THE CHALLENGES OF CYBERCRIMES IN INTERNATIONAL BUSINESS OPERATIONS AMONG COMMERCIAL BANKS IN KENYA

SUSAN N. ONCHOMBA

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFIMENT FOR THE REQUIREMENTS OF THE AWARD OF DEGREE OF MASTER OF BUSINESS ADMINISTATION, SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI

2018

DECLARATION

I, the undersigned, declare that this is my original work and has not been presented to any institution or university other than the University of Nairobi for examination.

Signed: _____ Date: _____

SUSAN N. ONCHOMBA

D61/83880/2016

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

Signed: _____ Date: _____

Mr. ELIUD O. MUDUDA

Lecturer,

School of Business,

University of Nairobi

DEDICATION

I dedicate this project to my family member Miss. Naomi Bwari Zablon, who has been a great support and constant encourager towards my education. May the Lord bless her greatly.

ACKNOWLEDGEMENTS

First, I give thanks to the Almighty God for granting me enough strength and courage to be able to complete this goal.

It was with great honor to work with my supervisor, Mr. Eliud O. Mududa, who played a major role of being a good mentor towards this journey of completing my work. His kind assistance, guidance, effortless time, advice and encouragement greatly helped me complete my goal. I also give special thanks to my moderator, Dr. Zachary B. Awino, through his keennessto details, and his great guidance, I was able to work keenly on the document with easiness.

To all my fellow classmates, I appreciate your great contributions and ideas which helped me greatly on my studies. I thank you all for the constructive criticisms during class seminars; you effortless input to my project was indispensable. Finally am extremely thankful to all my respondents, of all the commercial banks in Kenya who welcomed me to their premises and gave me valuable information that enriched this study.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMNS

ATM	Automatic Vending Machine
CBK	Central Bank of Kenya
CMA	Capital Markets Authority
FDI	Foreign Direct Investment
ICT	Information Communication Technology
IRA	Insurance Regulatory Authority
SPSS	Statistical Package for the Social Sciences

ABSTRACT

Throughout the years, the world has become a global village where businesses have shifted their operations from the domestic market to the international market. Technology has enabled this to happen around the globe by creating networks and business relationship. Technology development has not only impacted the globe positively, but also it has impacted negatively by introduction of cybercrimes which have been a great challenge to the business operating worldwide. Its existence has led to great corporate companies to go down into pitfalls because of losing billions and billions of money. The existence of cybercrimes has negatively affected the way businesses have been operating internationally. The objective of this study was to establish the challenges of cybercrime in international operations amongst all the banks in Kenya. The study design used in this study was cross sectional descriptive design. The target population of the study was 40 banking institutions in Nairobi. Primary data collection technique was employed, and was done through use of questionnaires which were given to be filled by the ICT managers who were knowledgeable in regards to cybercrimes. Descriptive statistics with the aid of excel sheets and Statistical Package for Social Sciences was employed. Findings indicate that, Identity theft and hacking affects banking operations to a great extent in the Kenya's commercial banks. In addition, the study found that, malware, phishing, online intrusion, card information skimming and electronic money laundering affected the operations of the banks to a moderate extent. Furthermore, the study has established that, compensation to customers due to loss of their money in cybercrimes is a threat to the growths of the banks. Moreover, study has argued that, using strong passwords, employing qualified ICT officers, having a backup plan for data, and creating employee awareness on cybercrimes, prevents effects of hacking substantially. Based on findings, the study recommends stringent measures to prevent or mitigate against the effects of cybercrimes. In addition, the study recommends that organizations should have a regular back up of their information. Furthermore, the study recommends that employers should build the capacity of their ICT staff and also create awareness on cybercrimes for other staff members and their clients as well, to mitigate against the challenge.

CHAPTER ONE: INTRODUCTION

1.1 Background of the study

The rapid development of technology and innovation has made various activities to be easily done around the globe (Hannan & Blundell, 2004).Currently, business activities are performed from a global perspective which has led to the economic growth of various nations. Generally, technology has created a great impact around the world and this has led to organizations in different nations to build networks, share ideas, acquire resources, buy and sell products that are unique to suit different customer's tastes and preferences among many other factors (Cole &Pontell, 2006). The use of Technology negatively has led to loss of millions of dollars, destruction of organizations hard work and has made countries economic activities to be in pitfalls. One of the areas that technology has created a negative impact is on cybercrimes. Cybercrimes are generally increasing than expected as technology grows rapidly; therefore issues with cybercrime investigations are becoming very complicated without proper frameworks set in place. Therefore getting a solution of such cybercrimes requires a very complicated task (Waithaka, 2016).

Various theories have been applied to study the concept of cybercrime in the international business. A case in point is the risk society theory by Beck and Ritter (2013), which argues that a shift from the traditional society to a new modern society with technology at the heart of the transformation has come with hazards such as cybercrime. This has become a major threat to the international businesses and banks in particular. On the other hand, the rational choice theory advocated by Cornish & Clarke (1986), holds that individuals weigh the costs and benefits of committing a crime and then make a decision. The question to be asked in this study is, has cybercrime become so lucrative as opposed to penalties for the vice? The answer to this question remains unclear despite the increase in cybercrime activities at both local and international level.

Banking industry plays an important role towards economic growth and development through job creation, capital development, tax revenue as well as the promotion of financial inclusion. Kenya has a vibrant banking industry with 43 banking institutions (1 mortgage finance company and 42 commercial banks). These comprises of both local and international banks.

Technology has transformed the way banks transact their businesses especially with introduction of online and mobile banking services which have come with risks of cybercrimes. However, there is limited theoretical and empirical evidence on the challenges that international businesses face in their operations in the wake of cybercrimes.

1.1.1. Concept of Cybercrime

Cybercrime is defined as criminal act done by use of a device that is a computer and the use of internet to harm companies or peoples reputation (Cole &Pontell, 2006). According to Kamini (2011), cybercrime is a crime committed on the Internet or illegal acts using a computer to commit fraud, forgery, identity theft, phishing, spam, junk emails, pornography, online gambling, intellectual property crime, cyber defamation and cyber-stalking or its used as a target victim whereby unauthorized access to computer networks, electronic information, denial of service attacks, malware, malicious, codes, email bombing, data diddling and Trojans.

This generally implies that all cybercrime activities that are committed, involve both the use of a computer and the individual as a victim depending on which two is the main target. A cybercriminal is an individual or person with guilt intention to commits an illegal act (Hannan & Blundell, 2004). These people perform such wicked act because they are motivated criminals, discontented employees in an organization they work, professional hired organized hacker, or even cyber terrorist who have intent to destroy or bring enormous loss of millions of established

organizations around the globe. Cybercrimes can lead to inability to complete contract created in deliver of goods or services and abuse of intellectual property rights. Banks tend to be targets to such attacks because criminals have motives to damage the reputation of firms. Loss of money by banks will lead to customers losing confidence in the organization. Banks tends to be vulnerable especially when attacks are made internally.

Cybercrime is a humongous threat to any nation's economic activities and it's well identified in financial firms. The utilization of electronic cards rather than cash around the world has greatly encouraged cybercrimes in various financial institutions. Banks have generally been the biggest target of these attacks and have lost millions of dollars due to the increase in cyber attacks. The introduction of technology has brought great innovation and creativity in the way the banking industry operates but it has also attracted the criminals with a negative motive to cause damages to the reputation of firms.

It is noted that the current liquidity crisis in Zimbabwe has led to an increased use of real - time gross settlement (RTGS) and payment cards (Mugari, 2016).Hacking, Money laundry, economic espionage, which is the stealing of trade secrets and identity theft are among the growing list of internet created crimes (Mugari, 2016).

1.1.2 International Business Operations

Trade has shifted from domestic level to international levels where foreign firms, businesses and new destinations are increasing (Mwai, 2015). As more businesses grow around the globe, it has attracted people and captivated companies to involve themselves in the International business activities. Private industries are involved in cross border transactions because they want to take advantage of opportunities provided and majorly make profits. Government institutions involve

themselves in cross border activities for purposes of creating a national image, investing in infrastructure, acquire profit and political interests.

