agnes Njeru who patiently guided me through this process.

Lastly my sincere gratitude goes to my parents, friends and classmates for all their assistance and support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

DEFINITION OF TERMS

Hacking is a criminal activity that relies on the dependence of computers and networks, including the Internet (Hutchison, 1997).

Cybercrime - also called computer crime, is any illegal activity that involves a computer or network-connected device, such as a mobile phone. It divides cybercrime into three categories: crimes in which the computing device is the target, for example, to gain network access; crimes in which the computer is used as a weapon, for example, to launch a denial of service (DoS) attack; and crimes in which the computer is used as an accessory to a crime, for example, using a computer to store illegally-obtained data. (Howard, 1997).

Phishing - is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication pay pal, e-Bay and online banks are targets. Phishing is typically carried out by e-mail or instant messaging and often directs users to enter details at a web-site although phone contact has also been used. Jaishankar, K. (2007).

Email spoofing – a term used to describe fraudulent e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. E-mail spoofing is a technique commonly used for spam e-mail and phishing to hide the origin of an e-mail message. (Lewis & Baker, 2013).

Cyber terrorism- is unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

ABBREVIATIONS &ACRONYMS

ATM	Automated Teller Machine
E-Banking	Electronic Banking
ICTD	Information and Communication Technologies and Development
ISP	Internet Service Providers
IT	Information Technology
MFS	Mobile Financial Services
MNOs	Mobile Network Operators

ABSTRACT

The aim of this study was to investigate whether there is a significant impact of cyber-crime related costs on the development of banking products that is financial innovation by Kenyan commercial banks. Given the fact that the cost of doing business under the new ever changing information communication and technology platform, the question was whether these costs are deterring banks from operating in this new risky environments and platforms or to what extent are these affecting the rate at which banks are developing new ideas and products that are transacted on an online platform. The research proposal adopted four independent variables to help estimate these effect which include prevention and detection costs, response costs and indirect costs and the rate of developed financial products as the dependent variable. The study used a questionnaire where it was administered to establish the effect of these factors. The respondents/ population of this research proposal was 957 bank employees, inclusive of 167 support staff, at NIC bank of Kenya. The study used a case study of the NIC bank of Kenya through purposive. A sample of 10% out of the bank employees minus the support staff gave a sample size of 80 respondents. The interview guides was to be self-managed to allow for convenience and reliability of the data. A pilot study was done on the area of study in order to measure the validity and reliability of the data collection instrument. The study adopted a descriptive research design where SPSS was used to model the relationship between the various selected variables and test there explanatory power. After the analysis the data was presented through the use of various presentation tools such as graphs pie charts and tables. The study analyzed and observed that prevention and detection costs such as insurance fees and IT compliance costs have an influence on development of banking products but were not significant. The other costs, direct costs, such as cost of business continuity direct financial loss, compensation payments, legal costs and indirect costs such as reputational damage and loss of confidence by customers were huge concerns and very significant influencers of development of innovated banking financial products and services. Therefore based on the study findings, the study recommends that developed banking products and services are becoming quite popular in the market and also very significant to all consumers, therefore banking service providers should consider providing novel technologies that are costs effective on the consumer and also on the bank operations

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

The term ICT according to Zuppo (2012) that is information and communication technology can be defined as a combination of communication applications and procedures and devices that include phones, computer and network hardware and software. Milis & Mercken (2002) Information and communication technologies have been implemented in various sectors in the economy such as the education sector, health care, financial sector to aid in service delivery. Information communication and technology has been customized over the years to fit in all sectors as it is needed based on the services that each sector provides.

According to Reynolds, Treharne & Trippo (2003) the rate at which human beings are transitioning from manual operations is now increasingly depending on digital communication and other innovations in the information and communication industry. In the financial sector ICT has been influential in enabling financial institutions in extending its services through financial inclusion of people unreachable by this services and also diversifying its services (Pilat, Lee & Van Ark2003).According to Agboola (2007) In this day an era people can now access simple services such as cash deposit and withdrawal, payment of bills and payment of other daily services from their phones, computers and other electronic devices that are being developed on a daily basis. Agboola (2007) connectivity therefore has increased enabling people to access market information, and relevant services which is helping to make life easier for people.

Information communication and technology has proved to be a powerful tool in extending economic opportunities to all individuals, groups, businesses and institutions all over the world

(Stiroh, 2002). According to Avgerou (2003) information communication technology has contributed to the concept of global economic shrinkage in terms of allowing connectivity for people form any point on the globe. According to statistics all new mobile owners and customers in the coming generations will be mostly from developing and third world states which is an indication that the ICT platform is enabling connectivity from those who are well developed to those who are developing. According to Agboola (2007) today businesses and financial institutions that invest heavily in information and technology have a competitive edge in terms of being more productive, growing faster, more investment opportunities and more profits.

Kshetri (2005) despite all the benefits accrued or linked to the extensive usage of information technologies, the increased dependency has also translated into a growing rate of criminal activities conducted via the same ICT platform. Bell (2002) the expansion of cyber functionalities has, however, also opened up new opportunities for people to carry out criminal activities online, and/or to use the Internet as a medium for their criminal objectives. The advantages of the Internet come with risks. Kshetri (2005) while organizations and individuals are exploiting its business benefits they may not realize that cyberspace confers the same benefits on those who wish to attack them.

Much has been done on how information and communication technologies or cyberspace is beneficial to all sectors of an economy, less has been done on the criminal activities that characterize this new revolution and it affects the activities of institutions today such as development of new financial products. Kshetri (2005) the understanding of cybercrime and its consequences, both economic and social, is still limited. Cybercrime has been also increasing at the rate at which new technological innovations are being invented. Bell (2002)

users of ICT technologies have been facing lots of criminal activities recently from cyberspace as a result of the risk that lie within the information communication sector. The cost of this criminal activity have now reached a significant point where a need to address them is long overdue. As cybercrime becomes more of an issue many organizations seek to protect themselves using courses to train employees in the very real risks of the online world. This paper seeks to address this costs and how they are affecting the performance of banks today and more specifically the development of new bank products.

1.1.2 Application of ICT in the Banking sector

Electronic banking (e-banking), also known as Internet banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels (Liao & Cheung (2002). E-banking includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the internet. Customers access e-banking services using an intelligent electronic device, such as a personal computer (PC), personal digital assistant (PDA), automated teller machine (ATM), kiosk, or Touch Tone telephone. The electronic transaction services are aimed at improving the market share and business growth of the financial industry.

Bell (2002) the terms computer crime, high-tech crime, digital crime, e-crime and cyber-crime can be used interchangeably with electronic crime**.** E-crimes are essentially crimes where the computer is used either as a tool to commit the crime, as a storage device, or as a target of the crime. As a storage device, computers can either store information that will assist in the execution of the crime or information that is illegal for the owners to possess, such as stolen

intellectual property. Computers are classified as a target if the information that they contain is altered or retrieved in an unlawful way, such crimes can range from amateur hacking to terrorism.

1.1.3 Cyber security issues in Kenya

Over the last few years, cyber security has gone from a concern that loomed large in the future for East Africa to an issue of pressing importance. Wyche et al, (2010) In Kenya one of Africa's largest economies and East Africa's central tech hub it is estimated that cybercrimes cost the country more than 2 billion Kenyan shillings (US$22.56 million) in 2013 (Otieno & Kahonge, 2014). The government of Kenya is losing an estimated Sh5 billion a year to cybercrime. A report by IT services consulting firm Serianu in partnership with PKF Consulting and USIU Africa titled "The Kenya Cyber Security Report 2015", shows that the country loses Sh15 billion (USD146 Million) to cybercrime, with the public sector accounting for Sh5 billion(Kaigen et al, 2015). The financial services sector follows at Sh4 billion while manufacturing and industrials at Sh3 billion in third place.

According to Kenya Cyber security report (Kaigen et al, 2015) an independent review of online banking; shopping and payments websites in Kenya, revealed that Kenyan online banking portals have limited security mechanism to protect the customer's login credentials to the platform. Out of 33 banks sampled, only 2 banks had client side encryption implemented. Kenyan banks last year migrated their customers from the magnetic strip to the more secure chip and-pin technology cards, increasing the security for ATM and Point of sale transactions, but it is now emerging that most of the fraudsters moved online where fraud has been on the rise.

Kaigen et al, (2015) due to high rate of cybercrime, banking institutions have been using huge part of their revenues to prevent cyber-crime. In the market, various IT-based banking products, services and solutions are available such as Phone Banking; ATM facility; Credit, Debit and Smart Cards; Internet. Banking & Mobile Banking; SWIFT Network & INFINET Network; Connectivity of bank branches to facilitate anywhere banking.

1.2 Statement of the problem

Recent studies published on the evolution ICT present concerning scenarios, characterized by the constant growth of cyber-criminal activities. Even though the level of awareness of cyber threats has increased, and law enforcement acts globally to combat them, illegal profits have reached amazing figures. The impact to society has become unsustainable, considering the global economic crisis.

The proliferation of, and rapid advances in, technology-based systems, especially those related to the internet, are leading to fundamental changes in how companies interact with customers Kaigen et al, (2015). Internet banking has become the self-service delivery channel that allows banks and various other businesses to provide information and offer services to their customers with more convenience via the web service technology. Kaigen et al, (2015) in addition to this, the challenging business processes in the financial services pressurized banks to introduce alternate business channels to attract customers and improve customer perception.

Kaigen et al, (2015) cybercrimes against banks and other financial institutions probably cost many hundreds of millions of dollars every year. Cyber theft of intellectual property and business-confidential information probably costs developed economies billions of dollars. Kaigen et al, (2015)these losses could just be the cost of doing business or they could be a major

new risk for companies and nations as these illicit acquisitions damage global economic competitiveness and undermine technological advantage. Kaigen et al, (2015) these costs are now greatly affecting the bottom line or profits generated from innovative activities by banks today. The above mentioned studies by Kaigen et al, (2015) plus other studies by Jackson et al (2004), and Kshetri (2005) only describe the economic impact in general, none of this studies narrow down to what costs banks are incurring as a result of cybercrime and how it is affecting performance and innovation. Therefore the study intends to establish the types, impact and mitigations of cybercrime related costs in the development of financial products in Kenyan Banks.

1.3 General objective

The effects of cybercrime related costs on development of financial products: A case study of NIC bank.

1.3.1Specific Research Objectives

The study specifically sought:

i. To establish the effects of cyber-crime prevention and detection costs on development of financial products by NIC bank in Kenya.
ii. To assess the effects of Cybercrime response costs on development of financial products by NIC bank in Kenya.
iii. To determine the effects of indirect costs on development of financial products by NIC bank in Kenya.

1.4 Research Questions

i. What is the effect of prevention and detection of cybercrime costs on development of financial products by NIC bank in Kenya?

ii. What is the impact of Cybercrime response costs on the development of financial products by NIC bank in Kenya?

iii. What is the effect of indirect costs on development of financial products by NIC bank in Kenya?

1.5 Scope of the Study

The study offers an in depth look into the effects of cybercrime related costs on development of financial products in Kenyan Banks. The study will narrow down to an analysis of NIC Bank of Kenya as one of the financial institutions in Kenya that has faced cyber-crime incidences recently.

1.6 Significance of the Study

1.6.1 Commercial Banks in Kenya

Commercial Banks in Kenya will significantly benefit from the study as they will be in a position to know where to invest in security measures to protect their systems against cybercrime. They will be interested to learn the Policies and regulations existing in combating cybercrime and compliance to the said policies. It will paint a clear picture on how much is being used to combat cybercrime and whether the cost benefit analysis in adoption and application of ICT technologies in relation to development of financial products is worth. It will help banks determine which costs are relevant and which once are necessary based on different environmental settings.

