UNIVERSITY OF NAIROBI

MANAGEMENT OF CYBER FRAUD IN COMMERCIAL BANKS IN KENYA: A CASE OF CHASE BANK

NYAMWARO N. BONARERI

C50/79525/2015

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT FOR REQUIREMENTS FOR THE AWARD OF MASTER OF ARTS IN SOCIOLOGY (CRIMINOLOGY AND SOCIAL ORDER) UNIVERSITY OF NAIROBI.

March, 2021.

DECLARATION

This Thesis is my original work and has never been presented in any other University for award of any degree.

Signature  Date 01/11/2021

Nyamwaro N. Bonareri

C50/79525/2015

This project has been submitted for examination with my approval as university supervisor.

Prof. Robinson Ocharo.

Signature  Date 02/11/2021

DEDICATION

I dedicate this study to my wonderful mother and my entire family for their unwavering support and throughout this journey. Their resolute belief in me and my ability to complete this program and kept me always moving forward. God bless you abundantly and thank you.

ACKNOWLEDGEMENTS

I would like to thank the Almighty God for granting me good health throughout my entire course. My geniune gratitude to Prof. Ocharo for his guidance throughout this research project. The completion of this research project would not have been possible without his assistance and supervision. To my peers I appreciate the constant consultations and discussions we shared and words of encouragement throughout my study duration.

I am forever indebted to the management of the University of Nairobi for their help guidance in this process; for providing resources which were pertinent in preparation of the same. The knowledge gained from the course work, prior to embarking on this project, made it possible to undertake my research work.

To my family, thank you for the patience and support accorded to me while I spent long hours putting together this research work. I am greatly indebted to the management and staff members of Chase Bank Kenya (In Receivership) for their support during the research period.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF GRAPHS

LIST OF ABBREVIATIONS

AML- Anti Money Laundering

ATM- Automated Teller Machine

CAPEX- Capital Expenditure

CBK- Central Bank of Kenya

CC- Credit Committee

CCTV- Closed Circuit Television

G20- Group of Twenty (countries that include Argentina, Austarlia, Brazil, Canada, China, European Union, France, Germany, India, Indonesia, Italy, Japan, Korea, Mexico, Russia, Saudi Arabia, South Africa, Turkey, United Kingdom, United States.

ICT- Information and Communication Technology

IR- In Receivership

ISO- International Standards

ISTF- Inter-departmental Information Security Task Force

IT- Information Technology

MS Excel- Microsoft Excel

PKI- Public Key Infrastructure

PwC- PricewaterhouseCoopers

SIEM- Security Information and Event Management

SME- Small and Medium Enterprises

SPSS- Statistical Package for Social Sciences

UK- United Kingdom

US- United States (of America)

USD- United States Dollar/ American Dollar

ABSTRACT

Kenya is experiencing a growing number of Cyber fraud that threaten national security Information communications and technology infrastructure as well as citizens privacy.The objective of the study was to establish the management of Cyber fraud in commercial banks in kenya.The specific objectives of the study were to find out the forms of Cyber fraud by commercial banks, to establish the challenges faced by commercial banks in managing Cyber fraud , to evaluate the effect of preventive measures in curbing Cyber fraud in Kenyan commercial banks. The units of analysis was Cyber fraud and units of observation was management staff of the bank. The study employed qualitative approach and Primary data was obtained by census method, while secondary data was obtained through various publications referenced .Data was measured and has been presented in frequency tables, graphs and percentages.The study observes that a strong system of internal control is the most efficient way of fraud prevention and technological infrastructure has a major effect on prevention of Cyber fraud . The study concludes that commercial banks in Kenya faced various forms of Cyber fraud like Cyber fraud spam, phishing and password sniffers to great extents.The study recommends that banks should implement systems and structures that reduce the opportunities for Cyber fraud. Besides strengthening internal control systems and structures, banks can use ICT tools to reduce opportunities or instill punitive measures for employee's engaging in fraud related incidences.

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

As the world embraces technology and discards traditional models of business the threat and risk of fraud has increased. Over the past few years, technological developments have been transforming the demeanor of commerce and monetarist transactions. The arrival of the internet and advances in information technology have multiplied the possibilities for moving digital information allowing financial services to be provided to a wider variety of institutional and retail clients at far lower transaction costs with important implications for access to financial services. With all the innovations new channels of committing crime have also evolved known as Cyber fraud crimes (Welch, 2009; Fatima, 2011).

Cyber fraud can simply be explained as illegal activities carried out with the aid of a computer system. These activities may involve targeting a computer, computer systems, information network or data in an attempt to steal valuable information (Douglas and Loader, 2000; Maat, 2004). Cyber fraud s may also involve offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly using modern telecommunication networks such as Internet (Chat rooms emails notice boards and groups) and mobile phones (Halder & Jaishankar, 2011). Wall (2001), categorizes Cyber fraud s into four major groups namely: Cyber fraud - deceptions, Cyber fraud -pornography, Cyber fraud -violence and Cyber fraud - trespass.

Cyber fraud s have become as real threat today and unlike traditional crimes such as robbing mugging or stealing Cyber fraud s can be committed single handedly and do not require the physical presence of the criminals. Such crimes may threaten as nation's security and financial health (Saul, 2007). Gathungu (2013) noted that Cyber fraud can be committed either internally within an institution, externally by outside parties targeting the institution, or both where perpetrators from within the institution work in liaison with external parties to defraud the institution.

In banking sector, Cyber fraud s are committed using online technologies to illegally remove or transfer money to different accounts and are tagged as bank fraud (Wall, 2001). Sometimes the intention of Cyber fraud criminals 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 (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 Cyber fraud s in the banking sector. A strong system of internal control is the most efficient way of fraud prevention. The banks should increase their efforts in sensitizing all concerned parties on the need for security in the organizations so as to fight fraud (Khanna & Arora, 2009).

Cyber fraud mitigation efforts within many businesses are hampered by a combination of limited board and top management engagement in addressing Cyber fraud security and Cyber fraud challenges limited

resourcing and Cyber fraud capabilities and limited investigation and reporting of Cyber fraud . Commercial banks minimize incidences of fraud through establishing good internal controls, discouraging collusion between employees and customers and having clear anti-fraud policies, monitoring employees, providing a whistle–blowing system, punishing offenders, conducting proactive auditing and effecting robust corporate governance practices (Albrecht, Albrecht, Albrecht, & Zimbelman, 2009). Corporate Cyber fraud mitigation as well as corporate Cyber fraud -risk management is hampered by many businesses continuing to see the threat as a purely technical issue rather than as a challenge for the board the entire organization and for business strategy. A 'compliance approach' that aims to meet minimum standards does not adequately deal with intelligent and evolving adversaries as threats are evolving faster than most defensive technologies and security practices.

Management of Cyber fraud in institutions across the globe varies. Cyber fraud in developing countries differs from that in developed countries. This has been attributed to structural difference like nature and quality of hardware, software and infrastructure; target ability of victims; Cyber fraud skill set; and associated opportunities, costs and benefits. Higher broadband penetration and internet connectivity as in developed countries attract more Cyber fraud -attacks as opposed to lower broadband penetration in developing countries which is unreliable for Cyber fraud activity. Cyber fraud awareness is low among the law enforcement especially in developing countries. Fighting Cyber fraud in developing economies is challenged by lack of resources to build institutions to combat it, the know-how, and poor

understanding of ICT, and lack of legal framework and enforcement policies to handle Cyber fraud s (Kshetri, 2010).

Crime-research.org indicates that as early as 2003 the United States was already leading the world in percentage of Cyber fraud -attacks at 35.4 percent followed by South Korea at 12.8 percent. Countries with high rates of computer piracy such as Russia have reacted slowly to Cyber fraud . As a result, many hackers and other Cyber fraud criminals can flourish in countries with few internet crime laws while attacking richer countries through their computer because it lacks rules and codes of a central authority which governs it as such internet has no geographical demarcation as remarked by Guillane and Fortinet (2009).

An audit report by PricewaterhouseCoopers- PwC (2011) showed that fraud has risen from a peripheral issue for banks and other financial institutions to a top three issue that managers and supervisors have to deal with especially in the East African region. In a study on 33 banks across Kenya, Zambia, Rwanda, Zambia and Uganda, fraud was identified as the major factor influencing risk management decisions and strategies for financial institutions.

In Kenya fraud especially in the banking industry has grown steeply over the last few years. Kenya is experiencing a growing number of Cyber fraud that threaten national security Information communications and technology infrastructure as well as citizens privacy. The country is losing an estimated 2 billion kshs. ($23.3 million) annually through Cyber fraud .The Central Bank of Kenya- CBK (2013) noted that fraud has grown in the last few years and has led to

billions of shillings in losses for banks in Kenya and that the major forms of fraud in Kenya that were to be given keen focus are: card, insider, electronic and cheque fraud. In addition, CBK noted that in the year 2012 over 36 fraud cases were reported to the Cyber fraud crimes Unit and Bank Fraud department of the Kenya Police Service and only 16 had been successfully investigated and prosecuted.