The domestic environment differs from that of international business, because international firms operate in an environment that is highly uncertain, the terms and condition of operations are very complex, contradictory, ambiguous and subject to rapid change. Therefore, IB environment requires firms to be flexible to changes that affect the external environment in order to achieve a competitive advantage. International business also involves having foreign investments in foreign nations. In most countries, Foreign Direct Investments (FDI) is used to represent a significant share of domestic product (Wilkins, 1974).Most organizations have different ways of involving themselves in international business such as having trade agreements, establishing of joint ventures, exporting and importing of goods and services, licensing with foreign firms, opening branches for producing and distributing goods in host countries, among many other legal requirements (Wortzel &Wortzel, 1981).

It's also important to identify the participants involved in cross border businesses. They include individuals, various financial institutions, Governments, Ngo's, Parastatals, and private companies (Mugari, 2016). There reason why financial institutions such as banks are involved in international business is to get opportunities to expand their businesses, acquire resources which are limited in a single country, to avoid wastage of available resources due to overproduction, to gain profit opportunities, and sometimes because of competitive pressures.

Other factors such as political, ecological, Technological, social-cultural, economical& competition tend to affect the environment in which international business is carried out. There outcome can be a positive or negative impact if organizations are not flexible to these changing environment.

1.1.3 Banking Industry in Kenya

The Kenya banking industry has revolutionized as technology continue to advance from time to time. The banking sector comprises of CBK, as a regulatory authority, 43 banking institutions, (1 mortgage finance company and 42 commercial banks) (CBK, 2017). It has 13 microfinance institutions, 3 credit reference offices (CRBs), 19 Money Return Providers (MPRs), 73forex offices, 8 non - operating bank holdings companies and 9 representative offices of foreign banks as at 31st December 2017. Locally owned banks are twenty five in number while fifteen are foreign owned (CBK, 2015 in the banking sector, electronic devices have played a significant role in satisfying the customer's tastes and preferences. The evolution of electronic banking has significantly changed the way financial institutions, especially banks, have typically run their businesses and the way customers undertake their banking activities. (Sayar, 2007).

Introduction of Online and mobile banking has made it easy for customers to do their banking transactions easier. Most Customers have opted to use online services because its fast and easier to use, saves on cost, its flexible and convenient for them with their busy schedules (Vrancianu & Popa, 2010).The introduction of mobile money transfer via mobile networks has made work easier for customers according to (Mbiti, 2011). The advancement of technology and online banking services has caused its own inconvenience, which has led to the unlawful transfer of funds to various accounts and has been labeled as banking fraud. (Wall, 2007).

According to Siddique and Rerman (2001) he discovers the following cybercrimes; ATM and use of credit cards fraudulently, Laundering of money, phishing scams, identity theft and denial of services among many others in financial institutions have rapidly increased over the years. Symantec Cyber says. According to the Symantec Cybercrime Survey (2012), 114 billion shillings

have been totally lost in cybercrimes around the globe and the resources used to combat these crimes have been twice as much lost.

1.1.4 Commercial Banks in Kenya

Banks are generally financial institutions that provide services to individuals, businesses and organizations. These services include deposits, current accounts services and saving accounts as well as facilitate loans to businesses. Most of the time, commercial banks are in the business of making profits by utilizing the short-term relatively liquid deposits and converting it to longer maturity loans.

According to(CBK, 2017) Banks are classified further into three categories; Tier 1, Tier 2 and Tier 3 based purely on their weighted index of all their net asset value, customer deposit, capital and reserves and the total number of loans and current accounts. The banks are mostly considered safe by CBK and control almost 50% of the Kenyan banking sector market share. As at December 31, 2017, there were eight large commercial banks with a dominance of 65.98% of the market share, eleven commercial banks which were medium in size holding 26.10% of the market share and twenty one small commercial banks with a dominance of 7.92% of the market share respectively. (CBK, 2017)

Almost 50% of the Kenyan banking sector market share. As at December 31, 2017, there were eight large commercial banks with a dominance of 65.98% of the market share, eleven commercial banks which were medium in size holding 26.10% of the market share and twenty one small commercial banks with a dominance of 7.92% of the market share respectively. (CBK, 2017)

Some banks have been excluded from the list such as Charterhouse bank because it’s under statutory management while imperial bank and chase bank are under receivership. In the banking

Industry of Kenya, commercial banks is regulated by three agencies to ensure prudence and governance in the sector is adhered to. These bodies include: the Capital Market Authority (CMA), Central Bank of Kenya (CBK) and Insurance Regulatory Authority (IRA). All of these are the primary responsibility of the Ministry of Finance (Ariemba, 2012).

1.2 Research Problem

Technology has necessitated organizations across the world to come up with networks, share ideas, acquire resources, buy and sell services and products that are tailored to meet the diverse customer tastes and preferences (Cole &Pontell, 2006). Besides the positive impact of technology such as ease of doing business, innovation among others, technology has also come with negative effects such as cybercrime which has led to loss of huge sums of money and disruption of business activities around the world (Waithaka, 2016).

Global evidence shows that cybercrimes mostly goes undetected, especially in industrial espionage where retrieving of confidential data and documented materials are hard to detect. Due to the rapid growth of technology, the Financial and banking services sector, the non-governmental cyber security market, the IT and telecommunication industry, the military defense forces, the gas and oil sector have become victims of this cyber-attacks. The Africa region has increasingly been faced with sophisticated cyber-attacks catapulted by rapid increase in internet penetration. The Cyber security market in Africa is estimated to grow from $0.92 billion in 2015 to $2.32 billion dollars by 2020 (CBK, 2017).

About 70% of businesses in Kenya that use the internet as a source of networking are exposed to the risks of cyber criminals and malicious insiders because their web devices are designed with their default privacy settings (Ariemba, 2012).. Increased internet penetration and technological advances have driven innovation and business growth. Innovation has exposed large public threats

of cybercrimes (Mwaii, 2015).The Kenya cyber security report 2015, gives a clear overview that Kenya has been losing about Kshs.15 billion equivalent to ($146 million) yearly due to cybercrime activities from Kshs2 billion ($ 22.56 Million) in the year 2013 (Waithaka, 2016). The banking industry is the most vulnerable target of cybercrime perpetrators (Ariemba, 2012).

Empirically, there has been limited empirical evidence regarding challenges of cybercrime especially in the banking institutions in Kenya. Most of the studies have focused on the factors driving cybercrimes and the impact but not challenges. In addition, these studies carried out did not breakdown the nature of costs banks encounter as a result of cybercrime. Furthermore, the most recent studies on the issue of cybercrime in Kenya have methodological challenges. For instance, Waithaka (2016) his research was based on the government agencies, he only selected 20 institutions for which the study considers it to be insufficient. With regards to Kangogo (2008) he used the general population; some of these people had no information with regards to cybercrimes. Therefore our study will fill the existing research gap by investigating further the various challenges of cybercrime in international business operation among the commercial banks of Kenya.

1.3 Research Objective

The objective of this study was to establish the challenges of cybercrime in international business operations among commercial banks of Kenya.

1.4 Value of the study

Cyber-crime in the past had not been seen as a business relevant problem but as technology has been advancing greatly, the challenges have also increased. Therefore the finding of this study will be of great help various stake holders. For bank managers, the study will give a positive revelation of the new cybercrime challenges which has been seen as something difficult to minimize as new

technology advances, especially when setting up new systems and recruiting new ICT expertise. These finding will provide information that will help them to be able to come with proper security procedure and policies to mitigate them against these dangerous vices.

The government institution and policy makers are important institution especially when it comes to making of new laws that are legally accepted in a nation. Therefore, understanding cybercrime challenges in business operations especially in commercial banks of Kenya will assist them to set up new policy formulation as a point of reference in key areas that need policies to level out the playing field for all banks.