1.6.2 Researchers

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

1.6.3 Academicians and practitioners

This study is important to academicians and practitioners in building their knowledge base and creating an insight in understanding the factors that create opportunities for white collar crimes in banking institutions and how it influences performance of financial institutions and most specifically banking institutions.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter discusses a review of literature related to the study. It covers theoretical, conceptual and empirical literature on the effects of cybercrime related costs on the development of financial products by commercial banks a case study of NIC bank of Kenya.

2.2 Theoretical review

2.2.1 Space Transition Theory

This theory was developed by Jaishankar in 2007 and published in his book on Crimes of the Internet (Jaishankar 2007). There has been inadequate theoretical explanations as to why there is a rampant increase in cyber related crimes. This theory of space transition theory tries to give an explanation for the phenomena of cybercrimes. This theory states that people who usually feel there criminal nature is repressed by the physical space have a tendency to engage in crime in cyber space which otherwise they would not commit in a physical setting due to their status and role. This nature of crime is associated with characteristics such as identity flexibility, dissociative obscurity which make it easy for people to commit offenses. The emergence of and advancements in the field of information and communication technologies has created a range of new criminal activities within the economic and social space. All these activities have had a great impact on how financial institutions and more specifically banks are performing. As this theory

states people involved in cyber related offenses are not hardcore but rather the white collar community who are within a closed community such as a bank. Detection becomes hard and the costs increase gradually at to a point where the impact on the intrusions bottom line is evident.

Therefore the postulations of this theory is that one of the factors contributing greatly to the increasing costs that banks are facing in relation to cyber space loopholes is the complex nature and characteristics and behavior of the offenders within the information and communication environment. The postulates of the theory are: Persons, with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position. Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cybercrime. Criminal behavior of offenders in cyberspace is likely to be imported to Physical space which, in physical space may be exported to cyberspace as well. Intermittent ventures of offenders in to the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape. Strangers are likely to unite together in cyberspace to commit crime in the physical space. Associates of physical space are likely to unite to commit crime in cyberspace. Persons from closed society are more likely to commit crimes in cyberspace than persons from open society. The conflict of Norms and Values of Physical Space with the Norms and Values of cyberspace may lead to cybercrimes.

History shows that the relationship between crime and technology is not new. Although the hardware has changed across the span of time but the basic crime ideas remain same. The significant change in modern time is on increase in personal computing power in a globalized communication network. The networked technology has become more than simply a force

multiplier, because not only the ideas about committing a crime are shared on a global scale, but these ideas are also put to practice across the global network at a very fast speed. Internet is a set of social practices; it is the kind of purpose to which we put the internet that creates the possibility of criminal and deviant activities. The internet provides the means to link up the many and diverse networks already in existence. Since commercialization of the internet during the mid1990s, it has grown manifold. Even though majority of worldwide total internet connections are located in developed countries, the fact is that these are growing at a very fast rate in developing countries too. An Unequal access also follows along existing lines of social exclusion within individual countries and factors such as employment, income, education, ethnic disability are reflected in the patterns of internet use .Castells (2002).These inequalities point out the social characteristics behind the emergence of cybercrime and cybercriminals. Thomas and Loader, (2000) conceptualize cybercrime as those Computer – Mediated-Activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Cybercrime has serious impact on society in the form of psychological disorder, social disorganization and economic losses. Even though all people suffer from its ill effects, the most vulnerable group is adolescent and youth.

2.2.2 Technology Theory

These theory is discussed broadly under computer ethics the philosophy of computing by Johnson (1985) which asserts that the response of technology to the cybercrime problems center on the use of computer security theories to design and evolve solutions that provides authentication, verification, non-repudiation and validation. Johnson, (1985) these theories and models rely on the use of cryptography, steganography, network protocols, and the use of software engineering process/models to develop systems that offer some form of

protection for users and the information infrastructure. Johnson, (1985) cybercrime thrives on the web today because the internet did not inculcate in its protocols from the onset a mechanism that allows a host to selectively refuse messages. The advancement in this field only considered what the technology could do for them and what profit margins it would create, what they failed to consider carefully was what harm the technology could cause to them in terms of losses and costs. Technology theory looks at the weaknesses in within the system that were not considered in the inception stages of every piece of technology being used in financial institutions today.

Banks are incurring a lot of costs today such as reputational damage costs, or opportunity costs, security costs and other costly variables due to the technological short comings within the systems being applied in their daily operations.

Today's society is in the midst of technological revolution. With advances in computers and telecommunications most businesses and many individuals have become highly dependent on computers and networks to carry out everyday activities (Howard, 1997; Sterling, 1992). Howard (1997) indicated that as of the 1996, 13 million hosts systems were accessing the internet. It has been estimated that by the year 2003, the number has risen and will have risen to a little over 200 million. The rush to embrace the new technology and has also introduced a new category of criminal activity and behavior, commonly known as hacking. Hacking is a criminal activity that relies on the dependence of computers and network, including the internet (Hutchison 1997, Stoll, 1985). Those individuals engaged in hacking activities have been termed hackers. The term hacker has had many connotations over the years. It was originally associated with the outstanding and radical programmers in the computer science fields. Today it is commonly referred to an individual engaged in a form of criminal behavior, hacking. Hacking can be

formally defined as either a successful or unsuccessful attempt to gain unauthorized use or access to a computer system. Society is now trying to come to an understanding of the new emerging criminal activity that knows no boundaries and creates a confusion on the preexisting criminal jurisdictions. Behavioral science has been lacking in its research into the phenomena of hacking and as such there has been a large research gap.

Reflecting social anxieties about this surprisingly new phenomenon, the early studies which attracted the most attention were those that focused on pathological internet use and "addiction" Young (1998), but as sociology delved deeper into cyberspace, some very basic questions became apparent. Do traditional concepts and theories suffice in our understanding of online behaviour? Do we have to modify these theories? Do we need to develop new ones? These questions arise out of the recognition that cyber space as a sociological realm is quite different from face to face environment. Geographical boundaries are transcended. Everything is recordable and no boundaries of "privacy" exist. Social interactions can be synchronous, asynchronous, or something in between. Under complete anonymity, people become more disinherited than usual, or they might experiment with different identities. Sensory experience is expanded to multimedia experiences with highly creative fantasies. All these features of online space are characteristic of contemporary society i.e. network society.

2.2.3 Opportunity cost Theory

Anderson et al, (2013) this theory does not focus on the events that contribute to the crime but on the opportunities that emerge as a result of preventive measures to curb the crime. Proponents of this theory argue that crimes transverse between location, time, target, direction, and method of committing the crime. Anderson et al, (2013) further assert that

Opportunity to commit a crime is a root cause of crime. Also, they posit that no crime can occur without the physical opportunity and therefore opportunity plays a role in all crimes, not just those involving physical property thereby reducing opportunity of crime. This theory plays right in the concepts of cybercrime within the financial sector. Opportunities that arise within the banking environment for example poor security measure create an opportunity for someone with an intention of committing crime and it is not limited to the internal environment but also the external environment. According to Buchanan (1991) opportunity cost stands for or can be defined as the benefit forgone as a result of taking another alternative. There are many opportunities presented by various security firms to curb the rate of cybercrime within financial institutions. The decision by managers and directors of this institutions the disregard the eminent risk that lurks out there leads to firms incurring a lot of costs that otherwise would have been averted by taking the opportunities presented to them. The optimal level of cyber security investment depends on factors related to the efficiency of the investment, its marginal cost, and the security returns from the investment, its marginal benefit. These factors are generally related to organizational and performance characteristics, such as an organization's existing information technology (IT)

characteristics, the compatibility of available cyber security technologies with current technologies, the security needs of the products and services the organization provides, and the preferences/perceptions of its customers. In addition, expectations of future threats or compromises, vulnerabilities, and technical change influence the timing of investments and thus the costs incurred and the benefits received.

Putting a number on the cost of cybercrime and cyberespionage is the headline, but the dollar figure begs important questions about the damage to the victims from the cumulative effect of losses in cyberspace. Cybercrime includes the effect of hundreds of millions of people having their personal information stolen. One estimate puts the total at more than 800 million individual records in 2013. This alone could cost as much as $160 billion per year. The constant reports of companies being hacked contribute to a growing sense that cybercrime is out of control. The most important cost of cybercrime, however, comes from the damage it does to company performance and to national economies.

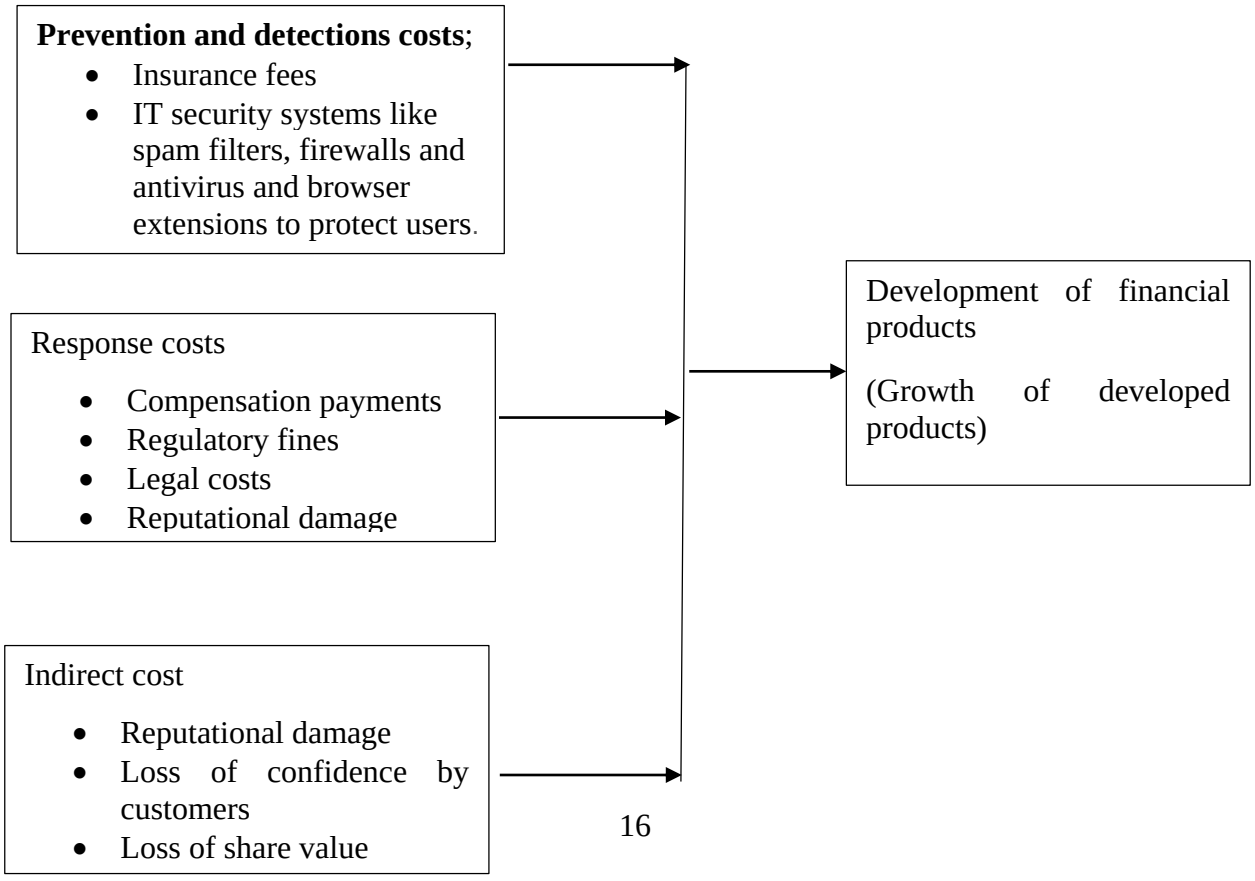
Opportunity cost is the value of forgone activities. Three kinds of opportunity costs determine the losses from cybercrime: reduced investment in research and development (R&D), risk-averse behavior by businesses and consumers, and increased spending on network defenses. For companies, the largest opportunity cost may be in the money spent to secure their networks. While companies would always spend on security even if risk in the digital environment was greatly reduced, there is a "risk premium" that they pay because of unstoppable cybercrime.