According to Banking Fraud Investigation Unit (2011) during the 1st quarter of year 2011, cheque fraud was the most common type of fraud while in the 2nd quarter forgery was leading' Same was the case in the 3rd quarter. Forgery rose mainly after cheques were stolen and signatures were forged. There were also cases where deposit slips were forged and fraudulent instructions issued to make transactions.

1.2 Statement of the Problem

With the rise of Cyber fraud , there is need to create a standard strategy that can be used as a minimum requirement for Cyber fraud security solution. But this does not mean taking a one-size-fits-all approach. Research has shown that a common approach and proposed frameworks for Cyber fraud security challenges in developing nations have shortcomings. It finds that developing nations imitate what is done in the developed world which the research concludes is not a good approach. The researcher reiterates that better approach starts by identifying the different challenges between the developing nations and the developed nations and how these differences impacts the national strategic approach. The researcher concludes that while the physical hardware and software may be the same the circumstances in a developing nation are different which necessitates a customized solution and strategy (Tagert, 2010).

Another problem as noted by French (2012) is that organizations are spending the majority of their efforts on external security without properly assessing the importance of internal security. With internal security being of a higher risk than external security, these additional security measures give users a false sense of security. The study tries to address the need for increased awareness of internal threats through security measures such as security awareness policies practices and procedures.

In Africa, the growing use of financial technology has put banks as the lead target of Cyber fraud . Serianu's Cyber fraud security Report (2016) posits that African countries lost at least 2 billion dollars in Cyber fraud -attacks in 2016. In East Africa, Kenya recorded the highest losses at 171 million dollars with Tanzania and Uganda losing 85 million dollars and 35 million dollars respectively. The report also noted that there is a low response level to Cyber fraud -attacks as many institutions budget very little to none at all for Cyber fraud security.

Kenya did not have a National ICT Policy until November 2004 when the Government of Kenya published a draft of it. As noted by Outa, Etta and Aligula (2006), there was a need for regulating and mainstreaming ICT in Kenya and as such, one of the proposals they offered was the amendment of Penal Code Cap 63 to recognize and punish Cyber fraud among other e-crimes. Only until July 2016 was the Cyber fraud Security and Protection Bill drafted and presented to the Senate by the Committee on Information and Technology, Kenya (Kagwe, 2016). This Bill is yet to be passed as law. This shows the slow approach in addressing Cyber fraud security in Kenya, with no proper legal framework.

There has not been a central monitoring and evaluation authority for Cyber fraud security in Kenya that may provide information and impart knowledge to the public on how to handle Cyber fraud -attacks and as such no harmonized strategies for the same. Uncertainty on the policies, procedures or guidelines to follow in handling the increasing Cyber fraud -attacks in Kenyan institutions has prompted the Central Bank of Kenya (CBK) to draft guidelines that are the minimum standards for financial institutions to handle Cyber fraud security issues. These institutions were required to submit their Cyber fraud security policy, strategies and frameworks to CBK by 31st August 2017 (CBK, 2017). Seeing as to how recent this action is, information on Cyber fraud crime management for specific institutions is not yet readily available. Given the prevalence of Cyber fraud fraud, it is important to examine the management of Cyber fraud fraud in commercial banks in Kenya where the context of focus will be Chase Bank Kenya.

1.3 Research Questions

The study seeks responses to the following research questions;

i. What are the common forms of Cyber fraud in commercial bank?
ii. What are the preventive measures to curb Cyber fraud in commercial banks?
iii. What are the challenges faced by commercial banks in dealing with Cyber fraud ?
iv. What is the moderating role of government policies in Cyber fraud ?

1.4 Objectives of the Study

The main objective of the study was to establish the management of Cyber fraud in commercial banks in kenya

Specific objectives

The study aimed at achieving the following specific objectives;

i. To establish the common forms of Cyber fraud in commercial banks.

ii. To examine the preventive measures to curb Cyber fraud in commercial banks.

iii. To establish challenges faced by commercial banks in dealing with Cyber fraud .

iv. To examine the moderating role of government policies in Cyber fraud .

1.4 Significance of the Study

This study is significant in providing useful information that may benefit various organizations as follows; the findings of the study would assist most commercial banks in Kenya in knowing the weakness in structures and systems erected to manage Cyber fraud and remedies to the same. It would assist them gauge the impact of technology, internal controls and Cyber fraud management with respect to their institutions.

To the Government of Kenya the study would help in formulating appropriate (monetary and fiscal) policies to govern the financial services industry. It would help the CBK into understanding the fraud leakages in financial institutions which affects the economy hence assist them in making proper regulations of control and monitoring for protection and compliance. It would also help them in updating their prudential guidelines which would in turn assist in the day to day running of the banking industry.

The study of Cyber fraud in commercial banks is recommended in any study of social science. It would also assist students undertaking; security, criminology auditing and accounting related courses at the university and other colleges. It would give them an insight and understanding fraud in the banking industry, control and preventive measures.

1.5 Scope and Limitation of the Study

The study focused on the management of Cyber fraud in commercial banks in Kenya with a focus on Chase Bank. The study sought information on the management of Cyber fraud in Chase Bank(In Receivership (IR))from top, middle and lower level staffs. The study had assumption that respondents had adequate knowledge and information .

The respondents reluctant in giving information fearing that the information sought may be used to intimidate them or print a negative image about them or the Bank. Some respondents turned down the request to fill questionnaires. The researcher handled this problem by carrying an introduction letter from the University and assuring them that the information given would be treated with confidentially and purely for academic purposes.

Staff working in financial institutions like Chase Bank, operate on tight schedules, as such, most of them were unable to complete the questionnaire in good time and this overstretched the data collection period. To mitigate this limitation the researcher made use of personal networks to persuade targeted respondents to fill up and return the questionnaires.

CHAPTER TWO:LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Introduction

This chapter contains empirical, theoretical and conceptual frameworks. It starts off by reviewing empirical literature which begins by identifying common forms of Cyber fraud committed around the world. It further examines the preventative measures used to manage Cyber fraud, and also some of the challenges faced in the management of Cyber fraud. Under the theoretical review, the Fraud triangle, Agency theory, and the Fraud Management Lifecycle are discussed. Thereafter, the conceptual framework gives a diagrammatic perspective of the study.

2.2 Empirical Review

2.2.1 Forms of Cyber fraud Fraud

Cyber fraud or ICT crime may involve the physical theft of a computer or its components or using a computer to gain illegal access to a computer system or network. From a general view point, Cyber fraud can be categorized as: Software Piracy, Hacking, Internet fraud, and Industrial espionage, all of which are illegal in many countries (Birbal and Taylor, 2005; Long, Millbery and Stuart, 2008). Longe & Chiemeke (2008) add on to this list acts such as Cyber fraud terrorism Cyber fraud stalking, Electronic spam mail, Phishing and Copy-cat websites. While some types of Cyber fraud s are specific to a given country, other types such as identity theft and false statements cut across all countries.

In software piracy there is unauthorized copying, use and selling of copyrighted content. Software piracy may involve: counterfeiting, internet piracy, duplication of pre-

installed software or licensed user software for unlicensed users. This is wrong as it is infringement on ownership rights, which is theft as it denies the owner potential revenue (Birbal and Taylor, 2005).

In industrial espionage, spies leak confidential information of a company in an attempt to gain advantage at the expense of the company. The information may be new product designs or even personal customer information. With such information exposed a company loses revenue, competitive edge, customers and even gets threatened with law suits. Industrial espionage is usually carried out as both an internal and external job; where employees of the company may work with external individuals or competing organizations to perpetuate the act. In 2005 Israeli Police broke an industrial espionage ring which targeted various companies where they planted a Trojan Horse Virus in the companies' computers and gathered confidential information. As a result of spying, victims lost competitive bids and thousands of customers. Hundreds of millions of dollars were also lost (Birbal and Taylor, 2005).

Hacking provides unauthorized access to a computer system and many hackers are excellent computer programmers. Hacking can be damaging especially if the hacker steals confidential information, alters or destroys data, or transfers money from bank accounts. Some of the methods used by hackers are to access computers are: impersonation, remote login, or even brute force to find passwords (Birbal and Taylor, 2005). Hackers may use methods such as sending Cyber fraud spam or Password sniffers to encode malware that when opened can access other computers.

Cyber fraud spam also known as electronic spam mails uses electronic messaging systems to send unsolicited bulk messages indiscriminately

(Schmalleger and Pittaro, 2009). Through wiretapping methods criminals have been known to access network cabling to eavesdrop on communications. Fraud through communication networks has risen with the increased use of cell phones and purchase of goods and services over the phone as people share their payment information on the same (Shandilya, 2011; Wada and Odulaja, 2012). Littman, 1997 reported that Kevin Poulsen, a notorious American hacker was able to access law enforcement and national security wiretap data prior to his arrest in 1991. In 1995, Amsterdam Police communications system was hacked by a criminal organization that succeeded in gaining police operational intelligence and in disrupting police communications. The effects of such activities are great with millions of dollars being lost annually (Herald Tribute, 2007).