The result of this study will be applied by management of other internet companies for their purpose to survive and protection of their business against these cybercrimes that are highly rampant. This study will be of great use to academicians and scholars, as it will form a basis of future research and will also assist in providing a literature review for future studies to both the lectures and students.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This section covers the literature review of the existing literature relating to this study. This study will focus more on challenges of cybercrimes in international business operations and their effect on commercial banks of Kenya. The study will comprise of the theoretical foundation which will elaborate further the theories that are stated and the empirical studies carried out from various scholars that will help us to have more knowledge on this subject matter.

On the empirical studies, the focus will be on the literature reviews of both the international and local studies. The variables that are going to be put into considerations are the independent variables which are the cybercrimes and the dependent variable which will be the international business operations focusing mainly on the challenges of cybercrime in international business operations among the commercial banks of Kenya.

Based on the theories and empirical studies, we will be able to identify the conception gap, the contextual gaps and the methodological gaps that are in relation to this study. This will assists the study to have a clear knowledge on the ideal design to be used. Finally, the variables incorporated in this study will facilitate in the formulation of questions.

2.2 Theoretical Foundation

The following theoretical reviews will be used to show more insights to this study. These theories are the risk society theory and the rational choice theory.

2.2.1 Risk Society theory

According to Beck and Ritter (2013), a sociologist, the risk society theory holds that there is a shift from the traditional and industrial society and towards a new modern risk society which is

individuals, global and self-confrontational. The German sociologist describes risk society as a systematic method of dealing with the consequences and frustrations induced and adopted by modernization itself. The nature of modern societies is such that the risk increases with the increasing complexity of societal production, consumption, governance and technological control systems.

Similarly, Bell (1998) when cited in King and McCarty (2009) describes risk society as a central political conflict and not a class struggle over the distribution of the wealth and natural resources, but rather that every other citizen is fully exposed to technology to some extent. Such as radioactive material, airborne, mass transport hazards such as aircraft, motor vehicle or train crashes, including cybercrime Then This suggests that somehow perversely technological and scientific development generates various types of unforeseen hazards and hence signify serious implications for society.

This theory will be instrumental in understanding the concept of risks that commercial banks face in the wake of technology which has also come with negative impact such as cybercrime. In particular, the theory will delve deep into the challenges or risks associated with cybercrime in Kenya commercial banks.

2.2.2. Rational Choice Theory

In 1970's the rational choice (RC) theory was developed. This theory explains that individual are rational or they tend to use logic and their choices are made in a rational way to increase their utilities. These people have no full control over the results of choices or outcomes. The RC theory shows that somehow the perpetrator actually makes a rational decision to actually commit an

offense and has already measured the financial benefits against the high cost of being thrown in prison.

In this theory, emphasis is put on punishment as a deterrent, to prevent crime from occurring. With certain forms of crime, the background of the offender seems to have very minimal influence on the rational choices he makes. The background factors such as education, upbringing, ethnicity, and social class according to (Cornish & Clarke, 1986).

The above theory will help the study to explore the rationale behind cybercrimes. In addition, the theory will be useful because it will enable us to understand the motive behind cybercrimes which are committed by insiders, and how they weigh or measure the benefits they will receive when they commit such crime without being detected against costs of becoming treated like criminals. Banks have always been victims to such cases especially where there is lack of proper policies and procedures set in place. The end result is that these banks loose large sums of money. Their customers tend to shift to more stable banks because they have lost their trust and confidence in the bank that's falling.

2.3 Cybercrimes in International Business

There are various types of cybercrimes committed at the international scene. There are four broad categories of cybercrime which includes cybercrimes against individuals, against society, against organizations and against properties. Crimes against Individuals include email harassments through use of computer, transmission of child pornography, hacking, indecent exposure, Cyber defamation, Email Spoofing, Internet Relay Chat(IRC), Malicious codes, Net extortion, Trafficking, Distribution, Posting ,Phishing, dissemination of obscene materials like piracy software and financial fraud. Although this type of crime occurs, it's usually minimal.

On the other hand, cybercrimes against properties include Vandalism, Threating, and Salami Attack among many others. This crime is prevalent in the financial institution and it disadvantage is that its amendments are so small that it would go unnoticed. With regard to crimes against organizations, these crimes occur especially when firms are targeted and when “Cracks” into bank accounts and their websites are attacked.

It’s known around the world that any system can be cracked if Security policies are not kept in place. While crime against society include forgery, cyber contraband, web jacking, sale of illegal extortion, Financial Crimes, data diddling, and logic bombs. This includes forgery of currency notes, revenue stamp and mark sheet.

2.4 Empirical Studies and Knowledge Gaps

Various studies have been conducted to analyses challenges arising due to cybercrimes in financial institutions across the world. Siddique and Rehman(2011) conducted research which focused more on establishing the adverse impact of cybercrime inside the India's banking sector. The purpose of this study had been to determine how online criminal activities affect banking and the entire banking sector in order to eliminate cyber crime. This study establishes several cyber crimes which occur in the banking sector. These included: Automatic Vending Machine (ATM) fraud, credit card fraud, and money laundering. In addition, the study found that banks incur huge costs to such criminal activities which lead to loss of customer confidence, which then leads to loosing the business because some of these dissatisfied customers migrate to other banks because of fear of losing more money in the current bank they have been keeping their finances.

Hannan and Blundell (2004) conducted a study into the effects of cybercrime on the bank in Australia. This study had two goals. The first would be to evaluate factors leading to cybercrimes in banking institutions, while the second objective sought to establish challenges of cybercrimes in

financial institutions. This study established that banks suffer from cybercrimes due to poor implementation of legal frameworks and security measures. In addition, it was established that banks face numerous both direct and indirect costs attributed to cybercrimes. Such costs include money spend in remedying the situation after an occurrence of a criminal activity, loss of money due to cybercrimes, interruption of banking services as well as lose of customers due to eroded customer confidence. The study recommended stringent adherence to legal and security measures in order to overcome cybercrimes in the Australia's banking sector.

A study by Raghavan and Parthiban (2014) focusing on commercial banks had sought to determine challenges of cybercrimes in several countries across the world. The study employed an-depth approach to analyses of the cybercrime activities and the payers involved in such activities. In was found out that most cybercrimes are committed with outside elements in collaboration with staff of the respective banks. Internal cybercrimes were also reported which included password fraud and unauthorized access to customer's information, illegal transfers of customer money. In addition, the study reported that loss of cash was the key direct cost of cybercrime in the banking sector globally.

Moore, Clayton and Anderson (2009) have established that cybercrimes are a result of idle nuisance hackers. In addition, the study argued that banks encounter a lot of challenges in their efforts to overcome risk exposures associated with network connections. Further, the study established that some banks have control measures over online fraud. However, banks incur more costs in prevention and cure mechanisms for cybercrimes.

Locally, Mugari (2016) established that banks take an average of ten (10) days to recover from cybercrime incidents, which adversely affects their business operations. For example, this study noted that in Kenya, banks lose an estimated4 billion Kenyan shillings per annum in efforts to

recover from the cybercrime. However, the study noted that this time is higher in other countries like India, where banks take up to 15 days.

Mwai (2015) conducted a study of the things driving cybercrimes among Kenyan commercial banks. Further the study showed there is a high degree of cybercrime even in the Kenyan finance sector. However, most employees interviewed indicated low level of awareness about cybercrimes. According to Waithaka, (2016) he states that the factors According to Waithaka, (2016) he states that the factors that influence cyber security in the national government ministries in Kenya.

This study noted that sabotage and system attacks, lack of management support in cybercrime security and the self - interest system exploitation of employees drove cyber security in Kenya's national government ministries. This study noted that sabotage and attacks to the systems, lack of management support in cybercrime security, and employee's system exploitation for self-interest drove cybercrimes. In Njoroge (2017) a case study was conduct on NIC bank of Kenya on the effect of cybercrime related to cost on development of financial innovation products and services. The study established that there was an increase on cost for cybercrime especially due to new innovation of products and services which negatively impacted on banking operations.