Another way to look at the opportunity cost of cybercrime is to see loss as a share of the Internet economy. Studies estimate that the Internet economy annually generates between $2 trillion and $3 trillion, a share of the global economy that is expected to grow rapidly. This estimates suggest that cybercrime is equal to between 15% and 20% of the value created by the Internet, a heavy tax on the potential for economic growth and job creation. Rarely does an organization undertake a comprehensive financial analysis (i.e. Cost-benefit or rate-of-return analysis) prior to making the investment or deciding on the level of investment. In fact, in many instances organizations

simply react to a cyber-attack or a compromise (hereafter referred to simply as a "breach") and spend what it takes to solve the existing problem.

Theorists of the internet agree that cyberspace makes possible near and instant interactions between individuals who are spatially distant, which creates possibility for new forms of association which in turn gives rise to cybercrime and cyber deviance. Cybercrime, in simple terms, is a crime that is facilitated or committed using a computer, network or hardware device. The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime. It can take place on the computer alone, or in other virtual or non-virtual locations. It is recognized that current legal definition of cybercrime varies drastically between jurisdictions.

2.3 Conceptual framework



Independent variable **dependent variable**

Fig. 2.1 conceptual framework

Mugenda and Mugenda (2003), define a conceptual framework as a hypothesized model identifying the concepts under study their relationships. Conceptual framework is the main structure that not only gives form and shape to the entire system, but also supports and holds together all other elements in a rational configuration. In this framework, there are certain factors that affect the development of financial products in commercial banks.These factors include but are not limited to: Prevention and detection costs, response rate costs, indirect costs that are result from cybercrime activities and rate of usage of developed products.

The independent variables constitute the Prevention and detection costs, response rate costs, indirect costs that affect the development of financial products these costs have a direct effect on development of financial products as this limits innovation in financial and banking sector. The ever rising rate of changing technology has increased the avenues for cybercrime activities in financial sector. This in itself calls for the banks to invest in sophisticated ways to mitigate against any eventualities that may arise;

The dependent variable which development of financial products have been affected by all this costs. This hinders innovations in the financial sector and the rate at which the new products are adopted in the market (Lewis & Baker, 2013). Cybercrime related costs have skyrocketed the cost of doing businesses in the financial sector and thus hindering the design of products,

services, or processes, because companies are less willing to turn new ideas into products (Anderson et al, 2013).

Crime wave' is an understatement when you consider the costs that businesses are suffering as a result of cybercrime. 'Epidemic' is more like it. Three years ago, the Wall Street Journal estimated that the cost of cybercrime in the U.S. was approximately $100 billion. The estimate disputed other reports which pegged the numbers by as much as ten times higher. In 2015, the British insurance company Lloyd's estimated that cyber-attacks cost businesses as much as $400 billion a year, which includes direct damage plus post-attack disruption to the normal course of business (Lewis & Baker, 2013). Some vendor and media forecasts over the past year put the cybercrime figure as high as $500 billion and more. From 2013 to 2015 the cybercrime costs quadrupled, and it looks like there will be another quadrupling from 2015 to 2019 (Lewis & Baker, 2013). Juniper research recently predicted that the rapid digitization of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015.According to Home Office in their 2001 report on the economic impact of crime in the UK35 define the various types of cost associated with cybercrime (Anderson et al, 2013).

2.3.1 Prevention and detection costs of Cybercrime

In any risky environment any institution and also individuals usually take measures to reduce the amount of loss that they may suffer as a result of a bad situation in this case cyber related crime (Lewis & Baker, 2013). This include individual and organizational security measures (such as installing physical and virtual protection such as antiviral software), insurance costs and costs associated with gaining compliance to required IT standards (for example the Payment Card Industry Data Security Standard, PCI DSS) (Anderson et al, 2013).

Cyber criminals are no different than traditional criminals in that they want to make their money as quickly and easily as possible. Cybercrime prevention can be achieved fairly quickly and in a cost-effective manner. Similar to target hardening for a residence or a business (e.g., lights, locks, and alarms), the more difficult it is for a cyber-criminal to successfully attack a target, the more likely he or she is to leave it alone and move on to an easier target.

Prevention costs are the monetary equivalent of any efforts to avert cybercrime (Lewis & Baker, 2013). They include the cost of keeping computers up to date by implementing an antivirus system. An antivirus system will only work if computers are monitored from time to time deployment, and maintenance of prevention measures, as well as indirect defense costs, such as inconvenience and opportunity costs caused by the prevention measures. The following ten tips are basic ways that cybercrime can be prevented Keep the computer system up to date Cyber criminals will use software flaws to attack computer systems frequently and anonymously. Most Windows-based systems can be configured to download software patches and updates automatically

Defense costs, like indirect losses, are largely independent of individual victims (Anderson et al, 2013).Often it is even difficult to allocate them to individual types of cybercrime. Defenses can target the actual crimes or their supporting infrastructure, and the costs can be incurred in anticipation of or reaction to crimes, the latter being to deter copycats. It is also necessary to consider, as some studies have done, expenditures on cyber security as part of the total cost of cyber espionage and cybercrime. One estimate predicts that governments and companies spend perhaps 7% of their information technology budgets on security. Another estimate put annual spending globally on cyber security software at $60 billion, growing at about 8% a year (Lewis

& Baker, 2013). The US Office of Management and Budget reported that in 2012, federal agencies spent more than $15 billion on cyber security-related projects and activities, accounting for 20% of all federal spending on information technology (Lewis & Baker, 2013). In many research and studies it has been asserted that, “institutions are extremely inefficient at fighting cybercrime; or to put it another way, cyber-crooks are like terrorists or metal thieves in that their activities impose disproportionate costs on society (Anderson et al, 2013).

Companies will always have to spend on cyber security, but if we assume that some percentage of the current spending would be unnecessary in a more secure cyber environment, that additional spending counts as part of the total cost (Lewis & Baker, 2013). Determining this “risk premium” for malicious cyber actions faces all the estimation problems in other categories of loss, but one initial reference point would be that companies spent almost a $1 billion in 2012 to insure against the risk of social media attacks, privacy breaches, cybercrime and cyber espionage. This relatively low figure may reflect imperfection in the insurance market as much as company perceptions of cyber risk (Anderson et al, 2013).

While losses due to cybercrime are troubling, they do not directly threaten national security, except to the extent that international cybercrime allows potential opponents to train and maintain proxy forces at others expense (Lewis & Baker, 2013). Direct losses to consumers may be the smallest component of the cost of malicious cyber activity. These are usually based on impersonating individuals to gain access to their financial resources or other forms of fraud, such as impersonating an antivirus company in order to persuade individuals to pay to have their computers cleaned.

2.3.2 Response costs of cyber crime

These takes into account direct losses to individuals and companies (including business continuity and disaster recovery response costs), and indirect losses arising from reduced commercial exploitation of IP and opportunity costs through weakened competitiveness. Consequential cost are those that have affected the banking institution directly (Anderson et al, 2013).

While companies fear reputation damage, there has been little work to quantify it. Companies suffer reduced valuation after public reporting of their being hacked, usually in the form of a drop in stock prices (Lewis & Baker, 2013). These losses can be significant—ranging from 1% to 5%—but appear not to be permanent. Stock prices usually recover by the next quarter. It would distort any calculation of loss to attempt to include these fluctuations in stock prices (Lewis & Baker, 2013).

However, it will be interesting to see if this changes as a result of new SEC regulations that require companies to report major hacking incidents, which may improve shareholder understanding about what hacks are commercially material (Lewis & Baker, 2013). Shareholders are unlikely to have good information about what was taken, let alone by whom and for whose benefit. Recovery of stock prices may not be so quick if investors decide that there has been significant damage to a company's intellectual property portfolio or if it sees a significant outflow of customers as a result (Anderson et al, 2013).

The most important area for loss is in the theft of intellectual property and business-confidential information economic espionage (Lewis & Baker, 2013). It is difficult, however, to precisely estimate the losses. This is in part because cyber spying is not a zero-sum game. Stolen

information is not really gone. Spies can take a company's product plans, its research results, and its customer lists today, and the company will still have them tomorrow. The company may not even know that it no longer has control over that information (Lewis & Baker, 2013). There are many ways to determine the value of intellectual property. One is to estimate what it would fetch on the market if offered for sale or for licensing. Companies can value their intellectual property by determining the income streams it produces and is expected to produce in the future (Anderson et al, 2013).

Companies can also estimate what it would cost to replace intellectual property as a means of estimating its value, although a reliance on inputs for estimating value can be very misleading (Lewis & Baker, 2013). The actual value of intellectual property can be quite different from the research and development costs incurred in creating it (Lewis & Baker, 2013). If a company spends a billion dollars on a product that fails in the market, and a foreign power steals the plans, the loss is not a billion dollars but zero the invention's market value (Anderson et al, 2013).

Service disruptions, such as denial of service attacks, may have only a limited cost on a national economy (although they can be disruptive for the company that experiences them). If the website of an online retailer is taken offline, they will lose sales, but the actual economic effect may be much smaller (Lewis & Baker, 2013). Intellectual property (IP) losses are the most difficult to estimate for the cost of cybercrime, but it is also is the most important variable for determining loss. IP theft shifts trade balances and national employment. Countries where IP creation and IP-intensive industries are important for wealth creation lose more in trade, jobs, and income from cybercrime (Lewis & Baker, 2013). The effect of cyber espionage on national security is

significant, and the monetary value of the military technology taken does not reflect the full cost to victim countries (Anderson et al, 2013). Cybercrime damages innovation. One way to think about the cost from cybercrime is to ask how investors would act if returns on innovation doubled. Companies would invest more and the global rate of innovation would increase. By eroding the returns on intellectual property (IP), cybercrime invisibly creates a disincentive to innovation.

Stealing business confidential information—investment information, exploration data, and sensitive commercial negotiation data—can yield immediate gain (Lewis & Baker, 2013). The damage to individual companies runs into the millions of dollars. One UK Company told British officials that it incurred revenue losses of $1.3 billion through the loss of intellectual property loss and subsequently suffered a disadvantage in its commercial activities (Lewis & Baker, 2013). Hacking of central banks or finance ministries could provide valuable economic information on the direction of markets or interest rates (Anderson et al, 2013).

These costs include the relevant actions that a banking institution has to take to respond to the losses that may have been suffered by other parties such as customers as a result of an attack through the online platforms. These includes costs such as compensation payments to victims of identity theft, regulatory fines from industry bodies and indirect costs associated with legal or forensic issues (Anderson et al, 2013).

The cost of cleaning up after a cyber-attack may be relatively small. One survey by (Lewis & Baker, 2013) found an average of about $9 million for large companies to clean up after a successful breach. Many of those incidents were of the lost-laptop variety, and one might expect the costs of curing actual cyber espionage intrusions to be much higher (Lewis & Baker, 2013).

One area for further research is increased insurance costs, as companies seek to control liability for breaches of their networks (Anderson et al, 2013).

A calculation of the cost of malicious cyber activity would need to consider opportunity costs, forgone opportunities, or lost benefits that would otherwise have been obtainable for activities in cyberspace (Lewis & Baker, 2013). Additional spending on cyber security that would not be required in a more secure environment is one example of an opportunity cost. Other examples include lost sales or lower productivity, a decision to avoid the internet for some activities (Anderson et al, 2013).