On the other hand, Password sniffers are programs that hackers install on networks they would like to penetrate. The program is able to monitor a network and collect specific data such as a username and a password as required when using certain common Internet services. Additional programs may also be used to automatically hide the existence of the sniffers. In 1994, it was estimated that about 100,000 sites were affected by sniffer attacks (Wada and Odulaja, 2012).

Internet fraud schemes make fraudulent offers to prospective victims and conduct fraudulent transactions using one or more components of the internet like chat rooms, email, websites, and so on. A good example is credit card fraud where a bogus business is set up luring unsuspecting people into giving their credit card information in order to steal their money (Birbal and Taylor, 2005). Other forms of internet fraud schemes include Phishing and Copy-cat websites.

Copy-cat websites are a recent trend in on-line fraud that takes advantage of consumers who are not familiar with the Internet or who do not know the exact web address of the legitimate company that they wish to visit (Wada & Odulaja, 2012). The consumer unknowingly enters confidential information into a fraudter's personal database, which the fraudter uses at a later stage either for his/her own purposes or sell to interested parties who may use it for credit card fraud, or identity theft.

Copycat websites are used in phishing, which is a high-tech identity theft that steals personal information from unsuspecting consumers like online banking account login and password to getting access to ATM. It also defraud legitimate businesses and financial institutions by creating illegitimate sites to pose as these institutions. Successful phishing must present a high credibility web presence that causes the victim to fail to recognize security measures installed in web browsers (Kochems and Keith, 2006; Cameroon, 2011). Litan, (2004) noted that American banks and card issuers lost 1.2 billion dollars in 2003 as a result of two million customers giving information to spoofed websites. In 2006, a study on phishing attacks found out that 90 percent of participants were fooled by well created phishing websites. It further noted that existing anti-phishing browsing clues were not effective and 23 percent of participants in the study did not look at the status bar, security indicators, or the address bar (Rachna, Tygar, & Hearst, 2006).

Cyber fraud threats in the wake of emerging transaction that constitute internet banking, mobile banking, mobile transaction and cloud expansion is seen as the most

deadly threat to the economy yet to be seen. With continued advancement in the ICT sector, Cyber fraud crimes are increasing at an alarming level. For instance, in 2011 Singapore reported that 80 percent of internet users had experienced Cyber fraud crime which was the fourth highest rate in the world (Symantec Corporation, 2011). In the U.S., a 33.1 percent increase in Cyber fraud crime was reported between 2007 and 2008 especially an increase in identity theft. It was further reported that the number of identity thefts rose by more than tenfold from 31,140 to 313,982 incidents in a time span of 9 years- 2000 to 2008 respectively. Additionally, identity theft remained at the top of the complaints list (National White Collar Crime Center, 2008; Federal Trade Commission, 2009, 2010, 2011).

The Center for Strategic and International Studies (2015), reported that costs of Cyber fraud crime fraud experienced by the G20 countries which lost more than 200 billion dollars to Cyber fraud. Kenya is fast embracing technology and dynamically changing to Electronic transaction reliance country and without proper national Cyber fraud security strategy in place to identify the threats we are up against it will be a losing battle. According to (Serianu-Kenya Cyber fraud Security Report, 2014) there is a sharp increase in the number of Cyber fraud -attacks to public, private and mostly financial institutions leading to loss of approximately Kes 2 billion with in the same year. This figure drastically rose to Kes 17.1 billion in 2016 (Serianu- Kenya Cyber fraud Security Report, 2016). Hence there is an urgency to manage the Cyber fraud vice before further destruction.

2.2.2 Management of Cyber fraud in Commercial Banks

The availability of quality technology within commercial banks is a factor that may determine the level of security in terms of encryption as well as internal controls in a particular financial institution. With the emergence of new technology and in particular the banking sector has transformed the manner in which business is done in the 21st century. However such technology has also brought about numerous challenges such as online fraud as well as increased money laundering fostered by the introduction of electronic money transfer services. The banking sector should thus adopt quality technology in order to keep up with the dynamics associated with technology in order to counter these challenges.

In this era of information and technology, banks have automated their services to provide convenient services to their customers. Computers are used to process customer transactions, transfer funds and also to process cheques. Other technologies include Automated Teller Machines (ATM), Internet Banking, Mobile Banking, Credit Cards and Smart Cards. To deter the ever increasing Cyber fraud attacks, there is a dire need for increased Cyber fraud security (Birbal and Taylor, 2005). So how do commercial banks protect their customers and themselves?

For starters, they need to protect both the physical components of a computer as well as the software or logical methods. Physical security involves physically locking computer hardware, security guards, alarms, monitoring cameras, scanners, fire-proofing storage areas, and so on. Software data security would involve passwords, audit trails or access logs, encryption, firewalls, and anti-virus software (Lawson, Jarvis Blundell and Reid, 2004; Birbal and Taylor, 2005; Long et al., 2008). Organizations can also use their

systems to manage Cyber fraud through fraud detection methods, corporate governance, internal controls, structural framework, information infrastructure, laws and regulations, and government action.

Fraud Detection technology is on demand among institutions as they invest in new systems and processes that make it difficult for criminals to target them. A good example is the Anti-Money-Laundering (AML) technology solution (Beck, Demirguc-Kunt and Levine, 2009). Such technological solutions simplify work flow and bring consistency to the audit process. Technology is able to look at transactions as a whole as opposed to a manual process that looks at transactions singularly. Other technologies like audit trails, access logs, and surveillance cameras assist to avoid criminal activity or identify and track down the perpetrators of such activity. Stafford (2013) noted that banks across the globe perceived Cyber fraud are among their top five risks considering that even high profile banks in the UK and the US, like Barclays and Standard were targeted by hackers to incur huge losses by stealing personal information of nearly 2.9 million credit card customers by hacking the software maker system of these bank. In order to curb such problems, a program known as Quantum Dawn 2 was launched which tests the efficacy of systems installed in banks in response to Cyber fraud -attacks.

Surveillance Systems include video surveillance from private to public spaces as used for traffic surveillance, domestic surveillance, ATM cameras, banking hall cameras, retail stores surveillance and so on. This technology started in the United States of America (US) in late 1950s to monitor private retail interests and traffic flows and has evolved into a police-managed and/or government funded open visual

surveillance system today (Hier, 2004; Greenburg and Roush, 2009). Over time Closed Circuit Television (CCTV) surveillance systems have been advanced to include more features. For example, in some cities like Boston and Newark, gunshot location technology is installed in surveillance systems to alert authorities to where guns have been fired. This also allows rapid emergency response of medical personnel and police to those locations (Mazerolle, et.al., 1998). In Shenzhen, China CCTV cameras have been installed with the capability of alerting police when an excess number of people crowd at one place. Additionally, facial recognition software has been developed that allows authorities to identify individuals under video surveillance. CCTV surveillance and street lighting, have been noted to be more effective in crime prevention (Welsh and Farrington, 2007; Hertz and Simon, 2011).

Corporate Governance provides sets of mechanisms and processes that top-level management use to direct their organizations to create value for their stakeholders. This means that there needs to be transparency and accountability in organizations dealings while keeping the stakeholders' interest in mind. Part of corporate governance involves risk management and not only on return on investment but also on fraud which has adverse negative effects on performance. With organizations converting to digital transactions, their corporate governance systems should also reflect on a digital platform; putting in place policies that enlighten employees, customers and even management on how to rightly use their computer management systems. Cyber fraud insurance is also a great way to manage Cyber fraud risk and some insurance companies in Kenya are now offering this cover. Proper corporate governance is capable of keeping track of all the operations of an organization, which may prevent problems like fraud and corporate

espionage. Therefore, top-level management support and commitment is vital for effective decision-making in risk management (Merchant and Van der Stede, 2007; Klein, 2008; Grabowski and Robert, 2009; Serianu-Kenya Cyber fraud Security Report, 2016).

Part of corporate governance is Internal Control which is a good practice for business as it provides managers with good information with which to make fair and accurate decisions. Internal control systems monitor and evaluate an organization's operations to ensure reliability of information systems to identify and report anomalies (Merchant and Van der Stede, 2007; Opromolla and Maccarini, 2010). Proper internal controls ensure effective and efficient operations that are in compliance with applicable laws and regulations (Spira and Page, 2003).

Proper Laws and Regulations go a long way in curbing criminal activities and providing justice where it is needed. Cyber fraud crime being a more recent trend and growing at an exponential rate seems to be out of the legal systems' reach. But some laws have been put in place like the Computer Misuse Act 1990 in the United Kingdom (UK) which is among the first of its kind to offer legal remedy for Cyber fraud crimes. This Act protects computer users from hacking: covering unauthorized computer access, unauthorized computer access with intend to commit an offence, and also unauthorized modification of data. It has been suggested that quality research and evaluation in criminal justice is important for policy development. Also, technological innovations can be very useful in policing and crime prevention and require training of those working in law enforcement, if they are to effectively tackle the problem of Cyber fraud crime (Welsh & Farrington, 2006; Braga, 2010; Stone and Travis, 2011).