2.5 Summary and Research Gaps

The concept of cybercrime has attracted a lot of debate in the world of academia due to the ever increasing cases of cybercrimes particularly in the financial sector. Various studies have therefore attempted to examine challenges, impact and drivers of cybercrime in both developing and developed countries. From the reviewed empirical findings, it can be deduced that most studies have addressed the issue of causes and the impact of cybercrimes (Hannan & Blundell, 2004; Siddique & Rehman, 2011; Raghavan&Parthiban, 2014) and not challenges. In addition, these studies did not breakdown the costs implications that banks encounter as a result of cybercrime.

Furthermore, this kind of literature is scarce in the Kenyan case. A few studies conducted in Kenya have largely focused on causes of cybercrimes (Mwai, 2015; Mugari, 2016; Waithaka, 2016), and not challenges. Moreover, these studies have largely focused on local perspective and not from the international perspective. Based on this conception gaps, contextual gaps and methodological gaps, the study seeks to investigate the challenges of cybercrime in international business operations among commercial banks of Kenya. The study focused on international business operations as a dependent variable and challenges of cybercrimes as independent variables.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

The research methodology outlines the steps the researcher has taken to achieve the stated objectives. A research design acts as a planning tool that detail how the study is to be carried out. It brings order in the whole study.

In this chapter, the researcher selected the type of the research design to adopt depending mostly on the objectives of the research study. The appropriate research design was cross- sectional descriptive design. The target population selected was 40 banking institutions in Nairobi region. These banks were grouped into tier 1, tier 2, and tier 3 respectively.

The researcher relied on primary data as suitable methods to use in collecting data from the identified population. A questionnaire was issued to 40 respondents who were the ICT managers of the commercial banks to fill. The data collected was also analyzed and presented so as to draw inferences, conclusions and recommendations of the study. All of these have been done to achieve the objective of the study.

3.2 Research Design

Research design is defined as a blueprint or method used to collect data and analyze measures of variables specified in the research problem according to Burns and Grove, (2003). A research design goes a long way to determining how data will be collected and analyzed. A research design is a framework that dictates the entire process of achieving research objectives.

The study adopted a cross sectional survey descriptive research design. (Cooper, 2003) posits that descriptive as a finding of who, how, where, what and when of a phenomena Kothari (2004).

Descriptive research design is appropriate in describing the characteristics of respondents without the manipulation of variables under the study Lewis, 2015.

The purpose of this study was to describe the challenges of cybercrime in the banking sector therefore this design explains the situations as it is, and, it is also a simplified method of research. Therefore it's the ideal design in describing the challenges of international cybercrimes in Kenyan commercial banks.

3.3 Population of the Study

A Population is defined as a group of persons chosen mostly from the population at large who are or hold different characteristics like age group, sex, gender, social status among many others. According to Pole and Lampard (2002), a target population is categorized as all the respondents of a given group or region from which generalization of findings will be based, whereas the accessible population is said to be those components within the field of questioning consists of population and the universe (Kothari, 2014).

Population plays a critical role in the study because it helps further the researcher to generalize the findings. This helps in making relevant inferences and deductions. Since the population is small, a census approach will be employed. A census is indeed an attempt to classify all characteristics in a large group and then to quantify one or more traits of those components. A census will provide specific information on all or many elements in the total population, thereby enabling totals for rare population groups or small geographic areas.

The population of the study selected was 40 banking institutions which were located in Nairobi region. The respondents were 40 ICT managers who belong to those banks who had knowledge of challenges of cybercrime in the banking sector.

3.4 Data Collection

This is a process whereby a researcher gathers information from relevant places to find answers mostly to research problems assess the hypothesis and evaluate the results. To achieve the objective of the study, the study used primary data, with an aid of a questionnaire. (See Appendix I). A questionnaire is a structured form, written or printed, consists mainly of structured series of questions designed to gather information on certain subject matter from one or more respondents. Therefore, the researcher used a closed ended questionnaire which was suitable in providing the respondents with suggestive solutions.

Questionnaires are ideal because they provide a structure way of collecting information. Data was collected through questionnaires which was dropped to the relevant bank officers and then later collected. Due to the busy schedule of these officers, it was proven difficult to secure an appointment with them.

Through the use of Questionnaires, information could be obtained relatively easily because the researcher wouldn't need to be present when the questionnaires are being completed. This is beneficial for large populations when interviews would be impractical

3.5 Data Analysis

Data analysis is defined as a systematic manipulation, processing, arrangement and organization of data to produce meaningful information. Data processing involves coding, editing, classification and tabulation of the data, collected before analysis.

For the purpose of achieving accuracy, consistency, uniformity and completeness, data collected was cleaned, coded and systematically organized in a manner that would facilitate analysis using SPSS which offers extensive data processing capabilities to analyze large and small data.

Descriptive statistics was applied to give central tendency measures such as such as means, standard deviations, minimum and maximums, as well as percentages were used. In addition, frequencies of variables were computed. The analyzed quantitative data was presented in tables and charts.

CHAPTER FOUR:DATA ANALYSIS, RESULTS AND DISCUSSION

4.1 Introduction

Although technology has made it easy for people and businesses to transact across the world, it has also come with the challenge of cybercrimes. This study sought to examine the challenges of cybercrime in international business operations among the commercial banks of Kenya.

This chapter presents research findings and discussions. There are two sections of this chapter, Section one presents, the response rate and background characteristics of the study sample, while section two presents study results based on the objective.

4.2 Response Rate

This study had targeted a population of 40 banking institutions in Kenya. However, the research managed to collected information from 32 commercial banks which represents 80% response rate (see Appendix I). It proved difficult to get responses of the remaining 8 banks during the data collection period. However, following Reierson et al. (2008) who argued that, 70% response rate is enough for data analysis, this study considered the 80% response rate to be more than sufficient.

4.3 Background Characteristics

The study considered various characteristics of the respondents to be very important. These included the tier of the bank, designation of the respondent, gender, age and educational level of the respondents. The summary of the responses are presented in this section.

4.3.1 Tier of the Bank

It was important to consider which tier the bank belonged to since, respondents were asked to mention the tier by ticking on the questionnaire. Figure 4.1 shows the results of these findings.

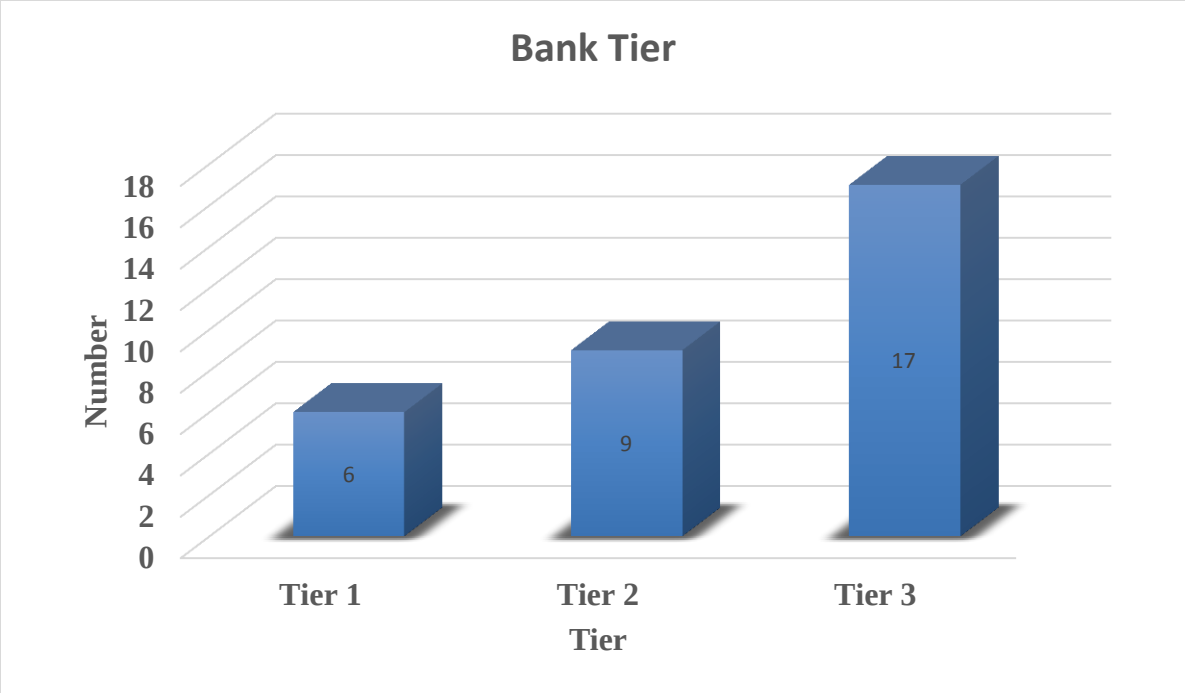

Figure 4.1: Bank Tiers

(Source: Survey Data, Excel output, 2018)