A survey cited in the European Commission Cyber security Strategy Document found that almost a third of Europeans are not confident in their ability to use the internet for banking or purchases and avoid revealing personal information because of security concerns (the greatest fear is over identity theft for purposes of financial fraud) (Lewis & Baker, 2013). A 2008 Study commissioned by the European Network and Information Security Agency (ENISA) found "growing public concerns about information security hinder the development of both markets and public services (Lewis & Baker, 2013)." A 2006 global survey taken by the International Telecommunication Union as part of its campaign to play a greater role in cybersecurity, based on 400 respondents, found that at that time, more than 40% of Internet users avoided some online transactions because of security concerns (Lewis & Baker, 2013). None of these figures are determinative, but they suggest that there could be forgone opportunities in the use of the internet for commercial purposes because of security concerns (Anderson et al, 2013).

Cleaning up cybercrime is expensive. The cost to individual companies of recovery from cyber fraud or data breaches is increasing. While criminals will not be able to monetize all the

information they steal, the victim has to spend as if they could use all the stolen data (Lewis & Baker, 2013). The aggregate cost for recovery is greater than the gain to cybercriminals. One study of the cost of cybercrime for Italy found that while the actual losses were only $875 million, the recovery and opportunity costs reached $8.5 billion (Lewis & Baker, 2013). The bill for recovery costs is where the real damage to society begins, and the effect on a business can include damage to brand and other reputational losses and harm to customer relations and retention (Anderson et al, 2013).

2.3.3 Indirect Costs

Indirect loss is the monetary equivalent of the losses and opportunity costs imposed on society by the fact that a certain cybercrime is carried out, no matter whether successful or not and independent of a specific instance of that cybercrime (Lewis & Baker, 2013). Indirect costs generally cannot be attributed to individual victims. That indirect losses is the first category to span both cybercrimes and its supporting infrastructure. The whole idea of distinguishing criminals' profit centers from the common infrastructure being employed in the crimes is to avoid allocating the collateral damage caused by the infrastructure to the actual types of cybercrimes, where they would show up as indirect losses (Lewis & Baker, 2013). Since the means (e.g., botnets) would not be around if there were not ends (e.g., phishing victims), we consider losses caused by the cybercriminal infrastructure as indirect by nature; irrespective of whether or not the legal framework formally criminalizes the means (Anderson et al, 2013).

Example of Indirect losses include: Loss of trust in online banking, leading to reduced revenues from electronic transaction fees, and higher costs for maintaining branch staff and cheques clearing facilities; Missed business opportunity for banks to communicate with their customers

by email; Reduced uptake by citizens of electronic services as a result of lessened trust in online transactions; Efforts to clean-up PCs infected with malware for a spam sending botnet

Direct loss is the monetary equivalent of losses, damage, or other suffering felt by the victim as a consequence of a cybercrime. Example of direct losses include: Money withdrawn from victim accounts; Time and effort to reset account credentials (for banks and consumers); Distress suffered by victims; Secondary costs of overdrawn accounts: deferred purchases, inconvenience of not having access to money when needed; Lost attention and bandwidth caused by spam messages, even if they are not reacted to.

2.3.4 Development of financial products

Technology has altered many aspects of financial transactions. In the area of lending, for instance, information on firms and individuals from a variety of centralized sources such as Dun and Bradstreet is now widely available. The increased availability of reliable timely information has allowed loan officers to cut down on their own monitoring. While, undoubtedly, some soft information that is hard to collect and communicate direct judgments of character, for example is no longer captured when the loan officer ceases to make regular visits to the firm, it may be more than compensated by the sheer volume and timeliness of hard information that is now available. Moreover, because it is hard information past credit record, accounting data, etc. the information can now be automatically processed, eliminating many tedious and costly transactions. Technology has therefore allowed more arm's length finance, and therefore expanded overall access to finance. Such methods undoubtedly increase the productivity of lending, reduce costs, and thus expand access and competition. Petersen and Rajan (2002) find that the distance between lenders and borrowers has increased over time in the United States, and the extent to

which this phenomenon occurs in a region is explained by an increase in the bank loan to bank employee ratio in that region, a crude proxy for the increase in productivity as a result of automation.

2.4 Empirical review

Siddique & Rehman (2011) did a study on the impact of electronic crime in the Indian banking sector. The aim of their study was to establish and also to come up with a conceptual framework of how the criminal activities being conducted online are affecting the banking and financial sector in India. According to their study the main goal of the Indian financial sector is to eliminate all possibilities of electronic crime. This process involves identifying the necessary costs that needs to be incurred to ensure secure transactions. Siddique & Rehman identified that several criminal activities take place through network connections this include activities such as ATM fraud, money laundering and credit card fraud. This study identified one of the fears and costs that the banks anticipate is the fact that these activities may lead to loosing of customer trusts hence losing business as some may opt to other banks.

Another study done by Hannan & Blundell (2004) on the issue relating to electronic crime and how it's not the only concept to be worried about. Their study focused mainly on two case studies, one of the study was to do an analysis of the important and crucial factors affecting the breakdown of electronic criminal activities in Australia. The other part of the study tried to address the costs that are incurred under the legal environment of the banks. The study found out that there are many consequences and costs that banks face from poor implementation of legal requirements and security measures. The study presented a number of options and solutions required in tackling policy strategies for future development.

Raghavan & Parthiban (2014) focused on the effect of cybercrime on bank finances. The main objective of their study was to discuss the problem of cybercrime in the banking sector. The study did an in-depth analysis of criminal activities and scenarios within the networks and identified the actors involved in each scenario. The study also identified and documented the various types of criminal activities that are plaguing the banking sector and the motives behind those who commit such crimes. This study identified that one of the costs emanating from such vice is the financial loss which represents a direct cost and a huge issue globally impeding the development of systems.

According to Moore, Clayton & Anderson (2009) they did a paper on the economics of online crime. According to their study, online criminal activities take place as a result of a number of idle nuisance hackers. The paper identifies that the banking institutions face a lot of problems trying to control their exposure to operational risks arising from network connections. Their study found that there are significant techniques and improvements that are viable in dealing with online fraud. The institutions must willing to incur security costs for this to take full effect and secondly the study suggested that in order to tackle online crime the banks must first understand the economic perspective.

Cybercrime according to Douglas and Loader (2000) can be defined computer mediated activities conducted through global electronic networks which are either illegal or considered illicit by certain parties. In the banking sector, the cybercrimes which are committed using online technologies to illegally remove or transfer money to different account are tagged as banking frauds (Wall, 2001).

The cybercrimes according to Wall (2001) can be categorized into four major categories i.e. cyber deceptions, cyber-pornography, cyber-violence and cyber-trespass. The banking frauds are sub-categorized in cyber-deception which can be defines as an immoral activities including stealing, credit card fraud, and intellectual property violations (Anderson et al., 2012).

There are number of frauds or cybercrimes witnessed in the banking sector, like ATM frauds, Cyber Money Laundering and Credit Card Frauds. However, in general all the frauds are executed with the ultimate goal of gaining access to user's bank account, steal funds and transfer it to some other bank account. In some cases the cyber criminals uses the banking credentials like PIN, password, certificates, etc. to access accounts and steal meager amount of money; whereas in other cases they may want to steal all the money and transfer the funds into mule accounts. Sometimes, the intention of cybercriminals is to just harm the image of the bank and therefore, they block the bank servers so that the clients are unable to access their accounts (Claessens et al., 2002; Hutchinson& Warren, 2003).

As a lot of vulnerabilities exist in the defense system of banking sector, thus there is a need to investigate the ways to increase awareness about the measures that can be undertaken to combat cybercrimes in the banking sector. However, not many studies in the past have been conducted in this area which would suggest ways to mitigate the risks and combat such crimes (Florêncio & Herley, 2011; McCullagh & Caelli, 2005). In order to understand the fraud system in banking sector we will have to understand and describe the attackers and defenders in this environment. The next section therefore describes the different actors which are involved in cybercrimes.

The banking industry across the globe is facing a challenging situation which is thought provoking due to the geopolitical and global macro-economic conditions. The banking sector is

forced to evaluate its current practices in order to analyze and manage their risks effectively. Technology-driven approaches have been adopted for the management of risk. Due to the growth of IT, penetration of mobile networks in everyday life, the financial services have extended to masses. Technology has made sure that banking services reach masses as it made these services affordable and accessible (KPMG, 2011).

However, this has also increased the risk of becoming targets of cyber-attacks. Cybercriminals have developed advanced techniques to not only cause theft of finances and finances information but also to espionage businesses and access important business information which indirect impacts the banks finances. Globally, USD 114 Billion is lost nearly every year due to cybercrimes, and the cost spend to combat cybercrimes is double is amount i.e. USD 274 billion (Symantec Cyber Crime Report, 2012).

On an average, banking facilities take 10 days to fully recover from a cyber-act which further adds to the cost of operation. Comparing the financial losses faced by the Indian Banking Sector, it is nearly 3.5% of the loss in cash in comparison to global loss. USD 4 billion is lost in recovering from the crime and USD 3.6 billion is spent to combat such crimes from happening in future. The average time taken to resolve the crime in Indian banking sector is also higher in comparison to global scenario i.e. 15 days (Muthukumaran B., 2008) In order to fight these cybercrimes, the banking sector needs to collaborate with global authorities and watchdog organizations so that a model can be developed which can help in controlling and dealing with such threats. The main issue of concern here is that there is absence of effective compilation service in the banking sector which can identify the trends in cyber-crime and compile a model

according to it. However, in the last few months, banks all across the globe have perceived cybercrime as among their top five risks (Stafford, 2013).

In conclusion most systems are one-step behind the tools adopted by cyber criminals which has resulted in demand of development of system which is flexible is meeting and destroying the incoming assaults. A solid defense system to resolve attack is the need of the hour before, during and after the attack.

2.5 Critique of existing literature

The research in this area that is cybercrime costs should lead to the identification of significant and important costs elements that should be considered and arranged in order of importance when it comes to tackling criminal activities taking place through online network platforms. The research is based on a solid rationale and hypothesis and is supported by strong empirical findings and analysis. There are one or two negligible weaknesses related to the definition of each cost factor, but this will be addressed by proper operationalization of each variable.

From literature review we see a lot of studies talking about the impact of cyber-crime or white collar criminal activities on bank performance or on performance of financial institutions. For example Siddique & Rehman (2011) in there study on the impact of electronic crime in the Indian banking sector. The aim of their study was to establish and also to come up with a conceptual framework of how the criminal activities being conducted online are affecting the banking and financial sector in India. According to their study the main goal of the Indian financial sector is to eliminate all possibilities of electronic crime. This process involves identifying the necessary costs that needs to be incurred to ensure secure transactions. Siddique & Rehman identified that several criminal activities take place through network connections this

include activities such as ATM fraud, money laundering and credit card fraud. Another study is by Hannan & Blundell (2004) on the issue relating to electronic crime and how it's not the only concept to be worried about. Their study focused mainly on two case studies, one of the study was to do an analysis of the important and crucial factors affecting the breakdown of electronic criminal activities in Australia.

Most of this studies concentrate on the overall effect of this new upcoming vice on the general performance of financial institutions, none is has concentrated on specific cost elements and how they are directly affecting banking in most countries.

Other studies have over the years only concentrated on once costs element which is the direct financial loss that is attributed to cyber-crime, whereas there are many other costs elements although not directly linked to financial loss that have had a great impact on performance of banks. For example cybercriminals have developed advanced techniques to not only cause theft of finances and finances information but also to espionage businesses and access important business information which indirect impacts the banks finances. Globally, USD 114 Billion is lost nearly every year due to cybercrimes, and the cost spend to combat cybercrimes is double is amount i.e. USD 274 billion (Symantec Cyber Crime Report, 2012). While companies fear reputation damage, there has been little work to quantify it. Companies suffer reduced valuation after public reporting of their being hacked, usually in the form of a drop in stock prices (Lewis & Baker, 2013). These losses can be significant—ranging from 1% to 5%—but appear not to be permanent. Stock prices usually recover by the next quarter. It would distort any calculation of loss to attempt to include these fluctuations in stock prices (Lewis & Baker, 2013).