The Government's Role is also very important in Cyber fraud security assurance especially for developing long-term strategies such as establishing information infrastructure. Currently, vulnerabilities and threats to the ICT infrastructure have increased risk to the economic environment. Criminals are able to skillfully attack computer systems and networks and cause damage to ICT infrastructure. This has brought attention to the security of information infrastructure and a reason for government to take strategic interest in national Cyber fraud security (Klein, 2008). The threat of Cyber fraud crime has led to the gradual adoption of Cyber fraud security services. In India for instance, Government had set up an Inter-departmental Information Security Task Force (ISTF) to deal with issues such as National information security threat perceptions; Public Key Infrastructure (PKI); Information security policy assurance and legal framework; research and technology development in information security; and nationwide Cyber fraud security education, training and awareness program (Holt and Lampke, 2010).

2.2.3 Challenges faced in Managing Cyber Fraud

Technological resources can get very expensive and can increase the cost of operations for a business. Cyber fraud -attacks only add into this cost through destruction of property or theft, and wastage of time as IT personnel spend time rectifying any problems created by Cyber fraud criminals. Other costs may come in the form of loss of customer trust and law suits against the company, in case these attacks target consumer personal information. On average banks will take at least 10 days to recover from a Cyber fraud -attack in addition to the cost of recovery. For instance in the Indian Banking Sector, USD four billion is lost in recovering from the crime and 3.6

billion USD is spent to combat such crimes from happening in future: while the average recovery time is 15 days (Muthukumaran, 2008).

Lack of resources is a great challenge especially in developing nations as massive resources are required to protect against Cyber fraud -attacks (Benjamin, 1990; Kshetri, 2010; Shandilya, 2011). For example, in the US a report by Homeland Security Press Release (2010) revealed that in 2009 a total of a billion dollars in federal stimulus funds was given to a dozen airports for upgrading baggage screening and checkpoint technology. In 2006, China spent over 3.4 billion USD on the development and implementation of CCTV systems (Klein, 2008). In great contrast, according to the Serianu-Kenya Cyber fraud Security Report (2016), 96 percent of organizations spend less than USD 5000 annually on Cyber fraud security.

Where laws are weak, Cyber fraud criminals thrive especially in developing nations where Cyber fraud security knowledge among law enforcement and regulatory institutions is inadequate (Kshetri, 2010). For instance in Kenya there is the ICT Sector Policy of 2006, the Kenya Information and Communications Act of 1998, and the Kenya Information and Communications regulations of 2010: despite these laws and regulations, the prosecution rate is still quite low and this is reflected in over Kes. 17 billion in losses to Cyber fraud crime. One of the reasons for inadequacy of Cyber fraud security bills, laws and processes could be that a high number of Cyber fraud crimes are not reported and those that are reported are rarely followed through to prosecution (Serianu-Kenya Cyber fraud Security Report, 2016).

Lack of Cyber fraud security knowledge and awareness poses a major challenge in the management of Cyber fraud. This has been observed in developing nations and it

affects individual members of the public as well as organizations. Cyber fraud criminals are increasingly trying to maintain a low profile and gain undetected access meaning there is a greater need to constantly upscale Cyber fraud technologies and techniques to effectively protect against Cyber fraud crime (Kshetri, 2010). The Serianu-Kenya Cyber fraud Security Report (2016) stressed on the need for Cyber fraud security education and awareness within the country. In Kenya there are low levels of Cyber fraud security awareness that have caused a great number of Cyber fraud -attacks to go unreported as people don't know how to handle them. An organization's capacity to respond to Cyber fraud crime depends on the awareness level of its members.

Another challenge is insider threat which affects the organization from within. This threat is brought on by the employees who intentionally attack the organization or are unintentionally used to commit Cyber fraud crime. The reasons for this could vary from espionage, organized crime, ignorance, opportunity or even out of greed. When it comes to espionage a competitor may use an employee as a spy to gain confidential information for competitive edge (Birbal and Taylor, 2005). Sometimes an employee may be part of an organized crime group that defraud a company and its customers for personal gain. A review by McGuire (2012) showed that 80 percent of Cyber fraud crime could result from some form of organized activity. The study further suggested that traditional organized crime groups were extending their activities to the digital world and their activities vary from purely online targets, use of online tools to enable crimes in the 'real' world, or a combination of both online and offline targets.

Serianu-Kenya Cyber fraud Security Report (2016) indicates that insider threat is the main cause of direct losses in Cyber fraud crime in Kenya. It indicates that over 80 percent of system related fraud and theft in 2016 was committed by employees and other insiders . It also noted that poverty due high unemployment rates in the region, pressured rogue employees within organizations to find extra means of income, hence turning to Cyber fraud crime. Whether motivated by poverty or greed, insider threat is increased when opportunity for malicious access into an organization's system network is provided. The report revealed some of these opportunities to be password sharing, employees bringing their own devices, privileged access, and system vulnerability. In system vulnerability it was noted that many organizations in Kenya were using obsolete systems and applications, unencrypted data protocols, misconfigured web servers, and use of default credentials.

2.3 Theoretical Review

This section discusses the theories on which this study is anchored. The study considers four guiding theories which include: rational choice theory The Fraud Triangle Theory, Agency Theory, and The Fraud Management Lifecycle.

2.3.1 Rational Choice Theory

Rational choice theory posits that cumulative social behavior results from the behavior of individual actor and choices (Homans, 1961). Homans(1961) maintains that choice in human being is centered on inclinations and constrictions.The philosophy in criminology observes man as an intellectual thespian who considers strategies and objectives, price and gains, and makes a sensible choice (Wittek, 2013). The key basics of all rational choice justifications are individual inclinations, opinions, and controls.

Inclinations represent the constructive or destructive evaluations persons attach to probable consequences of their actions (Wittek, 2013).

Wittek (2013), alludes that a community leader may have confidence that raiding one township may have a higher likelihood of triumph than raiding the other. According to Bauman et al (2021) the foundation for rational choice theory shoot from the logical theories of Cesare Beccaria and Jeremy Bentham. This theory is related to the classical school of criminology with the primary impression that individuals have unrestricted will, and can decide on how to act and respond to circumstances within their lives.

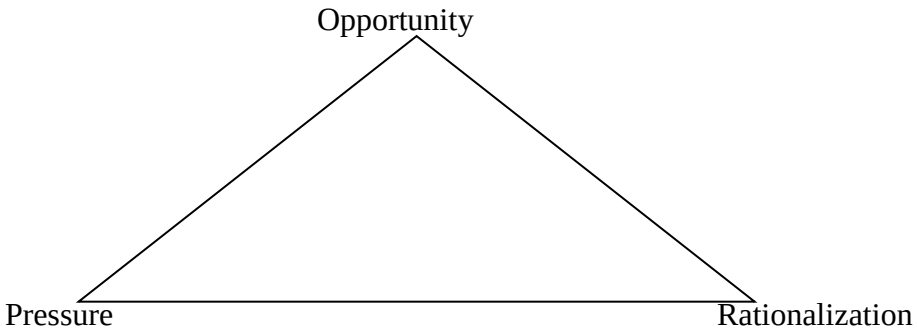
Rational Choice Theory helps the administration make the best-expected pronouncement, after bearing in mind several substitutions (Osinowo et al, 2021). Rational choice theory is a traditional concept in criminology, with deep roots in the Education. It has secured an advantaged place as a conventional criminological theory in the United States (Zhao et al ,2020). Ray et al (2020) suggests that individuals weigh risks and rewards when deciding whether to engage in offending and use accessible evidence, appraise illicit prospects grounded on the peril of the felony in contradiction of the latent plunders that conduct might produce.

The theory has made significant progress in social sciences, however its growth in sociology has been limited due to misunderstandings by the sociologists (Hechter &Kanazawa, 2020).This theory provides a wholistic frame work on Fraud Triangle Theory, Agency Theory, and Fraud Management Lifecycle used under the study to uncover the intentions behind the management of cyber fraud in commercial banks globally and by extension Kenya.

2.3.2 The Fraud Triangle Theory

This theory states that fraud is composed of three elements which are: Perceived Pressure Perceived Opportunity and Rationalization of the act of fraud (Albrecht, Albrecht, Albrecht and Zimbelman, 2009). This is shown in figure 2.1 below.

Figure 2.1: The Fraud Triangle (Albrecht *et al.*, 2009).



The theory assumes that for any act of fraud to take place all three elements have to be present and that these elements are interactive (Albrecht, Turnbull, Zhang, and Skousen, 2010). For instance, when an individual is under intense pressure probably from a personal problem (like financial debt) and perceives an opportunity (like being entrusted by an employer with treasury privileges), he/she may eventually rationalize that it is okay for them to use the company's money for their personal debt because they are in charge.

Pressure is considered as the incentive or motivation of the perpetrator to commit fraud. It can be due to some financial need (such as financial losses, debt, bills or gambling) or non-financial need (like greed; frustration at work; desire to report better results than actual performance; need to challenge the system; and so on). This

pressure may push an individual to take significant risks to obtain the desired resources (Rae and Subramaniam, 2008; Albrecht et al., 2009; Albrecht et al., 2010).