These results show that most of the commercial banks surveyed, 17 (53.13%) belonged to tier 3 followed by those from tier 2 category which were 9 representing 28.13%. In addition, Figure 4.1 indicate that 6 banks, representing 18.75% of all those conducted for an interview, belonged to tier one. Generally, these findings mean that most commercial banks in Kenya are tier 3.

4.3.2 Respondent Designation

The position held by the respondent in the bank was considered very crucial with regard to giving relevant information for the study. Table 4.1 presents tabulated results concerning the designation of the bank officials conducted.

Table 4.1: Respondent Designation

Bank Staff	Frequency	Percentage (%)
Assistant ICT manager	8	25
ICT Manager	24	75
Total	32	100

(Source: Survey Data, Excel output, 2018)

Findings from Table 4.1 indicate the majority, 24 (75%) of the bank officials who responded to the questionnaire were ICT managers, while 8 representing 25% of the sample were ICT assistants. These results imply that, the study collected information from officers who are well informed about issues related to technology, cybercrimes and their challenges to business operations.

4.3.3 Gender

The study considered very key to examine gender representation of the respondents especially at the time when the debate on affirmative action has taken a center stage in Kenya. The study had requested respondents to indicate their gender in the question, and Figure 4.2 displays summary results on this.

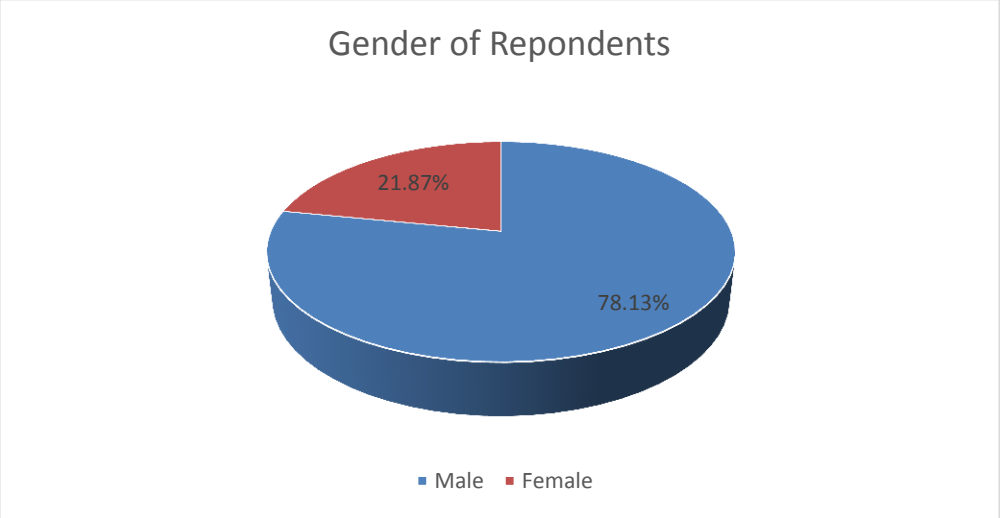

Figure 4.2: Gender of Respondents

(Source: Survey Data, Excel output, 2018)

Findings show that more males than females were interviewed. According to Figure 4.2, 78.13% of the respondents were male, and 21.87% were male. These results imply that there are more males than females working in the ICT departments within the commercial banks in Kenya. The results could also mean that banks have not achieved one third gender representations especially in the ICT departments as envisaged in the constitution. However, since the study did not consider female representation in other departments, the study could not conclude that banks have not adhered to, two third gender rule.

4.3.4 Age of Respondents

With regard to the age of respondents, Figure 4.3 presents the results.

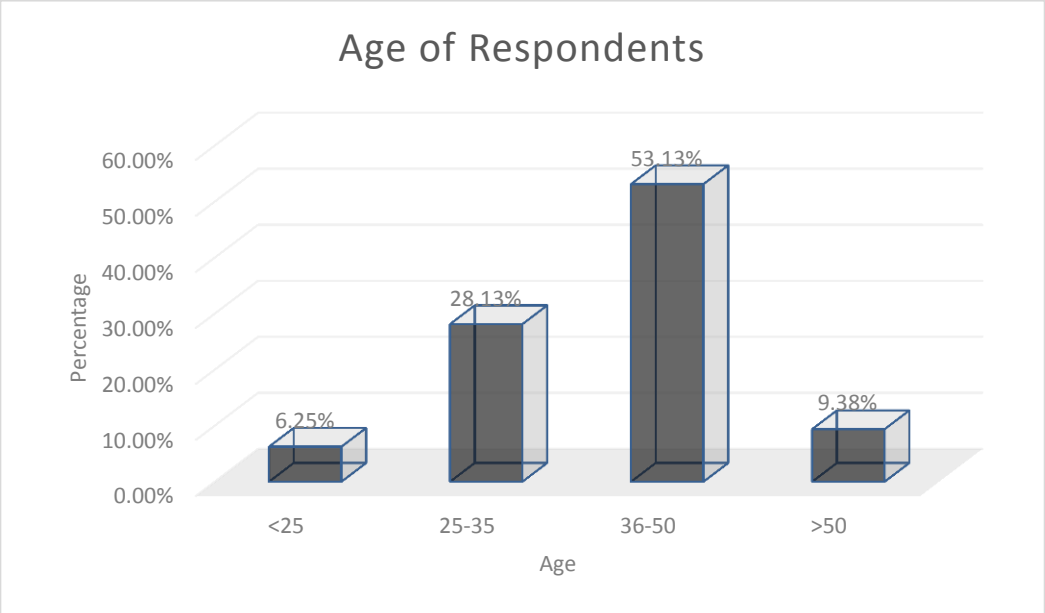

Figure 4.3: Age of Respondents

(Source: Survey Data, Excel output, 2018)

According to the findings, majority, 53 % of the ICT officials who respondent to the questionnaire were aged between 36-50 years, followed by those aged between 25-35 years at, 28.13%. In addition, 9.38% of the respondents were aged above 50 years, while 6.25% were below the age of 25 years.

4.3.5 Education level

The level of education of ICT officers is very important, in terms of efficiency, effectiveness and provision of security to the digital infrastructure of the organization. Thus, it was critical for the study find this by asking respondents to tick on the questionnaire, what their education level was. Summary findings are presented in Table 4.2

Table 4.2: Education of Respondents

Education	**Frequency**	**Percentage (%)**
Professional Certificate	0	0
Bachelor's Degree	22	68.75
Masters	10	31.25
PHD	0	0
Total	**32**	**100**

(Source: Survey Data, Excel output, 2018)

The results show that majority, 68.75% of the workforce in the ICT departments of the commercial banks have bachelor's degrees, while the rest, 31.25 % had masters degrees. This indicates that banks have deployed work force in their ICT departments with the necessary knowledge.

4.4 Challenges of Cybercrimes in International Business operations

The purpose of the study was to determine how cybercrimes affect the operations of international businesses. The study focused on commercial banks in Kenya. The objective of the study was to establish the challenges of cybercrime in international business operations among the commercial banks of Kenya. Respondents were asked various questions in the quest to respond to this objective. First, the study sought to enquire on whether the bank had computerized systems and e-banking. The summary findings are presented in Table 4.3.