2.6 Research gap

From the empirical review the studies done by Raghavan & Parthiban (2014 it is quite evident that their studies deal with the impact of cyber-crime on banks in general. The studies don't break down what costs banks have to consider and incur pre and post cyber-attacks and whether this costs have reached a point where banks have to reconsider the rate at which they are developing and adopting financially innovated products and services. Therefore the study identifies and research gap by trying to establish the types, impact and mitigations of cybercrime related costs in the development of financial products in Kenyan Banks.

2.7 Summary

The concept of Electronic Crime is a vital aspect. Since new information is available in an unbiased manner it is often not possible to detect crime on the basis of that information. Researchers make an attempt to study the Electronic crimes and major crimes of banking sectors. In the present globalized scenario, Information Technology is the factor responsible of further growth and development in the banking sector. Despite all these there are other factors that are very important and have to be considered this include direct and indirect costs of cyber-crime and what role they play in this ever changing and evolving information technology platform.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter introduces the research methodology including the research design, population of study, sampling methodology, and the data collection and analysis procedures. The study

adopted a quantitative approach. Data analysis was done by means of standardized statistical procedures. Questionnaires were used to capture quantitative data from banking agencies under consideration.

Research methodology refers to the steps or sequence of events needed to plan what data is to be analyzed. It provides a frame work of how the study is to be carried out (Stevens & Clow, 2008). Mathooko (2011) state that research methodology includes the research designs, data collection procedures and data analysis were applied in carrying out the research study. Research methodology helped in defining the research design to be used which then determined the data collection procedures and analysis employed. Research methodology is a way to systematically solve the research problem. It may be understood as a science of studying how research is done scientifically. In it, various steps are studied that are generally adopted by a researcher in studying the research problem along with the logic behind them.

3.2 Research Design

A research design is a plan showing how the problem under investigation will be solved. According to Cooper & Schindler (2003) a research design is a framework for specifying the relationship among the study's variables and outline procedures for every research activity ranging from sampling procedures to data collection to analysis and presentation of findings. Descriptive research design was adopted in the study since it helped in achievement of measurable findings. Descriptive research involves gathering data that describe events and then organizes, tabulates, depicts, and describes the data collection. The method was preferred because it allowed for an in-depth study of the subject in a quantitative aspect of the overall research. Descriptive research design aims to gather data without any manipulation of the

research context, focusing on individual subjects and going into depth and detail in describing them. In the study the variables were analyzed further by use of the named research design.

3.3 Population

A population is a complete set of individuals with the same common observable characteristics Mugenda and Mugenda (2010). Target population is the portion of the total population from which the study draws its respondent components. The study targeted the NIC bank of Kenya as its main case study. This was based on the purposive population selection technique since the study was more interested in extreme cases of bank fraud that provides the purest most clear-cut instance of the phenomena the researcher is interested in. NIC Bank had over 24 branches in Kenya. The respondents of this research proposal were employees in NIC bank in Kenya drawn from the 24 branches. There are 957 employees 167 of whom are support staff. (Source; www.nic-bank.com).

3.4 Sampling frame

A sample is a smaller group or sub-group obtained from the accessible population (Mugenda and Mugenda, 1999). This subgroup is carefully selected so as to be representative of the whole population with the relevant characteristics. Each member or case in the sample is referred to as subject, respondent or interviewees. Sampling is the process of selecting a number of individuals for a study (Kothari, 2004).

A sampling frame is a comprehensive list of all sampling units, which a sample can be selected. According to (Mugenda & Mugenda, 2003), a sample size of more than10% is a good representation for the descriptive survey in a relatively large population. Therefore, 80 participants were selected randomly from the employees to respond to the questionnaire.

3.5 Sampling design

The study employed purposive sampling technique in selecting the respondents in each bank branch. With this sampling technique, only case objects that contain information required by the researcher are selected (Palys, 2008). The respondents were the bank employees involved in implementation and overseeing and offering of the online banking services, policies and activities.

3.6 Data collection Instruments

The main data collection instruments used in this study include was the questionnaire. This was used for the purpose of collecting primary quantitative data. Primary data was observed and collected directly from first-hand experience (Davies, 2002). The questionnaire comprised of open ended question to allow ease in data analysis, interpretation and tabulation of the questionnaire. The questionnaire was divided into the main areas of investigation except the first part which captured the demographic characteristics of the respondents. Other sections were organized according to the major research objectives.

3.7 Data collection procedure

Prior to the commencement of data collection, the researcher obtained all the necessary documents, including an introduction letter to the bank. Audience with the NIC branch managers in Kenya was also sought to clarify the purpose of the study. Upon getting clearance, the researcher in person distributed the questionnaires to the sampled employees. Use of questionnaires was expected to ease the process of data collection as all the selected respondents were to be reached in time. During the distribution of the instruments, the purpose of the research was explained.

3.8 Reliability and Validity of Data

The reliability was ensured by testing the instruments for the reliability of values (Alpha values) as recommended by Cronbatch, (1946). Cronbach's recommends analysis for Alpha values for each variable under study. According to Sekaran (2001) Alpha values for each variable under study should not be less than 0.7 for the statements in the Instruments to be deemed reliable. Consequently, all the statements under each variable were subjected to this test and proved to be above 0.7. A measure is reliable when it is error free and consistent across time and across various items in the instrument. A test questionnaire was administered to 10 employees. According to Mugenda and Mugenda (2003) subjects in the actual sample should not be used in the pilot study. The pilot study was used for checking the validity of the questionnaire. The validity of the data collection instruments was done with the help of an Expert (the Researcher's Supervisor) to edit the questionnaire.

3.9 Pilot Test

Pilot test otherwise known as pre-testing is conducted to detect weakness in the design, data collection instruments and procedures that will be used to carry out the study. As argued by Mugenda and Mugenda (2003), pre-testing of tools helps the researcher assess the efficiency and clarity of the instruments and their uses. Cooper Donald & Schilnder, (2003) further explain that pre-testing allows errors to be identified and acts as a tool for training the research team prior to the actual data collection time. This study pre-tested the questionnaire on at least 10% that is 10 employees of the targeted population which was 957 as is in line with Kothari (2004). He suggests that for a sample size between $0< n< 100$, pre-testing 10% of the questionnaires is ideal to serve validity and reliability purposes of the data collection tool.

3.10 Data processing and Analysis

The completed questionnaires was edited for completeness and consistency. The data was then coded to enable the responses to be grouped into various categories. Data collected was purely quantitative and it was analyzed by descriptive analysis methods such as measure of central tendency e.g. mean, mode, median and measure of dispersion such as standard deviation, ration as well as percentages. The descriptive statistical tools assisted in describing the data and determining the extent to be used. Data analysis also used SPSS to generate quantitative reports. The researcher then presented the analyzed data through tables, pie charts, and graphs.

3.10.1 Regression analysis

$(Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_3 X_3 + \varepsilon)$ becomes:

Where, is Y the dependent variable (Development of financial products), X_1 is the prevention and detection cost, X_2 is the response cost and X_3 is the indirect costs

3.10.2 ANOVA analysis

The researcher conducted ANOVA analysis to test the validity and the goodness of fit of the above regression model in measuring the predictive nature of the dependent variables on the dependent variables.

CHAPTER FOUR

DATA ANALYSIS AND DISCUSSION

4.1 Introduction

This chapter presents the research findings and results of the study. Data analysis was conducted

for each of the specific objective. Descriptive statistical analysis was used to identify frequencies and percentages to answer all of the questions in the questionnaire.

4.2 Response Rate

In this study a total of 80 questionnaires were distributed, a total of 80 questionnaires were returned representing a response rate of 100%. According to Mugenda and Mugenda (2003), a 50% response rate is appropriate for analysis.

4.3 Reliability Analysis

Cronbach's Alpha was used to test reliability of the proposed constructs. The research findings indicated that Prevention and detection costs had a coefficient of 0.840, Response rate costs had a coefficient of 0.821, indirect costs had a coefficient of 0.886 and Development of financial products had a coefficient of 0.852. According to Mugenda and Mugenda (2003) a coefficient of 0.70 or more implies high degree of reliability of the data. Therefore all the factors showed that the Cronbach's Alpha are above the required coefficient of 0.70 thus the results of the study are highly reliable as indicated in Table 4.1.

Table 4.1: Reliability Tests of the factors.

Factors	Reliability Cronbach's Alpha	Comments
Prevention and detection costs	0.840	Accepted
Response rate costs	0.821	Accepted
Indirect costs	0.886	Accepted
Development of financial products	0.852	Accepted

4.4 Distribution of Demographic Characteristics of the respondents

4.4.1 Demographic Characteristics of the respondents

According to study findings in Table 4.1; majority of the 55% were females while 45% were males; majority of respondents 55% had 36 to 50 years; 35% of the respondents had 25 to 35

years while 10% had below 25 years. 40% of respondents were never married, 40% were married while 20% were divorced. Majority of the respondents 60% had attained the 1st degree, 30% of the respondents had masters holders while 10% had attained PHD.

Table 4.2: Demographic Characteristics of the respondents

Gender	Frequency	Percent
Male	36	45
Female	44	55
Total	80	100
Age of the respondents		
Below 25	8	10
25 to 35	28	35
36 to 50	44	55
Total	80	100
Marital status		
Married	32	40
Divorced	16	20
Never married	32	40
Total	80	100
Level of education		
1st Degree	48	60
Masters	24	30
PHD	8	10
Total	80	100.0

The implementation of innovated banking services in the banking sector needs the experienced people. This study indicated that majority of the respondents had experience in the banking sector, and most were well educated hence provided reliable information. .

4.4.2 Distribution of average income per month and response on Computerization of operations

According to study findings in Table 4.3, majority of the respondents 60% were paid 50001 to 150000, 35% were paid 150001 to 300000 while 5% were paid less than 50000.All respondents 100% indicated their operations have been computerized.

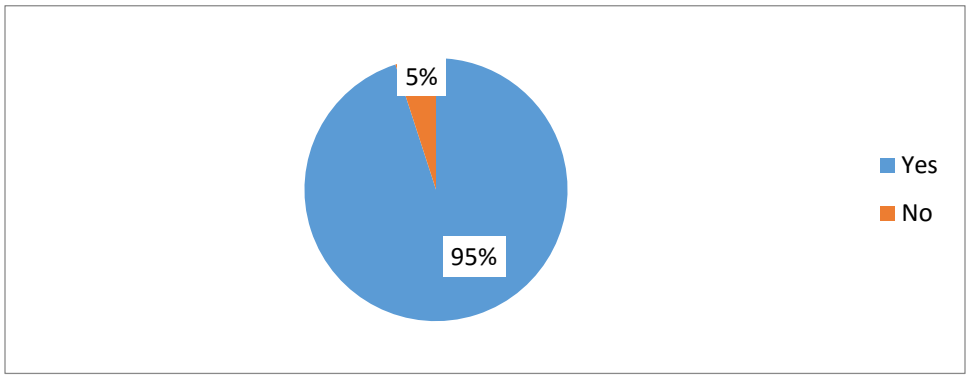
Table 4.3: Distribution of average income per month and response on Computerization of operations

Average income per month	Frequency	Percent
Below 50000	4	5.0
50001-150000	48	60.0
150001-300000	28	35.0
Total	80	100.0
Computerization of operations		
Yes	80	100

4.4.3 Response on presence of e-banking services

From the study findings in Figure 4.1, majority of the respondents 95% indicated they have e-banking services while 55 indicated they do not have e-banking services. This finding is in line with most studies that are recognizing the presence and importance of e-banking services in the developed and mostly in developing countries (Nyangosi, Arora, and Singh, 2009).