For fraud perpetrators to commit fraud there has to be some perception of opportunity which is a weakness in a system that he/she can exploit. These opportunities may be weak internal controls, vulnerable systems, poor performance quality, weak laws, ignorance, privileged access, and so on (Rae and Subramaniam, 2008; Albrecht et al., 2009; Cohen, Ding, Lesage, and Stolowy, 2011). Opportunities also arise when an employee gains too much trust from an organization that has weak or non-existent internal controls. Kelly and Hartley (2010) explain that the opportunity to successfully embezzle is created when an organization places trust in a few long term employees who gradually get more authority and freedom to make decisions and thus have more direct access to financial assets and an understanding of how the system works.

Rationalization is the justification of fraudulent behavior by the perpetrator. It involves the perpetrator considering that their actions are acceptable usually as a result of lack of personal integrity or other moral reasoning (Albrecht et al., 2009; Rae & Subramaniam, 2008). Some individuals feel they are deserving of an employer's assets and will allow themselves to commit a dishonest act knowingly and intentionally. Therefore, rationalization is dependent on an individual's personal code of ethics and thus a strong moral code can stop one from justifying fraudulent behavior (Cohen et al., 2011).

An organization's management can use the three elements of the fraud triangle to easily identify areas of its system vulnerable to fraud. Although the fraud triangle can be used to effectively predict patterns of fraud, this theory also has its

weaknesses. Fraud is complex and involves a combination of other factors. For instance it does not sufficiently explain the social and behavioral aspects of fraud like organized crime, predatory behavior and societal attitudes. It also does not address why incidences of fraud may occur with good internal controls in some cases, and may not happen in other cases although internal controls are poor (Rae and Subramaniam, 2008; Albrecht et al., 2010).

2.3.3 Agency Theory

Agency theory was first proposed by Jensen and Meckling (1976) who described it as a principal-agent relationship between shareholders as the principal and management as the agent. This theory borrows from economic models that argue that most people are motivated by self-interest and self-preservation. It therefore considers a situation where the personal interests of top management (agent) do not align with company and shareholder (principal) interests. According to Davis, Shoorman and Donaldson (1997) research on fraud shows that management commits crime because it is in their short-term, personal interest. It further suggests that in order to curb fraud and other deviant management behavior, incentives to management should align with shareholder goals, and the need to create controls to limit the opportunities for executives to maximize their own utility at the expense of shareholder interest.

Agency theory assumes that having an optimal control mechanism between the principal and agent is in the principal's best interest as management will not fulfill its duty to shareholders because it has a sense of ethical duty but because meeting the shareholders' requests will maximize management's utility (Eisenhardt,

1989; Donaldson & Davis, 1991). Agency theory is an effective tool for analyzing financial statement fraud; however, it only focuses on top management and ignores others non-management participants that also assist in committing fraud. Also, other than self-interest the theory does not consider other reasons for committing fraud.

2.3.4 The Fraud Management Lifecycle

The fraud management lifecycle consists of interrelated interdependent and independent actions functions and operations (Albrecht *et al.*, 2009). It is made up of eight stages that are considered in management of fraud. These stages are Deterrence, Prevention, Detection, Mitigation, Analysis Policy, Investigation and Prosecution.

Deterrence stage stops fraud before it happens by making it difficult for fraudters to commit fraud, creating fear of consequences and discouraging fraudulent activity from being attempted (Wilhelm, 2004; Kimani, 2011). Closely associated is the Prevention stage which occurs after deterrence has failed but before the suspicion or detection of fraud has been accomplished. Prevention is intended to provide security and protect an enterprise and its processes against fraud. Detection stage identifies and locates fraud before, during and after it takes place. It encompasses three activities: fraud testing, fraud attempts and fraud successes. Detection in all three areas are vital to provide the needed support for the rest of the stages by pointing out any vulnerabilities the fraudter may use (Wilhelm, 2004).

Once there is suspicion of fraud or it has been detected, the Mitigation stage begins with speedy reponse intended to lower the extend of damage, associated losses, cost of recovery, and also decrease the impact of the fraudulent activity. Therefore there

is a need to act as urgently as possible (Wilhelm, 2004; Albrecht *et al.,* 2009; Ledgerwood & White, 2006). Analysis is the next stage where impact of fraud management activities is evaluated by considering data on performance from the previous stages (that is deterrence, detection, prevention and mitigation stage activities) to provide the appropriate feedback for management to make informed, calculated and relevant decisions (Wilhelm, 2004). This leads to the Policy stage where fraud policies are developed and deployed to reduce the incidence of fraud and the inconvenience to legitimate customers and to allocate resources required to successfully combat it. In crafting fraud policies, the fraud management staff has to consider factors from both internal and external environment meaning they not only consider the fraud management department but also other departments within the enterprise and other participants from outside the enterprise. Therefore they leverage knowledge from all the different parts to address the fraud problem as a whole. Policy seeks to reduce losses, improve operational scalability and maintain cost effectiveness (Wilhelm, 2004; Wright, 2007).

The other stage is investigation whereby sufficient evidence and information is obtained so as to stop fraudulent activities; to prosecute and convict apprehended fraudters; and to recover assets or get restitution (Albrecht *et al.,* 2009). Wilhelm (2004) discussed three primary areas tha fraud investigations focus on: internal investigations, external investigations and law enforcement coordination. Internal investigations deal with employees, consultants and other contractors that work with the organization, while external investigations consider customers, organized crime groups, competitors and other entities outside the organization. Coordination of law enforcement according

to Gottschalk (2010) involves maintaining an effective relationship with law enforcement authorities and providing the necessary information and resources to them. This is finally followed by the Prosecution stage. Here prosecutorial and judicial authorities consider the evidence obtained during investigation and if sufficient use it to convict the fraudters. Thus there are three goals of prosecution regarding fraud: to prevent more theft by punishing fraudters; to defend and create awareness to a business' reputation of deterring fraud; and to obtain restitution or recovery where possible (Wilhelm, 2004; Albrecht et al., 2009). The fraud management lifecycle is a great process of protecting, identifying and keeping track of fraudulent activities within an organization and offering remedial restitution where affected. The lifecylce assumes that players at all stages participate accordingly and have resources to to manage fraud; but not many organizations can afford the resources to have an effective and efficient fraud management process especially when it comes to Cyber fraud crime fraud. Another issue would be investigation and prosecution stages require working with law enforcement authorities but without proper Cyber fraud laws or Cyber fraud awareness among law enforcement, it would prove almost impossible to get a conviction or any restitution.

2.4 Conceptual Framework

The conceptual framework in Figure 2.2 indicates that management of Cyber fraud is done through having reliable systems in place to fight the different forms of Cyber fraud that may attack the banks' computer network infrastructure. The security and systems in place should function to curb the diverse forms of Cyber fraud threats that are emerging in the online technology transactions in the banking sector. The introduction of online technology in the sector has exposed contemporary banking to Cyber fraud

attacks, but with proper infrastructural systems in place the bank should be able to mitigate, prevent and resolve the Cyber fraud threats from occurring. The systems and security used in management of Cyber fraud crime fraud are independent variables as they determine the penetration and effects Cyber fraud in the bank, while the solution to manage the challenges of Cyber fraud threats is the intervening variable that will dictate the impact of Cyber fraud crime fraud within the organization.

Figure 2.2: A conceptual framework illustrating the management of Cyber fraud in commercial banks.