Table 4.3: Computerised Systems and E-Banking

Computerized Systems	**Frequency**	**Percentage (%)**
Yes	32	100
No	0	0.00
Total	**32**	**100**
E-Banking	**Frequency**	**Percentage (%)**
Yes	32	100
No	0	0.00
Total	**32**	**100**

(Source: Survey Data, Excel output, 2018)

The results indicate that all banks have computerized systems. In addition, the study found out that all banks have e-banking services. This implies that commercial banks in Kenya are vulnerable to cybercrimes attacks.

4.4.1 Types of Cybercrime and their Effects on Business Operations

The study sought to find out the extent to which the listed types of cybercrimes affected their business operations. Respondents were asked to indicate their response on a Likert scale where: 1=No extent, 2=little extent, 3=Moderate extent, 4-Great extent, 5=Very great extent.

Summary results are presented in Table 4.4

Table 4.4: Types of Cybercrimes

Cybercrime activities	Mean	Std. Deviation	N
Identity theft	4.08	0.222	32
Malware	3.07	0.285	32
Phishing	3.15	0.297	32
Online intrusion	3.17	0.275	32
Hacking	3.90	0.115	32
Card Information Skimming	3.25	0.168	32
Electronic Money laundering	3.14	0.210	32

(Source: Survey Data, SPSS output, 2018)

Findings from the study reveal that identity theft affected affects banking operations to a great extent (4.08), while malware affected business to a moderate extent (3.07). In addition, the results show that phishing affected banking operations to a moderate extent (3.15) as well as online intrusion with a mean of 3.17. Further the respondents agreed to a moderate extent that, card information skimming and electronic money laundering affected banking operations moderately. These had a mean of 3.25 and 3.14 respectively. Moreover, findings showed that hacking having a mean of 3.90 affected banks operations to a great extent.

Generally, these findings imply that these cybercrimes interferes with the operations of commercial banks moderately. These could take the form of interruptions due to intrusion, hacking, phishing and other types of cybercrimes.

4.4.2 Causes of Cybercrimes in the Banking Sector

The researcher sought to determine causes of cybercrimes in the international business, focusing on the banking sector in Kenya. Respondents were asked to indicate their level of agreement on several statements regarding this issue, using the scale 1-5; strongly Disagree (SD)-1, Disagree (D)-2, Neutral (N)-3, Agree (A)-4, strongly Agree (SA)-5. Table 4.5 presents summary findings.

Table 4.5: Causes of Cybercrimes

Description	Mean	Std. Deviation	N
That most of the cybercrime activities committed are through the bank employees who have been working for a long period in the bank?	4.06	0.923	32
That the motivating factor to this cybercrime activities in banks, is employees Greed?	3.40	1.009	32
That the motivating factor to this cybercrime activities in banks, is layoff done for ease of minimizing losses?	3.24	1.368	32
Customers are the ones who have indulged themselves to these fraudulent activities by not keeping their passwords & pin secure leading to fraudulent cybercrimes that occur.	2.04	1.367	32
That cybercrime may be done by rival or competitive firms with intent of ruining the reputation of the organization?	2.45	1.304	32
That money that has been stolen through use cybercrime especially via online platforms can be difficult to trace and retrieve?	4.94	1.148	32
Outsourcing technology has influenced Cybercrime in the Bank Industry?	4.98	1.171	32
Credit cards & Debit cards have largely contributed to Cybercrime activities?	3.04	0.345	32

(Source: Survey Data, SPSS output, 2018)

Findings indicate that respondents agreed (4.06) that most cybercrime activities are committed by bank staff. However, most respondents were neutral (3.40) as to whether employees of the bank are motivated by greed to commit cybercrimes, as well as bank layoffs (3.24).

In addition, most respondents disagreed that cybercrimes occur as a result of customers not keeping their pass words secure (2.04), and they also disagreed that cybercrimes are initiated by the rival companies (2.45). Furthermore, most bank officials who were interviewed strongly agreed (4.94) that it was very difficult to trace money lost in the cybercrime activities, and thatoutsourcingof technology (4.98) has influenced cybercrimes in the bank industry. Moreover, most respondents remained neutral on the assertion that credit and debit cards (3.04) have contributed to cybercrimes in the banking industry.

On the question of –To what extent has the cybercrimes attacked online and mobile banking, Respondents were asked to indicate their response on a Likert scale where: 1=No extent, 2=little extent, 3=Moderate extent, 4-Great extent, 5=Very great extent.

Table 4.6below displays summary of the findings.

Table 4.6: Extent of Cybercrimes on Online and Mobile banking

Description	Mean	Std. Deviation	N
Mobile Banking	3.30	0.023	32
Online Banking	4.76	0.178	32

(Source: Survey Data, SPSS output, 2018)

Findings indicate that cybercrimes affect online banking to a very great extent (4.76), and mobile banking to a moderate extent (3.30). This implies that online banking is the most vulnerable platform for cybercrime perpetrators.

4.4.3 Challenges of Cybercrime in banking operations

On the challenges of cybercrimes, respondents were asked to indicate their level of agreement regarding various constructs on cybercrime challenges using the Likert scale: 1-5; strongly Disagree

(SD)-1, Disagree (D)-2, Neutral (N)-3, Agree (A)-4, strongly Agree (SA)-5.Summary results are presented in Table 4.7.

According to the findings, majority of the respondents disagreed that compensation to customers as a result of cybercrimes affects normal operations with a mean of (2.06), but at same time, most of them agreed these costs of compensation (3.70) are a threat to the growth of bank products. In addition, while most ICT officials strongly disagreed with the statement that banks pay regulatory fines related to non-compliance toCBK standards with regard to cybercrime security which affects bank operations (1.24), most disagreed that banks pays more non-compliance fines to the government and that this interferes with development of new products and the growth of such products (2.04).

Furthermore, in the majority of the banks surveyed, most disagreed that Legal suits arising from cybercrime cases limits product development and growth in the bank (2.33), while on the other hand, most banks strongly agreed (4.87) that cybercrimes is as major challenge to the bank's image.

Moreover, the study has revealed that most respondents remained neutral (2.54) on the statement that cybercrimes leads to frequent interruptions in bank's operations, while on the other hand, most banks disagreed that cybercrimes in the bank have made customers to lose trust in the bank (2.07) and thus affecting its operations.

Finally, the results of the study show that most respondents remained neutral (3.214) on the question that cybercrimes are a major challenge to the bank's share value.

Table 4.7: Challenges of Cybercrimes

Description	Mean	Std. Deviation	N
Bank's compensate the victims of cybercrime which hinder its normal operations;	2.06	.923	32
Bank's costs for compensating victims of cybercrime is a challenge to the growth of its products;	3.70	0.129	32
The bank pays regulatory fines related to non-compliance to CBK standards with regard to cybercrime security which affects bank operations;	1.24	0.213	32
The bank pays more non-compliance fines to the government which interferes with development of new products and the growth of such products;	2.04	0.307	32
Legal suits arising from cybercrime cases limits product development and growth in the bank;	2.33	0.504	32
Cybercrimes in the bank is a major challenge to the bank's image;	4.87	1.142	32
Cybercrimes leads to frequent interruptions in bank's operations	2.54	0.861	32
Cybercrimes in the bank have made customers to lose trust in the bank and thus affecting its operations;	2.07	0.781	32
Cybercrimes are a major challenge to the bank's share value.	3.214	0.325	32

(Source: Survey Data, SPSS output, 2018)

4.4.4 Measures to Counter Cybercrimes in Banks

The researcher sought to find out the extent to which banks have put in place measures to prevent cyber-attacks. Respondents were asked to indicate their response using a Likert where;1=No extent, 2=little extent, 3=Moderate extent, 4-Great extent, 5=Very great extent. Summary results are presented in Table 4.8.