Figure 4.1: Response on presence of e-banking services

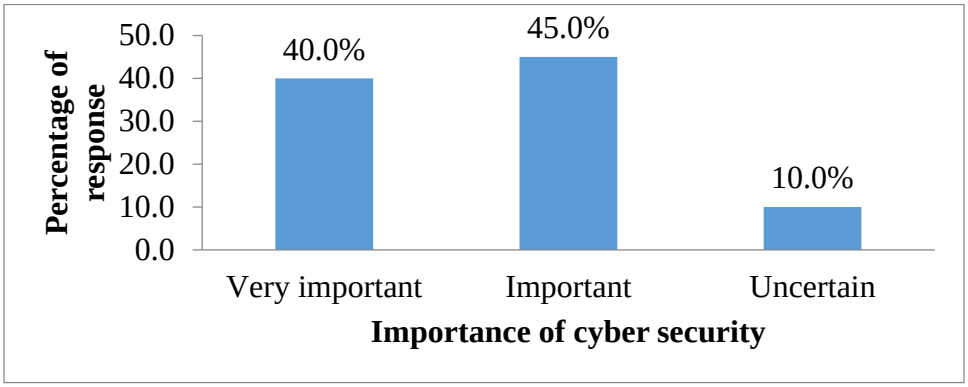


4.4.4 Response of importance of cyber security with reference to e-banking services

According to study findings in Figure 4.2, majority of the respondents 45.0% indicated that cyber security is important with reference to their e-banking services, 40% of the respondents

indicated that cyber security is very important while 10% indicated they were uncertain. The researcher tried to pinpoint how cyber security is becoming a major concern within the financial sector, this notion was supported by the study where the majority highlighted cyber security as major issue this was also in line with findings of Fatima (2015) where pinpointed cyber security as a concern whose solution should be sought out.

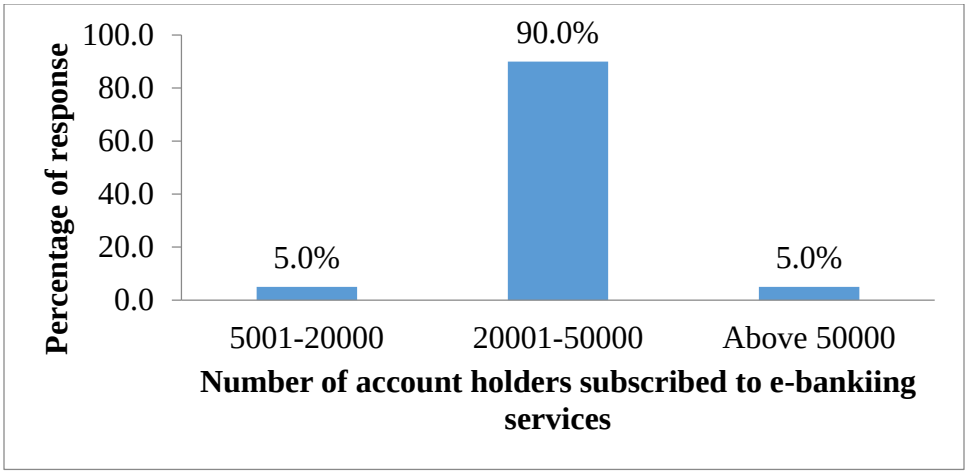
Figure 4.2: Response of importance of cyber security with reference to e-banking services



4.4.5 Response on number of account holders subscribed to e-banking services

According to study findings in Figure 4.3, majority of respondents 90% indicated about 20001 to 50000 of the respondents have subscribed to e-banking services, an equal 5% indicated 50001 to 20000 and above 50000 had subscribed to e-banking services. The researcher here tried to show how much e-banking is becoming popular among customers which was indicated by the percentage of uptake and usage of both online and e-banking services.

Figure 4.3: Response on number of account holders subscribed to e-banking services



4.5 Factors affecting the development of financial products

4.5.1 Impact of prevention and detection cost on development of financial products

According to study findings in Table 4.4, in average the respondents agreed that the insurance cost of protecting against cyber related criminal activities affecting the bank innovative activities are too high, thereby affecting how banks are using new products and services as shown by a mean of 3.70 and standard deviation of 0.560, in average the respondents agreed that the there are many fees and charges required to meet IT compliance standards that a bank must comply to when operating on online platforms as shown by a mean of 3.90 and standard deviation of 0.542, the respondents agreed that it is an expensive venture to identify and assign specific responsibilities by job function for detecting and reporting suspected unauthorized activity.as shown by a mean of 3.90 and standard deviation of 0.628, the respondents agreed that the bank has different insurance accounts set aside to protect customers against losses that may arise from attacks on newly innovate financial products and services as shown by a mean of 3.55 and standard deviation of 0.926, the respondents further agreed that the banks have in place a framework for monitoring the firm's network environment to detect potential cyber security events as shown by a mean of 3.58 and standard deviation of 0.678. This finding was in line with the argument of Lewis and Becker who asserted that Companies will always have to spend on cyber security, but if we assume that some percentage of the current spending would be unnecessary in a more secure cyber environment, that additional spending counts as part of the total cost (Lewis & Baker, 2013).

Table 4.4: Responses on prevention and detection cost; (Insurance fees, IT compliance costs)

Response	N	Minimum	Maximum	Mean	Std. Deviation
The insurance cost of protecting against cyber related criminal activities affecting the bank innovative activities are too high, thereby affecting how banks are using new products and services	802	4		3.70	.560
There are many fees and charges required to meet IT compliance standards that a bank must comply to when operating on online platforms	802	5		3.90	0.542
It is an expensive venture to identify and assign specific responsibilities by job function for detecting and reporting suspected unauthorized activity.	802	5		3.90	0.628
The bank has different insurance accounts set aside to protect customers against losses that may arise from attacks on newly innovate financial products and services	802	5		3.55	0.926
The banks have in place a framework for monitoring the firm's network environment to detect potential cyber security events.	762	4		3.58	0.678

4.5.3 Impact of response cost on development of financial products

According to study findings in Table 4.6, in average the respondents agreed that banks are required to compensate victims of identity theft whose information has been hacked; these increases the banks costs hence regulating the adoption rate of some of products, services and processes being innovated as shown by a mean of 3.75 and standard deviation of 0.703, in

average the respondents agreed that there are numerous regulatory fines that are associated with lack of compliance to some of the standards issued by the banking oversight committee which affects the rate at which banks adopt innovated products, services and processes as shown by a mean of 3.60 and standard deviation of 0.739.

On average the respondents agreed that banks fear the costs that they may incur from legal suits directed towards them by affected parties of cyber-attacks, hence cautious on the adoption of new products and services as shown by a mean of 3.65 and standard deviation of 0.797, respondents agreed that legal forensic issues associated with cyber-criminal activities may lead to the closure of the entire business, therefore banks are cautious on what to adopt in terms of newly innovated banking products and services as shown by a mean of 3.55 and standard deviation of 0.810, further the respondents agreed that legal and court cases from cyber-attacks take long time to end hence they tend to interfere with daily operations of a bank affecting the bank's profitability, banks therefore prefer well established and secure products and services as shown by a mean of 3.60 and standard deviation of 0.866. This findings indicated that banks fear the consequence of dealing with a cyber-attacks supported by (Anderson et al, 2013). This was an indication that issues such as recovery of stock prices may not be so quick if investors decide that there has been significant damage to a company's intellectual property portfolio. Despite this assertion and finding, Lewis and Baker (2013) were opposed to this findings claiming that the cost of cleaning up after a cyber-attack may be relatively small.

Table 4.6: Response cost to cyber-crime; (Compensation payments, regulatory fines, legal costs)

	N	Minimum	Maximum	Mean	Std. Deviation
Banks are required to compensate victims of identity theft whose information has been hacked; these increases the banks costs hence regulating the adoption rate of some of products, services and processes being innovated.	802	5		3.75	.703

There are numerous regulatory fines that are associated with lack of compliance to some of the standards issued by the banking oversight committee which affects the rate at which banks adopt innovated products, services and processes.	802	4	3.60	.739
Banks fear the costs that they may incur from legal suits directed towards them by affected parties of cyber-attacks, hence cautious on the adoption of new products and services.	802	5	3.65	.797
Legal forensic issues associated with cyber-criminal activities may lead to the closure of the entire business, therefore banks are cautious on what to adopt in terms of newly innovated banking products and services	802	5	3.55	.810
Legal and court cases from cyber-attacks take long time to end hence they tend to interfere with daily operations of a bank affecting the bank's profitability, banks therefore prefer well established and secure products and services	802	5	3.60	.866

4.5.4 Indirect costs impact on development of financial products

According to study findings in Table 4.6, in average the respondents agreed that Continues successive cyber-attacks on a bank tend to damage how customers view it, in return affecting the overall business as shown by a mean of 3.75 and standard deviation of 0.540, the respondents agreed that cyber transactions, online services, new products and processes constitute a large proportion of a banks research and development costs as shown by a mean of 3.70 and standard deviation of 0.719.

The respondents agreed that loss in confidence of cyber transactions, online services, new

products and process by customers and businesses translates in indirect losses from R&D, therefore banks are regulation what new financial innovations to adopt and the rate of adoption as shown by a mean of 3.90 and standard deviation of 0.704, the respondents were neutral whether legal and court cases from cyber-attacks take long time to end hence they tend to interfere with daily operations of a bank affecting the bank's profitability, banks therefore prefer well established and secure products and services as shown by a mean of 3.40 and standard deviation of 1.026, the respondents further agreed that there is a high chance that reputational damage and loss of confidence would lead to reduction in share price, which may be particularly acute as shown by a mean of 3.80 and standard deviation of 0.877. The researcher sought to examine secondary costs that banks incur as a result of cyber-crime, the study observed that indirect costs had a great impact on bank operations as also observed by (Hannan & Blundell, 2004). This finding is also backed by (Anderson et al, 2013) who claimed that loss of trust in online banking as a result of cyber-attacks led to massive loss revenue.

Table 4.7: Responses on indirect costs (Reputational damage, loss of confidence by customers, loss of share value)

Responses	N	Minimum	Maximum	Mean	Std. Deviation
Continues successive cyber-attacks on a bank tend to damage how customers view it, in return affecting the overall business.	803	5		3.75	0.540
Cyber transactions, online services, new products and processes constitute a large proportion of a banks research and development costs.	803	5		3.70	0.719
Loss in confidence of cyber transactions, online services, new products and process by customers and businesses translates in indirect losses from R&D, therefore banks are regulation what new financial innovations to adopt and the rate of adoption.	803	5		3.90	0.704

Legal and court cases from cyber-attacks take long time to end hence they tend to interfere with daily operations of a bank affecting the bank's profitability, banks therefore prefer well established and secure products and services	802	5	3.40	1.026
There is a high chance that reputational damage and loss of confidence would lead to reduction in share price, which may be particularly acute	802	5	3.80	0.877

4.5.4 Development of financial products

The respondents were neutral on whether the bank general opinion is that these costs are 'business-as-usual' costs that would have been incurred anyway, therefore they don't impact development and adoption of new products and services as shown by a mean of 3.35 and standard deviation of 1.159, the respondents were neutral on whether there reduced profitability as a result of high costs of protection against attacks has resulted to less adoption of innovated services and products by the bank.as shown by a mean of 3.15 and standard deviation of 1.202, the respondents agreed that disaster recovery processes from an immediate attack usually affect the daily operations and continuance of normal business operations; hence there is a reduction in the rate at which banks are adopting new innovations as shown by a mean of 3.75 and standard deviation of 0.948. The respondents agreed that banks main business is from consumers therefore to safe guard their reputation they tend to avoid adoption of new products and services considered vulnerable and risky as shown by a mean of 3.65 and standard deviation of 0.915. The respondents showed a lot of concern in relation to innovative ideas of money and banking transactions some of which revolved around secure trading practices but despite their worries the study categorized these costs and part of operations and that the benefit outweigh the costs as also supported by (Petersen and Rajan, 2002)