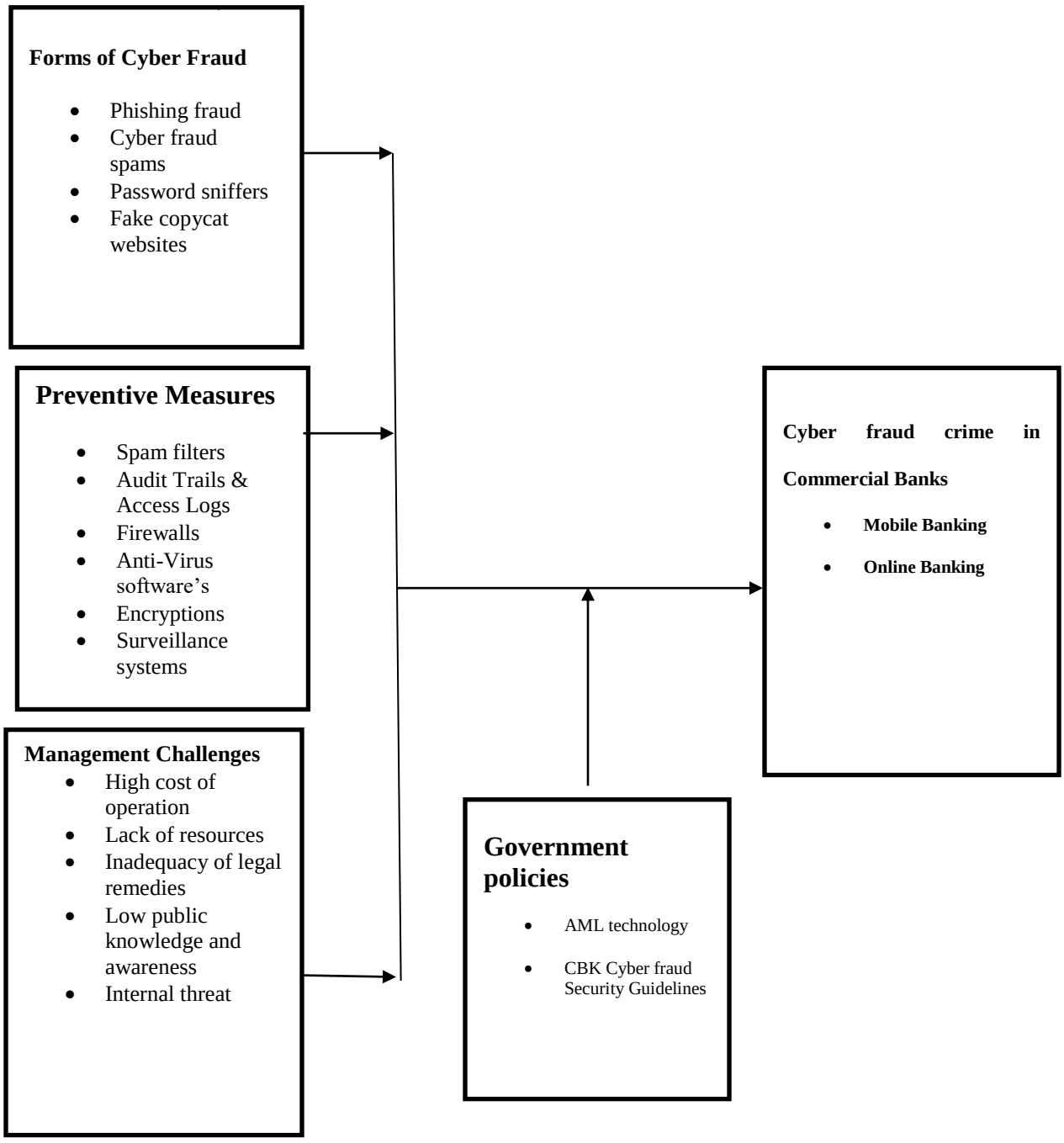


Figure 2.1: Conceptual Framework

CHAPTER THREE:RESEARCH METHODOLOGY

3.1 Research Design

The study employed qualitative approach as it was more elaborate in obtaining relevant data. A cross-sectional survey design was used as it was appropriate to determine in a short time-frame the current Cyber fraud management practices and was very useful in identifying common forms of Cyber fraud within the organization.

3.2 Site Description

Chase Bank Ltd is among the forty three commercial banks in Kenya and offers financial solution to SMEs, corporates and retail clients. The company was founded in 1995 and is based in Nairobi, Kenya. For over 20 years Chase Bank has been known as the “Relationship Bank” within the commercial banks. The bank provides a broad range of conventional and sharia’s compliant financing products through its vast branches found within Nairobi, Mombasa, Kisumu and Nakuru.

In 1997, the bank moved its headquarters to the capital city, Nairobi. The bank had branches strategic locations within the city: the City Centre, Village Market, Hurlingham, Parklands, Eastleigh and Riverroad. As the bank increased their presence countrywide, they went on to open more branches in Mombasa, Kisii, Eldoret, Narok, Garissa and Thika. In total the bank had 62 branches countrywide.

In April 2009, the bank was awarded 'Fastest Growing Bank' at banking awards 2009 while in December of the same year, the customer deposit figure crossed the Ksh. 10.2 billion mark. The Bank was awarded ISO 9001:2008 certification by Bureau Veritas. Chase Bank’s Board of Directors established a Credit Committee (CC),

consisting of certain members of the Chase Bank Board and certain officers of Chase Bank and this committee was given responsibility to establish the credit and lending policies of the Bank.

On 7th April 2016, Chase bank became the third lender in Kenya to go into receivership in less than twelve months after Imperial Bank and Dubai Bank closure. Chase Bank attracted too much attention owing to the fact that it was a second tier bank and home to a good number of individual clients, corporates and SMEs. The bank struggled with threat of closure as the rates of Cyber fraud s kept escalating. This study therefore sought to investigate the management of Cyber fraud s in Chase Bank.

The target population of the study was the management staff at the Chase Bank headquarters in Nairobi. This is the central office where Cyber fraud –crime management strategies are formulated and implemented and therefore would be possible to get responses within a reasonable time. The population included staff in the following eight (8) departments: Human Resource, Risk & Compliance, Forensics, Security, Information & Technology, Digital Banking, Internal Audit, and Transactional Monitoring department.

3.3 Sample Design

A census was carried out to cover the eight departments. At least one (1) respondent considered most knowledgeable in the area to provide information sought by this study was selected to represent each department. This technique was preferred because respondents were selected depending on experience and special knowledge of their roles in Cyber fraud management at Chase Bank. All the eight heads of departments were considered for the study and where

the head of department was not available the deputy head of department took their place. The overall respondents for the study were 8.

3.4 Unit of Analysis

The unit of analysis was Cyber fraud crime management at Chase Bank Ltd.

3.5 Unit of Observation

The units of observation for this study were the respective heads of departments who would provide specialised information regarding their departments. In the event where a head of department was not available for the interview, the deputy head was requested to step in as a key informant. The respondent was assumed to be knowledgeable in his/her department and have worked in the department for atleast two years.

3.6 Data Collection

Data collection was undertaken solely by the researcher through focused interviews with the aide of an interview guide and administration of questionnaires. The interviews were to be carried out on the heads of the respective departments that is Forensics, IT and Digital Banking to provide detailed information about Cyber fraud crime, while questionnaires were issued to the head of departments within each department to provide more information about their experiences in Cyber fraud management techniques. Therefore, three (3) face to face interviews and five (5) questionnaires were carried out. Each department's data collection instruments differed in questions asked due to differences in the nature and roles of each department. The research instruments contained both structured and non-structured questions. Likert type of questions were also used for purposes of enabling easy rating /ranking of answers,

coding and data analysis and a closing open ended section. The research instruments were divided into two major sections: the first section consisted of a brief background regarding the background information of Chase Bank which was the subject of the study. Section B focused on the management of Cyber fraud fraud in Chase Bank.

3.7 Validity and Reliability

To increase precision of responses, the interviews were face to face so as to read the body language and minimize deception. This method also minimized blank responses, ensuring the data instrument satisfied the researcher's questions. Questionnaires issued to departmental heads and their deputy head of department were to be answered individually and privately to improve objectivity by avoiding pressure from others. Also questionnaires were compared against each other to analyze for common responses within each department to increase the reliability of data obtained. For more informed data, only respondents with at least two (2) years of experience in their respective areas of expertise were selected for the study.

3.8 Data Analysis

Descriptive analysis was used to analyze the data and summarize the findings, because it is simpler for comparisons and identifying trends (Mugenda & Mugenda, 2003; Neuman, 2006). According to Cooper and Schindler (2006), descriptive studies describe characteristics associated with the subject population and help the researcher get the description of existing phenomena. Moreover, it explores the existing status of two or more variables at a given position in time and whether a relationship exists between them; hence most suited in investigating management of

Cyber fraud fraud in commercial banks in Kenya with a special focus on Chase Bank.

Collected data was manually entered into the computer through word processing tools like MS Excel and SPSS which helped the researcher to analyze the data. Data was presented using graphs, frequencies, percentages, means and other central tendencies. The use of differential statistics like percentages simplifies data and also translates it into a standard form for comparisons offering both qualitative and quantitative descriptions of the study (Cooper and Schindler, 2006).

3.9 Ethical Considerations of the Study

While undertaking this study, respondents were treated with respect. The researcher introduced themselves and sought permission to perform the research from the organization in focus. Respondents participated in this study voluntarily. A copy of the study was made available to the participating organization on request. Personal information of individuals was treated with confidentiality.

CHAPTER FOUR: DATA ANALYSIS, PRESENTATION AND INTERPRETATION

4.1 Introduction

This chapter presents research findings and discussion on management of Cyber fraud in Commercial Banks in Kenya where the main focus was on Chase Bank Limited. The discussion of the findings is guided by the objectives of the study. Attempts are made to explain why the findings are the way they are and to what extent they are consistent with or contrary to past empirical findings and theoretical arguments. It presents the general information from the respondents, gives the findings on forms of Cyber fraud, provides the results on the challenges faced in managing Cyber fraud and highlights the findings on the effects of technology in prevention of fraud.

4.2 Response Rate

The study targeted the management staff members working at the head offices of Chase Bank Limited in Nairobi. From this population, the study selected a sample of 8 respondents from the population census in collecting data with regard to management of Cyber fraud in Chase Bank Limited. The number of questionnaires administered was five (5) and three (3) interviews were to be carried out. All questionnaires were returned properly filled and three interviews were successfully carried out. This represented a successful response rate of 100% as indicated in Table 4.1.