Table 4.8: Measures to Counter Cybercrimes in Banks

Description	Mean	Std. Deviation	N
Use of strong passwords to prevent hacking of computer systems	4.45	0.055	32
Creating awareness on employees on cybercrime activities	3.36	0.098	32
Backing data frequently to avoid loss of digital information	4.04	0.297	32
Banks have set policies to avoid malicious insiders from taking advantage of the bank system and securities	3.17	0.275	32
The bank has invested in employing qualified ICT professionals	3.90	0.115	32

(Source: Survey Data, SPSS output, 2018)

According to the findings, most respondents agreed to great extent (4.45) that banks use strong passwords to prevent hacking of computers, and to a moderate extent (3.36) that banks create awareness among their employees on cybercrime activities. In addition, most banks back their data frequently to avoid loss of information to a great extent (4.04), Furthermore, banks invest in employing qualified ICT professionals to a great extent (3.90).On the other hand, the banks have set policies to avoid malicious insiders to a moderate extent (3.17). This is dangerous because banks are vulnerable when it comes to malicious insiders.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

Cybercrimes have become a major threat to the international businesses in the wake of technological advancement and globalization. The study examined the challenges associated with cybercrimes in the international business operations among the commercial banks of Kenya.

This chapter presents the summary of findings as discussed in chapter four. In addition, conclusions and recommendations are also discussed in this chapter, as well as limitations of the study. Furthermore, suggestions for further studies are made.

5.2 Summary

The aim of this study was to establish the challenges of cybercrime in international business operations among the commercial banks in Kenya. The study focused on all commercial banks in the county of Nairobi. These commercial banks, both local and foreign located in Nairobi by virtue of it being the capital city of Kenya. Apart from the challenges of cybercrime, the study also examined such related aspects as: types and causes of cybercrimes, as well as measures put in place by the commercial banks to prevent cybercrime activities.

A descriptive survey design was employed in this study to explain challenges of cybercrimes within the Kenyan banking sector. This study employed primary data which was collected from commercial banks using a questionnaire. The study had targeted 40 banking institutions. However, the researcher managed to collect data from 32 commercial banks representing a response rate of 80% which was considered sufficient for data analysis. On data analysis, descriptive statistics such as, means, standard deviations, minimum, maximum values, percentages and frequencies were considered.

Findings on background statistics reveal that there are more males than females ICT officers in the commercial banks in Kenya (see Figure 4.2). In addition, this indicates that banks have employed more professional staff in their ICT departments (See Table 4.2).Turning to the results based on the objective, the study indicate that identity theft affected banking operations to a great extent in the Kenya's commercial banks. Similar results are reported with respect to hacking.

In addition, these results show that, malware, phishing, and online intrusion affected business operations to a moderate extent. Similar findings were observed with regard to card information skimming and electronic money laundering.

Regarding causes of cybercrime, the study has established that most respondents were non-communal on whether cybercrimes committed by bank staff are due to their greed. This was after a revelation that cybercrimes in the commercial banks are perpetrated with employees. In addition, the study has also found that most cybercrimes do not result from customers not keeping their passwords secure (see Table 4.4). Furthermore, the study has also discovered that cybercrimes are not instigated by rival banks. Moreover the study has reported that tracing lost money as a result of cybercrime was a difficult task.

Findings have also indicated that monetary compensations to customers who have lost their cash because of cybercrimes do not affect banking operations. However, most respondents noted that such compensations are a threat to the growths of the banks. This could be because, any money compensation imply reduction of capital at the bank's disposal. In addition, while most ICT officials strongly disagreed with the statement that banks pay regulatory fines related to non-compliance to CBK standards with regard to cybercrime security which affects bank operation, most disagreed that banks pays more non-compliance fines to the government and that this

interferes with development of new products and the growth of such products. The study has also learned that law suits as a result of cybercrimes does not limit banks' operations and that cybercrimes do not lead to loss of trust in the banking institutions by customers. Majority of the banks were neutral on the effect of cybercrimes on its share value.

Finally, on the measures to prevent cybercrimes, the study has found that using strong passwords prevents cases of hacking to great extent. In addition, the study has established that creating employees awareness on cybercrimes helps to prevent cybercrime activities to moderate extent. Furthermore, the study has found that banks backing data, and employing qualified ICT officials, helps to safeguard information systems by great extent.

5.3 Conclusion

Based on the findings and summary, this study makes several conclusions: First, the study concludes that identity theft and hacking affects banking operations to a great extent in the Kenya's commercial banks.

Secondly, the study concludes that malware, phishing, online intrusion, card information skimming and electronic money laundering affects operations of the banks to a moderate extent. According to the finding, it can also be concluded that compensation to customers due to loss of their money in cybercrimes are a threat to the growths of the banks. Finally, the study concludes that, using strong passwords, employing qualified ICT officers, having a backup plan for data, and creating employee awareness on cybercrimes, prevents effects of hacking substantially.

5.4 Recommendations

Following the revelation that commercial banks operations are affected by cybercrime activities, it's important to set up stringent measures to prevent or mitigate against the effects of cybercrimes. Such measures that are important to recommend include employment of qualified ICT officers, and use of strong passwords.

In addition, the study recommends that organizations should have a regular back up of their information. This could mitigate against the effects of loss of such data should the system be hacked. Furthermore, the study recommends that employers should build the capacity of their ICT staff and also create awareness on cybercrimes for other staff members and their clients as well, to mitigate against the challenge.

5.5 Limitations of the Study

The study was conducted on commercial banks in general. Better results would have been observed if for instance, a comparison between local and foreign banks was factored in. This study was purely descriptive and hence, very difficult to determine clearly, what is the effect of cybercrimes on banking operations. The study was limited to interviewing bank ICT officials. May be a better perspective of the findings would have been realized with the inclusion of customers, suppliers and other stakeholders of the commercial banks.

5.6 Suggestion for Further Studies

This study recommends a further study which would incorporate, both descriptive and correlation analysis. This could give a more cleareffect. In addition, the study suggests a further investigation where the perspective of customers, suppliers and other stakeholders is incorporated.

REFERENCES

Beck, U., & Ritter, M. (2013).*Risk society: Towards a new modernity*. London: Sage Publications.

Burns, N. & Grove, S.K. (2003).*Understanding nursing research*. (3rd Ed). Philadelphia: W.B. Saunders Company.

Cooper, D.R. & Schindler, P.S. (2003).*Business research methods*. (8thed.).McGraw-Hill Irwin: Boston.

Cornish, D. B.& Clarke, R. (1986). *The Reasoning Criminal: Rational Choice Perspectives on Offending*, New York: Springer-Verlag

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).

Kamini, D., (2011). Cyber Crime in the Society: Problems and Preventions. *Journal of Alternative Perspectives in social Science3* (1), 240-259.
Retrieved from https://www.japss.org/upload/11. Dashora[1].pdf

Kangogo, C., (2008). Cybercrime in Kenya: Myth or Reality.University of Nairobi Research Achieve. Retrieved fromhttp://erepository.uonbi.ac.ke/handle/11295/29547

King, L., & McCarthy, D. (2009).*Environmental Sociology: From Analysis to Action.* (2nd ed.). New York: Rowman and Littlefield Publishers, Inc.

Kothari, C. (2004). *Research methodology: Methods and techniques*. (2nded.). New Delhi: New Age International Publishers.

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health promotion practice*, *16*(4), 473-475.

Mbiti, I. & Weil, D. N. (2011).*Mobile banking: The Impact of M-Pesa in Kenya.*TheNational Bureau of Economic Research Working Paper 17129-http://www.nber.org/papers/w17129

Moore, R. (2005): *Cybercrime: Investigating High Technology Computer Crime*, Cleveland, Mississippi: Anderson Publishing.

Moore, R. (2015). *Cybercrime: Investigating high-technology computer crime*. London: Routledge Taylor & Francis Group.

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

Mugari, I. (2016). Cybercrime-The Emerging Threat to the financial Services Sector in Zimbabwe. *Mediterranean Journal of Social Sciences MCSER publishing, Rome-Italy 7* (3), 135-143.