Table 4.8: Development of financial products

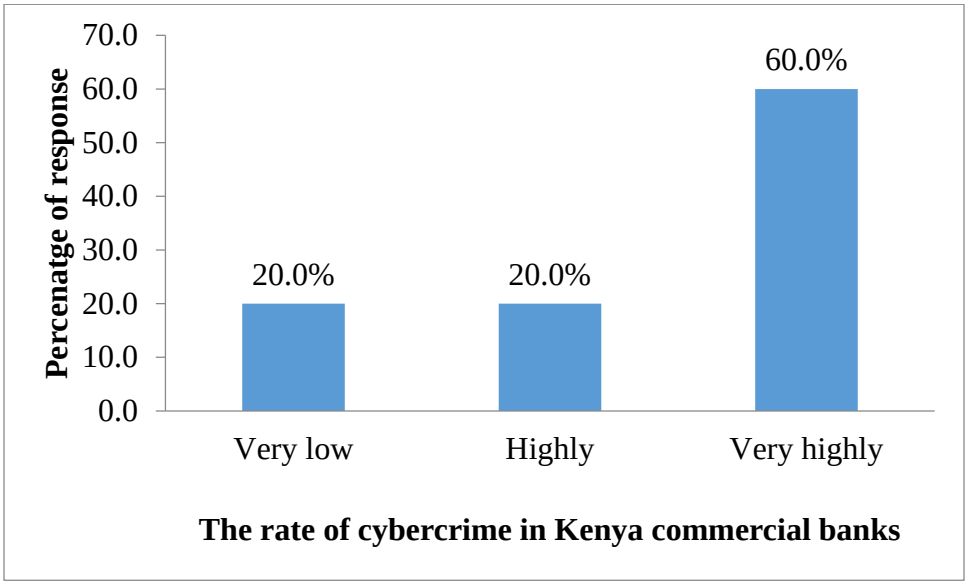
Responses	**N**	**Minimum**	**Maximum**	**Mean**	**Std. Deviation**

The bank general opinion is that these costs are 'business-as-usual' costs that would have been incurred anyway, therefore they don't impact development and adoption of new products and services	802	5	3.35	1.159
Reduced profitability as a result of high costs of protection against attacks has resulted to less adoption of innovated services and products by the bank.	802	5	3.15	1.202
Disaster recovery processes from an immediate attack usually affect the daily operations and continuance of normal business operations; hence there is a reduction in the rate at which banks are adopting new innovations.	802	5	3.75	.948
Banks main business is from consumers therefore to safe guard their reputation they tend to avoid adoption of new products and services considered vulnerable and risky.	802	5	3.65	0.915

4.5.5 Response on rate of cybercrime among Kenya commercial banks

According to study findings in Figure 4.4, majority of the respondents 60% indicated that they are very highly concerned by the rate of cybercrime in Kenya commercial banks, 20% of the respondents indicated they were highly concerned by the rate of cybercrime in Kenya commercial banks while 20% indicated that they lowly concerned.

Figure 4.4: Response on rate of cybercrime among Kenya commercial banks



4.5 Regression analysis

The researcher conducted regression analysis to determine statistical significance between the independent variables (Indirect costs, Prevention and detection costs, and Response rates) and dependent variable Implementation of strategic plan.

Table 4.9: Model summary

Model	R	R Square	Adjusted R Square
1	.864	.747	.733

R-square is the Coefficient of determination that explains the extent to which changes in the dependent variable can be explained by the change in the independent variables or the percentage

of variation in the dependent variable (Development of financial products) that is explained by all the three independent variables (Indirect costs, Prevention and detection costs and Response rates). From Table 4.9, the value of Adjusted R-Square is 0.733. This implies that, 73.3% of variation of Development of financial products independents. From the findings, there is remaining 24.9% which implies that there are factors not studied in this study that affects Development of financial products.

Table 4.10: ANOVA table

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	38.420	4	9.605	55.286	.000
	Residual	13.030	75	.174		
	Total	51.450	79			

a. Dependent Variable: Development

b. Predictors: (Constant), Indirect costs, Prevention and detection cost , Response rates costs

The ANOVA test is used to determine whether the model is important in predicting the Development of financial products. At 0.05 level of significance the ANOVA test indicated that in this model the independent variables namely; Indirect costs, prevention and detection costs and Response rates are important in predicting Development of financial products as indicated by significance value=0.001 which is less than 0.05 level of significance (P-value=0.001<0.05).

Table 4.11: Coefficient of Multiple determinations of the variables

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.538	.584		4.347	.000

Prevention, detection cost	and-	-.105	.132	.048	.796	.429
Response rates costs		-.533	.114	.315	4.657	.010
Indirect costs		-.752	.129	.412	5.813	.023

a. Dependent Variable: Development of financial products

From the findings in table 4.11 above, at 5% level of significance, prevention and detection costs was not a significant predictor of Development of financial products where (P-value=0.429<0.05). Response rates costs was a significant predictor of Development of financial products where (P-value=0.010<0.05). Indirect costs was a significant predictor of Development of financial products where (0.291<0.05).

Where, is Y the dependent variable (Development of financial products), X_1 is the prevention and detection cost, X_2 is the response cost and X_3 is the indirect costs

As per the SPSS generated regression Table 4.11 the equation

$(Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_3 X_3 + \varepsilon)$ becomes:

$Y=2.538-0.105X_1-0.533X_2-0.752X_3$

According to the equation taking all factors constant; the Development of financial products was 2.538. A unit increase of prevention and detection cost would lead to a 0.105 decrease in Development of financial products; a unit increase in Response rates costs leads to 0.533 decrease in Development of financial products. A unit increase in indirect costs leads to 0.752 decrease in Development of financial products. Therefore according to the study findings Indirect costs contributes more to decrease in Development of financial products.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECCOMENDATION

5.1 Introduction

This chapter presents the summery of key data findings, conclusion drawn from the findings highlighted and recommendation made there-to, the conclusions and recommendations drawn were focused on addressing the objective of the study. The researcher intended to determine whether the independent variables (prevention and detection cost, response cost and indirect costs) have an impact on development of financial products.

5.2 Summary of finding

5.2.1 Prevention and detection cost

The study established that prevention and detection cost is one of the major considerations when it comes to development of financial products but not a significant factor as indicated by the p-value. In any risky environment any institution and also individuals usually take measures. To reduce the amount of loss that they may suffer as a result of a bad situation in this case cyber related crime. The study observed that many banks consider the risk that they may face when developing financial products. As observed there was a significant chance of reduction in financial product development as a result of a unit increase in anticipation cost. The bank may feel at risk and exposed to insecurity and uncertainty that makes them anxious about adopting new technologies. They include direct defense costs, i.e., the cost of development, deployment, and maintenance of prevention measures, as well as indirect defense costs, such as inconvenience and opportunity costs caused by the prevention measures. Defense costs, like indirect losses, are largely independent of individual victims and highly influence banking operations in general.

5.2.2 Costs in response to cyber-crime

The study established Response rates costs was a significant predictor of Development of financial products as indicated by the p-value. The study showed that there was a high percentage chance of decrease in development of financial products as a result of increase in response costs. Banks consider a lot of factors when it comes to offering highly innovated services and products that customers need. These costs include the relevant actions that a banking institution has to take to respond to the losses that may have been suffered by other parties such as customers as a result of an attack through the online platforms. As observed by other researchers most of these costs includes costs such as compensation payments to victims of identity theft, regulatory fines from industry bodies and indirect costs associated with legal or forensic issues. The findings of these study, although were in contradiction with other studies who stated that the cost of cleaning up after a cyber-attack may be relatively small.

5.2.3 Indirect costs associated with cyber-crime

Finally the study analysed the impact of indirect costs associated with cybercrime and their impact on development of financial products in banks today. The analysis found out that these variable had the largest significant influence on the dependent variable with a large percentage chance of decrease in development of financial products as a result of perceived increase in indirect costs. Indirect loss is the monetary equivalent of the losses and opportunity costs imposed on society by the fact that cybercrime is carried out, no matter whether successful or not and independent of a specific instance of that cybercrime. The findings are supported by studies who observed that since the means would not be around if there were not ends, we consider losses caused by the cybercriminal infrastructure as indirect by nature; irrespective of whether or not the legal framework formally criminalizes the means.

5.2.4 Development of financial products

The study finally analyzed opinions relating to development of financial products and how it is affected the stated costs. Part of the respondents views were that the costs stated above that is the prevention and detection cost, perceived response cost and indirect cost were costs incurred by businesses on normal daily circumstances and that they have not significant impact on the development of financial products and other novel technologies. For example the respondents

were neutral on whether there was reduced profitability as a result of high costs of protection against attacks has resulted to less adoption of innovated services and products by the bank. The rest of the respondents were in support of some of the findings of the study that these costs play a major significant role in determining daily business operations and more so the development of financial products for example the respondents agreed that disaster recovery processes from an immediate attack usually affect the daily operations and continuance of normal business operations; hence there is a reduction in the rate at which banks are adopting new innovations.

5.3 Conclusion

The study revealed that all the independent variables (prevention and detection cost, response cost and indirect cost) had a negative impact on the dependent variable (development of financial products). It is evident that the adoption of new technologies and innovated services and products have had an impact both positive and negative on operations of banks today. On the positive side they have helped improved service delivery to customers and hence improving the bottom line of the banks. But it is also quite evident and significant that these new trend shave had a huge negative impact on banking operations such the common increasing vice of white collar crime and more so cyber space criminal activities. Therefore these study sought to examine the influence of costs related to adoption of these new trends and novel technologies. The study analyzed and observed that prevention and detection costs such as insurance fees and IT compliance costs have an influence on development of banking products but were not significant. The other costs, direct costs, such as cost of business continuity direct financial loss, compensation payments, legal costs and indirect costs such as reputational damage and loss of confidence by customers were huge concerns and very significant influencers of development of innovated banking financial products and services.

5.4 Study recommendations

Crime wave' is an understatement when you consider the costs that businesses are suffering as a result of cybercrime. Therefore based on the study findings, the study recommends that developed banking products and services are becoming quite popular in the market and also very significant to all consumers, therefore banking service providers should consider providing novel technologies that are costs effective on the consumer and also on the bank operations.

5.4.1 Prevention and detection cost

Crime is inevitable given the nature of the current environment that banks operate in today. Despite the fact that one cannot predict when crime will take place the study has observed that prevention and detection cost are quite significant in determining the operations of the business/banks. The researcher therefore recommends that banks adopt more cost effective measures and more stable technologies that don't provide loopholes for criminal activity to take place. As banks are investing large amounts in the development of this products there should also invest more in prevention and detection strategies.

5.4.2 Costs in response to cyber-crime

The study observed that the aftermath of a cyber-attack is characterized by a number of stake holders being affected not just the bank. The study recommends that banks should enter into agreements with other financial institutions that provide insurance cover to provide insulation over some of the costs that banks face in order to prevent reduction of operations hence resulting loss of revenue.

5.2.3 Indirect costs associated with cyber-crime

One of the studies observed that these costs are normal part of doing business hence don't affect operations that much. But despite these assertion the findings of these research observed that indirect costs are much more significant than the other costs. Therefore the researcher recommends that banks should seek legal recourse and government support in formulating policies that determine what is termed as cyber-crime and what penalties should be imposed on culprits.

5.2.4 Development of financial products

The study recommends that the benefits of developed financial products are much more hence banks should engage in innovation to match competition in the industry but at the same time adopt cost effective strategies to tackle the issues that may arise as a result of use of these products.