Table 4.1: Response Rate

Response	Frequency	Percent
Returned questionnaires	5	62.5
Interviews conducted	3	37.5
Total	**8**	**100.0**

Source: Research Data, 2017

Mugenda and Mugenda (2012) assert that 50% response rate is adequate 60% is good while 70% and above is rated to be very good. From the foregoing the response rate provides adequate data to proceed with the analysis. The use of drop and pick method personal visits and follow-up telephone calls and e–mail communication to the respondents explaining the purpose of the study and its usefulness to the organization improved the response rate. This was supplemented with a letter of introduction and a letter of authority to conduct research in Chase Bank from the University of Nairobi.

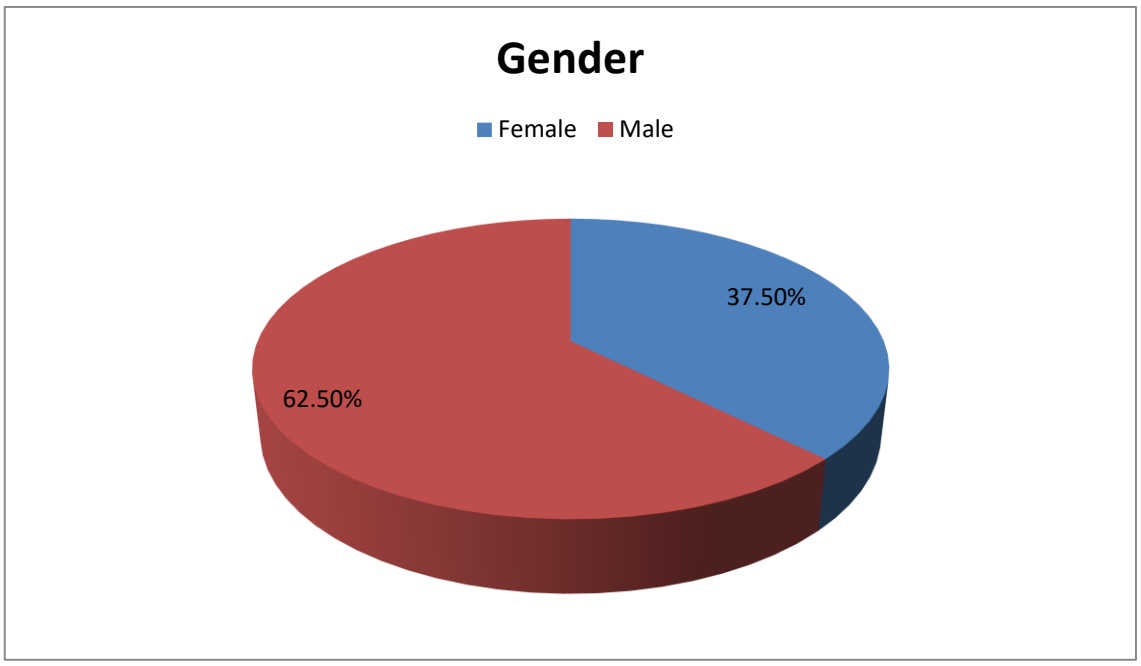
4.3 Demographic Characteristics

This section covers information describing the basic characteristics namely; gender, age bracket, years of service, level of education, designation and department of the respondents.

4.3.1 Gender of the Respondents

thestudy sought to establish the gender of the respondents who took part in the study. The respondents were expected to comprise both male and female staff members working in Chase Bank Kenya. The question of gender was considered important in the study primarily because it could help the researcher get a balanced view from both males and females.

Figure 4.1 Distributions by Gender



The findings in regard to gender revealed that 62.5% were males while 37.5% of them were females that is 3 female and 5 male. The findings show that Chase Bank has both male and female management staff members. However the male are more than the female management staff members in the technology departments. Chase Bank heaquarters in Nairobi had observed the gender rule to a moderate extent. The bank has 712 employees while senior management comprises of 75 employees. The total population of employees comprises of 331 males to 381 females (46% males to 54%

females), while in senior management there are 51 males to 24 females (68 % males to 32% females). The findings implied that the views expressed in these findings are gender sensitive and can be taken as representative of the opinions of both genders as regards to management of Cyber fraud in Chase Bank Kenya. The gender rule in Kenya stipulates that not more than two-thirds of the appointmentments or employment shall be of the same gender.

4.3.2 Age Bracket

The study sought to investigate the composition of the respondents in terms of age brackets to understand their familiarity with the management of Cyber fraud in Chase Bank Kenya. Table 4.2 shows the results obtained from the study.

Table 4.2 Distribution by Age Bracket

Age	Frequency	Percent
31-40 yrs.	5	62.5
41-50 yrs.	3	37.5
Total	**8**	**100.0**

As seen in Table 4.2, majority of the respondents (62.5%) were of age 31-40 years and the remaining 37.5% were of age 41-50 years. The results show that majority of respondents have a high level of information, responsibility and leadership potential which enhances the reliability and relevance of information collected. The study findings show that majority of the respondents were youthful young adults (31-40 yrs). Young (youthful) employees offer a cost-effective workforce since they are productive, more flexible, tech-savvy and innovative. The older employees (41-50 yrs.)

present experience, practical knowledge and expertise in the organization. It is important for a company to have the right mix between old and young.

4.3.3 Length of Service in the Organization

The respondents were asked to indicate their length of service in the bank. The years of practice are important in examining the reliability of the information collected from a given population under investigation. The results are presented in Table 4.3.

Table 4.3 Length of Service in the Bank

Service time	Frequency	Percent
2-5 yrs.	4	50.0
6-10 yrs.	4	50.0
Total	**8**	**100.0**

As shown in table 4.3, majority of the respondents had worked in the bank for a period of 2-5 years (50%) followed by 50% who had worked in the bank for 6-10 years. The results further show that the organization enjoyed services of the young, productive, as well as experienced employees. The fact that majority of the respondents had been in their departments for over two years, improves the reliable of the information given as the respondents were well knowledgeable on the forms of fraud experienced within the organization.

4.3.4 Level of Education

Like all other commercial banks in Kenya, Chase Bank employs staff members in different work stations hence different academic qualifications. The study thus sought to establish the highest academic qualifications attained by the respondents. The results are presented in Table 4.4 below.

Table 4.4 Highest Level of Education

Education	Frequency	Percent
Bachelors	2	25.0
Masters	6	75.0
Total	**8**	**100.0**

The study findings show that majority (75%) of the respondents indicated that they had acquired a Masters Degrees while 25% indicated that they had acquired Bachelor's Degrees. The minimum entry level of education in the banking sector is a degree. The study results show that majority of the employees were well educated; which means that they understood the questions asked on the subject matter. This improves the reliability of the information given by the respondents. Besides, some employees were still pursuing higher education to equip them with information on the changes in technology advancements and the ways to setup proper structures in their daily engagements.

4.3.5 Job title

The respondents were asked to indicate their job titles. The study sought to collect data from the heads of departments and or the managerial team working in Chase bank Kenya. As such, the study sample included Functional heads and deputy head of departments. This was relevant to assess the distribution of the respondents across the management levels. The results are presented in Table 4.5.

Table 4.5 Distribution by Designation

Designation	Frequency	Percentage
Functional heads	6	75.0
Deputy HOD	2	25.0
Total	**8**	**100.0**

As shown in Figure 4.5, majority of the respondents were functional heads (75%) while 25% were deputy head of departments in Chase Bank. The respondents picked from the management level due to their experience and knowledgeable, therefore had a broad understanding of the issues sought by the study. From these results, the respondents that participated in the study are mainly those involved in the formulation and implementation of the decisions concerned with management of Cyber fraud within the organization and hence their insights are viewed as more resourceful for knowledge and policy recommendations among Kenyan commercial banks.

4.4 Forms of Cyber Fraud

This section addresses the first objective of the study which sought to establish common Cyber fraud in Chase Bank. The address the objective, the respondents were asked to indicate the extent to which the bank experienced the various forms of Cyber fraud. Accordingly, the respondents were required to indicate the whether the bank implemented the Central Bank Policy Guideline to counter Cyber fraud.

4.4.1 Extent the Bank Experiences Cyber fraud Fraud

The respondents were asked to state the extent to which they experience Cyber fraud. This was the respondents' perception of the Cyber fraud they experienced based on the number of fraud noted by the bank. The results are presented in Table 4.6.

Table 4.6: Extent the Bank Experiences Cyber Fraud

Extent	Frequency	Percent
No extent	1	12.5
Little extent	3	37.5
Moderate extent	4	50.0
Total	**8**	**100.0**

As shown in table 4.6, most of the respondents (50%) were of the opinion that the bank experience Cyber fraud to a moderate extent and 12.5% of the respondents were of the view that the bank does not experience Cyber fraud. These results are an indication that commercial banks in Kenya experience Cyber fraud

to a significant level. This confirm to the audit report by PricewaterhouseCoopers- PwC (2011) which showed that fraud has risen from a peripheral issue for banks and other financial institutions to a top three issue that managers and supervisors have to deal with especially in the East African region.

4.4.2 Level the Bank Has Implemented the Central Bank Policy Guideline to Counter Cyber Fraud

The respondents were asked to indicate their perception on the extent to which Chase Bank had implemented the Central Bank Policy Guideline to counter Cyber fraud fraud. The findings are presented in Table 4.7.