Mwai, M.N. (2015). Factors contributing to the Occurrence of Cybercrime on E-banking in Commercial Banks in Kenya.(Unpublished MBA thesis). United States International University, Kenya. Retrieved from http://erepo.usiu.ac.ke/handle/11732/636

Njoroge, E.W. (2017). Effect of Cybercrime related costs on Development of Financial Innovation Products and service: A case study of NIC bank of Kenya. (Unpublished MBA thesis). University of Nairobi, Kenya. Retrieved from http://ir.jkuat.ac.ke/bitstream/handle/123456789/4001/LIZ%20DOCUMENT%20%281%29.pdf?sequence=1&isAllowed=y

Pole, C.J. &Lampard, R. (2002).*Practical Social Investigation: Qualitative and quantitative methods in social research.* Harlow: Prentice Hall

Raghavan, A. R., &Parthiban, L. (2014).The effect of Cybercrime on Banks finances. *International Journal of Current Research & Academic Review, 2*(2), 173-178.Retrieved fromhttps://www.scribd.com/document/235452341/A-R-Raghavan-and-Latha-Parthiban

Draugalis, J. R., Coons, S. J., & Plaza, C. M. (2008). Best Practices for Survey Research Reports: A Synopsis for Authors and Reviewers. *American Journal of Pharmaceutical Education,72*(1), 11.doi:10.5688/aj720111

Sayar, C. &Wolfe, S. (2007).Internet banking market performance: Turkey versus the UK. *International Journal of Bank Marketing, 25* (3), 122-141.

Siddique, I., &Rehman, S. (2011). Impact of Electronic Crime Sector. *International Journal of Business Information technology*, Vol -1 No. Pg. No. 159-164.

Internet Security Threat Report2013.(n.d.). Retrieved from https://www.symantec.com/security-center/threat-report

Vrancianu, M. & Popa, L. A. (2010).Considerations Regarding the Security and Protection of E-Banking Services Consumers Interests. *The Amfiteatru Economic Journal*, 1228: 388-403.

Waithaka, S. (2016). Factors Affecting Cyber Security in National Government Ministries of Kenya. (Unpublished MBA thesis). University of Nairobi, Kenya .
Retrieved from http://erepository.uonbi.ac.ke/handle/11295/100423

Wall, D. (2001).*Crime and the Internet: Cybercrimes and cyber fears*. London: Routledge.

Wilkins, M. (1974).*The maturing of multinational enterprise: American business abroad from 1914 to 1970*. Cambridge, MA: Harvard University Press.

Appendix I: Research Questions

Section A: Background Information

1. Bank Name……..
2. **Tier of the bank:** Tier 1 ( ) Tier 2 ( )Tier3 ( )
3. **Designation** in the bank…….(mention)
4. **Gender:** Male ( ) Female ( )
5. **Age:** Below 25 ( ) 25 to 35 ( ) 36- 50 ( ) above 50 years ( )
6. **Education level:** Professional Certification( ) Bachelor's Degree ( ) Masters ( ) PHD ( )
7. Does the bank have computerized systems: Yes ( ) No ( )
8. Does your bank have E-banking services: Yes ( ) No ( )

Section B: Challenges of Cybercrime on Banking Operations

9. Please indicate by ticking in the numeric variable what represents your opinion regarding challenges of cybercrime on banking operations. Use the scale 1-5; strongly Disagree (SD)-1, Disagree (D)-2, Neutral (N)-3, Agree (A)-4, strongly Agree (SA)-5

Description	SD	D	N	A	SA
Bank's compensate the victims of cybercrime which hinder its normal operations;					
Bank's costs for compensating victims of cybercrimes a challenge to the growth of its products;					
The bank pays regulatory fines related to non-compliance to CBKstandards with regard to cybercrime security which affects bank operations;					
The bank pays more non-compliance fines to the government which interferes with development of new products and the growth of such products;					
Legal suits arising from cybercrime cases limits product development and growth in the bank;					
Cybercrimes in the bank is a major challenge to the bank's image;					
Cybercrimes leads to frequent interruptions in bank's operations					
Cybercrimes in the bank have made customers to lose trust in the bank and thus affecting its operations;					
Cybercrimes are a major challenge to the bank's share value.					

10. Kindly specify to what extend the bank have put measures in place to prevent them from cybercrime attack? (Tick the suitable variable in the box provided according).

    1=No extent, 2=little extent, 3=Moderate extent, 4=Great extent, 5=Very great extent.

No	Questions	1	2	3	4	5
1	Use of strong Passwords to prevent hacking of computer systems.					
2	Creating awareness to employees on cybercrimes activities.					
3	Backing data frequently to avoid loss of digital information					
4	Has bank set policies to avoid Malicious insiders from taking advantage of the bank systems and securities?					
5	Has the bank invested in employing qualified ICT professionals?					

11. Among the listed types of cybercrime, Kindly specify to what extent have they affected the bank's business operations (tick)

Types of Cybercrime activities	**1**	**2**	**3**	**4**	**5**
Identity theft					
Malware					
Phishing					
Online intrusion					
Hacking					
Card Information Skimming					
Electronic Money laundering					

12. The use of Online & Mobile banking platform have been the greatest achievements in the banking industry. Kindly specify to what extent have these cybercrime attacks through these platforms have affected the bank industry? (Tick the suitable variable in the box provided accordingly). 1=No extent, 2=little extent, 3=Moderate extent, 4-Great extent, 5=Very great extent

Online platforms	**1**	**2**	**3**	**4**	**5**
Mobile banking					
Online Banking					

13. Please indicate by ticking in the numeric variable what represents your opinion regarding causes of cybercrime in the banking industry. Use the scale 1-5; strongly Disagree (SD)-1, Disagree (D)-2, Neutral (N)-3, Agree (A)-4, strongly Agree (SA)-5

No	Questions	1	2	3	4	5
1	That most of the cybercrime activities committed are through the bank employees who have been working for a long period in the bank?					
2	That the motivating factor to this cybercrime activities in banks, is employees Greed?					
3.	That the motivating factor to this cybercrime activities in banks, is layoff done for ease of minimizing losses?					
3	That Customers are the ones who have indulged themselves to this fraudulent activities by not keeping their passwords & pin secure leading to fraudulent cybercrimes that occur					
4	That cybercrime may be done by rival or competitive firms with intent of ruining the reputation of the organization?					
5	That money that has been stolen through use cybercrime especially via online platforms can be difficult to trace and retrieve?					
6	Outsourcing technology has influenced Cybercrime in the bank Industry?					
7	Credit cards & Debit cards have largely contributed to Cybercrime activities?					

Appendix II - List of Commercial Bank in Kenya.

No.	Tier I Banks	No	Tier 3 Banks
1	Kenya Commercial Bank	1	Gulf African Bank
2	Equity Bank	2	Victoria Commercial Bank
3	Barclays Bank	3	Giro commercial bank
4	Standard Chartered Bank	4	African Banking Corporation
5	Co-operative Bank	5	Sidian Bank Ltd
6	Commercial Bank of Africa	6	Habib Bank A.G. Zurich
7	Diamond Trust Bank	7	Guadian Bank
8	Stanbic Bank	8	Credit Bank
		9	First Community Bank
	Tier 2 Banks	10	Jamii Bora Bank Ltd
1	I & M Bank Ltd	11	Development Bank of Kenya
2	NIC Bank	12	M- Oriental Commercial Bank
3	Bank of Baroda (K) Limited	13	Transnational Bank
4	Citibank N.A Kenya	14	Consolidated Bank of Kenya
5	National Bank of Kenya	15	Paramount Bank
6	Prime Bank Limited	16	Spire Bank
7	Family Bank Ltd	17	UBA Kenya Bank
8	Bank of India	18	Middle East Bank
9	HFC Ltd	19	Equitorial Bank
10	Eco Bank Kenya	20	Fidelity Bank
11	Bank of Africa (K)	21	Guaranty Trust Bank
		Under statutory management	
		1	Charterhouse Bank * *
		Under receivership	
		1	Imperial Bank * *
		2	Chase bank* *