5.5 Areas for Further Research

The study sough to determine the impact of prevention and detection cost, response costs and indirect costs on the development of financial products in Kenyan banks. part of the findings were inconclusive as they were opposed to most of the previous literature and therefore the researcher recommends that further research should be done to establish the exact influence of cybercrime related cost on development of financial products.

REFERENCES

Agboola, A. (2007). Information and communication technology (ICT) in banking operations in Nigeria–An evaluation of recent experiences. *African Journal of Public Administration and Management*, *18*(1), 1-102.

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 Berlin Heidelberg.

Avgerou, C. (2003, May). The link between ICT and economic growth in the discourse of development. In *Proceedings of the International Federation of Information Processing, IFIP* (Vol. 9, pp. 373-386).

Bell, R. E. (2002). The prosecution of computer crime. *Journal of financial crime*, *9*(4), 308-325.

Claessens, J., Dem, V., De Cock, D., Preneel, B., &Vandewalle, J. 2002. On the security of today's online electronic banking systems. Computers &Security, 213: 253-265.

Douglas, T., & Loader, B. D. 2000. Cybercrime: Security and surveillance in the information age: Routledge.

Florêncio, D., & Herley, C. 2011. Where Do All The Attacks Go? Economics of Information Security and Privacy III pp. 13-33. Springer New York.

Goodman, R. (1997). The Strengths and Difficulties Questionnaire: a research note. *Journal of child psychology and psychiatry*, *38*(5), 581-586.

Hannan, M., & Blundell, B. (2004). Electronic Crime-it's not only the big end of town that should be worried. In *Australian Computer, Network & Information Forensics Conference* (pp. 94-102).

Hox, J. J., & Boeije, H. R. (2005). Data collection, primary vs. secondary. *Encyclopedia of social measurement*, *1*, 593-599.

Hutchinson, D., & Warren, M. 2003. Security for internet banking: a framework. Logistics Information Management, 161: 64-73.

Jaishankar, K. (2007). Establishing a theory of cybercrimes. *International Journal of Cyber Criminology*, *1*(2), 7-9.

Kigen, P. M., Muchai, C., Kimani, K., Mwangi, M., Shiyayo, B., Ndegwa, D., & Siyanda, S. (2015). *Kenya Cyber Security Report 2015*. Serianu Limited.

Kothari, C. (2004). Research Methodology, Methods and Techniques. New Delphi: International P Limited.

Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management*, *11*(4), 541-562.

Lewis, J., & Baker, S. (2013). The economic impact of cybercrime and cyber espionage. *Center for Strategic and International Studies, Washington, DC*, 103-117.

Liao, Z., & Cheung, M. T. (2002). Internet-based e-banking and consumer attitudes: an empirical study. *Information & Management*, *39*(4), 283-295.McCullagh, A., & Caelli, W. 2005.

Who goes there? Internet banking: A matter of risk and reward. Paper presented at the Information Security and Privacy.

Milis, K., &Mercken, R. (2002). Success factors regarding the implementation of ICT investment projects. *International Journal of Production Economics*, *80*(1), 105-117.

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

Mugenda, O.M., &Mugenda, A.G. (2010).Research methods qualitative & quantitative approaches. Nairobi: African Centre for Technology Studies

Muthukumaran. B (2008). Cyber Crime Scenario in India, Criminal Investigation Department Review, pp.17-23

Otieno, E. O., & Kahonge, A. M. (2014). Adoption of Mobile Payments in Kenyan Businesses: A case study of Small and Medium Enterprises (SME) in Kenya. *International Journal of Computer Applications*, *107*(7).

Pilat, D. D., Lee, F., & Van Ark, B. (2003). *Production and use of ICT: A sectoral perspective on productivity growth in the OECD area*. OECD Publishing.

Raghavan, A. R., & Parthiban, L. (2014). The effect of cybercrime on a Bank's finances.

Reynolds, D., Treharne, D., & Tripp, H. (2003). ICT—the hopes and the reality. *British journal of educational technology*, *34*(2), 151-167.

Siddique, I., & Rehman, S. (2011). Impact of Electronic Crime in Indian Banking Sector-An Overview. *International Journal of Business & Information Technology*, *1*(2).

Stafford P. (2013) [Online] Cybercrime threatens global financial system. Available at: http://www.ft.com/cms/s/0/9804988c-3722-11e3-9603-00144feab7de.html#axzz2tMwSTsmF.

Stiroh, K. J. (2002). Are ICT spillovers driving the New Economy? *Review of Income and Wealth*, *48*(1), 33-57.

Symantec Cyber Crime Report, 2012 [Online] Cybercrime Report. Availableat: http://now-static.norton.com /now/ en /pu/images /Promotions /2012/ cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912. Pdf

Wall, D. 2001. 1 Cybercrimes and the Internet. Crime and the Internet: 1.

Wyche, S. P., Smyth, T. N., Chetty, M., Aoki, P. M., &Grinter, R. E. (2010, April). Deliberate interactions: characterizing technology use in Nairobi, Kenya. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2593-2602). ACM.

Zuppo, C. M. (2012). Defining ICT in a boundary less world: The development of a working hierarchy. *International Journal of Managing Information Technology*, *4*(3), 13.

APPENDICES

APPEENDIX A LETTER OF ACCEPTANCE

"Date" 2016

Dear Respondent,

RE: RESEARCH QUESTIONNAIRE FOR CYBER CRIME COSTS.

My name is ELIZABETH NJOROGE a post-graduate student at Jomo Kenyatta University of Agriculture and Technology Karen campus pursuing a master's in business administration programme (finance option). As part of my partial fulfillment of my degree, I am carrying out a research study on "The effects of cybercrime related costs on the development of financially innovated products and services; A case study of by NIC bank." In regards to this endeavor, I would be very grateful if you could share your wealth of knowledge by completing the attached questionnaire. Your answers will be handled with highest, respect, secrecy and discretion.

Kindly return the completed questionnaire to me.

Regards,

ELIZABETH NJOROGE.

APPEENDIX B QUESTIONNAIRE

PART A: GENERAL INFORMATION

Gender: Male [ ] Female [ ]

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

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

4. Highest Level of Education:

Professional Certification [ ] 1st Degree [ ] Masters [ ] PHD [ ]

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

6. Average income per month:

Below 50,000[ ] 50001-150,000[ ] 150,001-300,000[ ] 300,001and above [ ]

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

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

9. How important is cyber security with reference to your e-banking services:

Very important [ ] Important [ ] uncertain [ ] Not important [ ]

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

11. How many account holders have subscribed to the use of E- Banking services?

0 to 5000[ ] 5001-20,000[ ] 20,001-50,000[ ] above 50,000[ ]

PART B: FACTORS AFFECTING THE DEVELOPMENT OF FINANCIAL PRODUCTS.

PREVENTION AND DETECTION COSTS; (Insurance fees, IT systems like firewalls, antivirus)

12. Please tick the numeric variable that most corresponds to your personal opinion on how prevention and detection costs affect the rate of development of innovated financial products and services.

Use the scale 1-5; strongly Disagree (SD)-1, Disagree (D)-2, Neutral (N)-3, Agree (A)-4, strongly Agree (SA)-5

		SD	D	N	A	SA
1	The insurance cost of protecting against cyber related criminal activities affecting the bank innovative activities are too high, thereby affecting how banks are using new products and services					
2	There are many fees and charges required to meet IT compliance standards that a bank must comply to when operating on online platforms					

3	It is an expensive venture to identify and assign specific responsibilities by job function for detecting and reporting suspected unauthorized activity.					
4.	The bank has different insurance accounts set aside to protect customers against losses that may arise from attacks on newly innovate financial products and services					
5	The banks has in place a framework for monitoring the firm's network environment to detect potential cyber security events.					
6	The bank has appropriate measures to deal with successful attacks or intrusions to its system					

Do you think the bank has setup mechanisms to monitor their network?

Yes No

Explain, if your answer is yes.

What do you think the bank spends on insurance cost to protect themselves from cybercrime incidents?

a. Ksh.300,000
b. Kshs 1M
c. Above 1M

RESPONSE COSTS OF CYBER CRIME; (Compensation payments, regulatory fines, legal costs)

14. Please tick the numeric variable that most corresponds to your personal opinion on how perceived response costs affect the rate of development of innovated financial products and services.

Use the scale 1-5; strongly Disagree (SD)-1, Disagree (D)-2, Neutral (N)-3, Agree (A)-4, strongly Agree (SA)-5

		SD	D	N	A	SA
1	Banks are required to compensate victims of identity theft whose information has been hacked, this increases the banks costs hence regulating the adoption rate of some of products, services and processes being innovated.					
2	There are numerous regulatory fines that are associated with lack of compliance to some of the standards issued by the banking oversight committee which affects the rate at which banks adopt innovated products, services and processes.					
3	Banks fear the costs that they may incur from legal suits directed towards them by affected parties of cyber-attacks, hence cautious on the adoption of new products and services.					
4.	Legal forensic issues associated with cyber-criminal activities may lead to the closure of the entire business, therefore banks are cautious on what to adopt in terms of newly innovated banking products and services					

5	Legal and court cases from cyber-attacks take long time to end hence they tend to interfere with daily operations of a bank affecting the bank's profitability, banks therefore prefer well established and secure products and services.					

Do you think a NIC Bank will compensate you in case you lost money through a cybercrime incident in their bank?

Yes No

Explain if your answer is yes.

INDIRECT COSTS; (Reputational damage, loss of confidence by customers, loss of share value).

15. Please tick the numeric variable that most corresponds to your personal opinion on how perceived indirect costs affect the rate of development of innovated financial products and services.

Use the scale 1-5; strongly Disagree (SD)-1, Disagree (D)-2, Neutral (N)-3, Agree (A)-4, strongly Agree (SA)-5

		SD	D	N	A	SA
1	Continues successive cyber-attacks on a bank tends to damage how customers view it, in return affecting the overall business.					
2	Banks main business is from consumers therefore to safe guard their					

	reputation they tend to avoid adoption of new products and services considered vulnerable and risky.					
3	Cyber transactions, online services, new products and processes constitute a large proportion of a banks research and development costs.					
4.	Loss in confidence of cyber transactions, online services, new products and process by customers and businesses translates in indirect losses from R&D, therefore banks are regulation what new financial innovations to adopt and the rate of adoption.					
5	Legal and court cases from cyber-attacks take long time to end hence they tend to interfere with daily operations of a bank affecting the bank's profitability, banks therefore prefer well established and secure products and services.					
6	There is a high chance that reputational damage and loss of confidence would lead to reduction in share price, which may be particularly acute					

Would you close your bank account in NIC Bank if they were involved in a cybercrime related incident?

Yes No.

Explain if your answer is Yes.

Development of financial products

16. Please tick the numeric variable that most corresponds to your personal opinion on development of innovated financial products and services.

Use the scale 1-5; strongly Disagree (SD)-1, Disagree (D)-2, Neutral (N)-3, Agree (A)-4, strongly Agree (SA)-5

Statements	**SD**	**D**	**N**	**A**	**SA**
The bank general opinion is that these costs are 'business-as-usual' costs that would have been incurred anyway, therefore they don't impact development and adoption of new products and services					
Reduced profitability as a result of high costs of protection against attacks has resulted to less adoption of innovated services and products by the bank.					
Disaster recovery processes from an immediate attack usually affect the daily operations and continuance of normal business operations; hence there is a reduction in the rate at which banks are adopting new innovations.					
Banks main business is from consumers therefore to safe guard their reputation they tend to avoid adoption of new products and services considered vulnerable and risky.					

Do you think that the cost incurred in protecting them from cybercrime incidents would affect development of the financial products?

Yes No.

Explain if your answer is Yes.

THANK YOU FOR YOUR ENDLESS ENDEAVOUR IN ENSURING THE SUCCESS OF MY RESEARCH