Table 4.7: Level of Bank's Implementation of the CBK Policy Guideline to Counter Cyber fraud Fraud

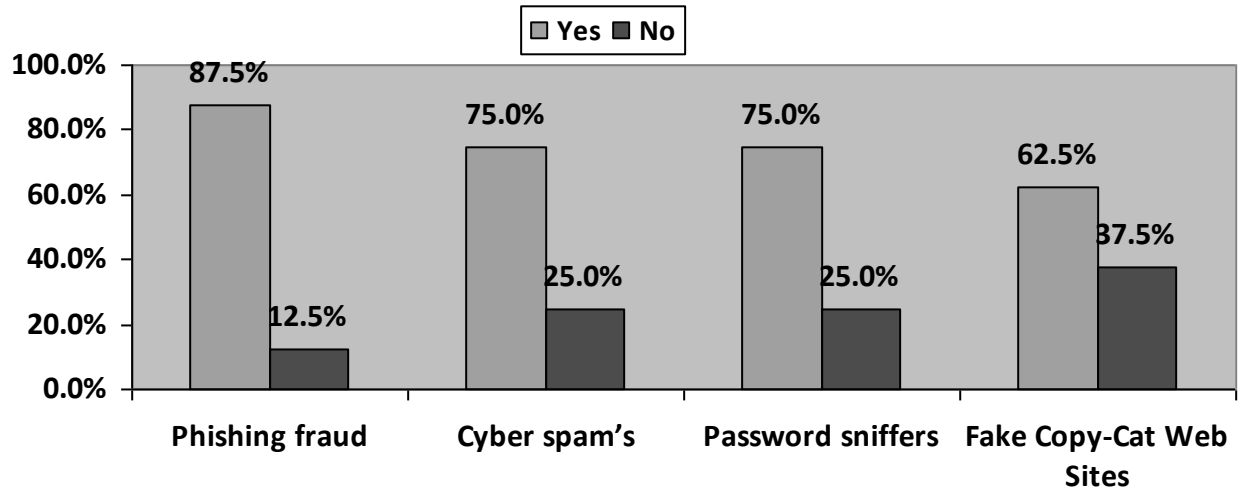
Extent	Frequency	Percent
Great extent	3	37.5
Very great extent	5	62.5
Total	**8**	**100.0**

The results presented in Table 4.7 show that most of the respondents were of the opinion that to a very great extent (62.5%), the bank has implemented the central bank policy guideline to counter Cyber fraud. At the same time 37.5% of the respondents felt that to a great extent bank has implemented the central bank policy guideline to counter Cyber fraud fraud. According to these results anti-fraud policy supported by effective procedure for prevention and detection are key weapons for the financial firms in the fight against fraud. Fraud control policies should provide guidelines on ways to reduce the risk of fraud.

4.4.3 Cyber Fraud Experienced

The respondents were asked to identify the Cyber fraud incidents experienced by the bank. The findings are shown in graph 4.1 below.

Graph 4.1: Cyber Fraud Incidents Experienced By the Bank



The results in Graph 4.1 above shows that of all the Cyber fraud listed, the banks has frequently experienced phishing fraud (87.5%), followed by Cyber fraud spam's and password sniffers (75.0%) and fake copycat web sites (62.5%) respectively. From these results, it is clear that there is a high number of Cyber fraud to Kenyan financial institutions due to the rising utilization of technological transactions that constitute internet banking, mobile banking, mobile transaction and cloud expansion.

4.4.4 Severity of the Cyber Fraud

The respondents were asked to indicate the degree of severity of the Cyber fraud identified. A five point likert scale was used whereby a mean score of 1 represent very small extent, 2 represent small extent, 3 represent moderate extent, 4 represent large extent and 5 represent very large extent. The study findings are presented in Table 4.8.

Table 4.8: Rating of Severity of the Cyber fraud Fraud

Cyber fraud fraud	Very Small Extent F	Small Extent F	Moderate Extent F	Large Extent F	Very Large Extent F	Weighted Total	Weighted Average
Phishing fraud	-	-	2	3	3	**33**	**4.1**
Cyber fraud spam's	-	-	1	4	3	**34**	**4.3**
Password sniffers	-	-	-	4	4	**36**	**4.5**
Fake Copy-Cat Web Sites	-	-	-	5	3	**35**	**4.4**

(Weighted average= $\frac{\Sigma WnFn}{\Sigma F}$ where $\sum$ is the summation of variables given, *W* is the weight given by our rating scale 1 to 5; *n* is the category to which each rate is allocated to e.g. very small extend, ..very large extend; *F* is the frequency given by number of respondents.) NB: Weighted mean has been rounded off to the nearest 1.

The study findings in Table 4.8 show that the respondents indicated that password sniffers were the most severe Cyber fraud crime occurrence within the organization with a weighted average of 5. The findings also show that fake copycat web sites, Cyber fraud spams and phishing fraud were severe in the bank to large extent. The results show that the respondents unanimously rated all the Cyber fraud to a level of great to very great extent. As per the findings Cyber fraud crime attacks are growing at a rapid rate and the financial institutions should have strong internal and external controls to keep their clients' money safe and their reputation within the industry.

The respondents were further asked to explain how the Cyber fraud influenced the management of Cyber fraud at the bank. The respondents indicated that theses Cyber fraud fraud have influenced the management of Cyber fraud in the bank through; auditing of the systems to identify any vulnerable, sensitization of staff on Cyber fraud ,

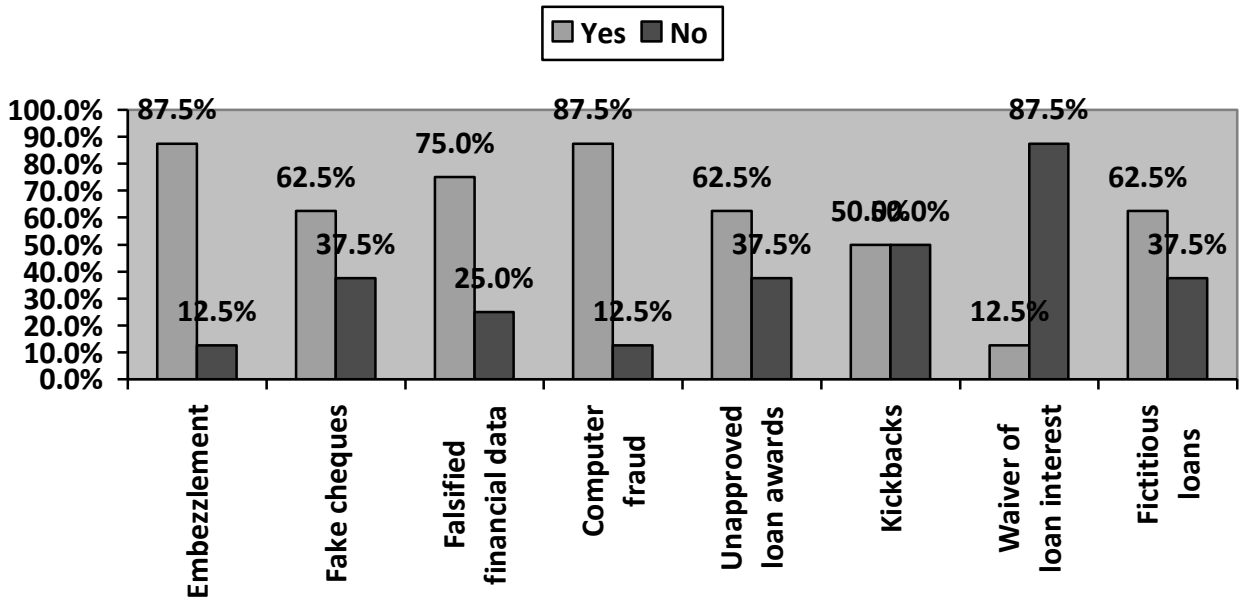
procurement of versatile IT securities infrastructures, use of CAPEX requirements and review policies on security. The local law enforcement agency lacks the technical expertise as well as sufficient regulatory powers and automated equipment to investigate complicated evidence collection because of intangible nature of Cyber fraud space and prosecute fraudulent digital transactions. Therefore lack of Cyber fraud space legal legislation provides a safe haven for Cyber fraud criminals.

The bank is therefore forced to setup its own stringent security protocols. In light of trying to protect corporate reputation, investor and public confidence most Banks are reluctant to report Cyber fraud -criminal activities, but quietly pick learnings rebuild from the attack by implementing controls to mitigate recurrence of the events. In the advent of advancement of technology, Banks have instituted layered security to cushion against various type of attacks e.g. at infrastructure level firewalls, setup of vlans, IP whitelisting, VPN tunnels, access control list, at application level SSL certificates, single sign on, addition of middleware within the network to prevent direct access to core banking applications.

4.4.5 Extent Various Forms of Fraud in the Bank Lead to Cyber fraud

The study also required the respondents to indicate the extent to which various aspects relating to Cyber fraud. The results are as depicted in Graph 4.2.

Graph 4.2: Extent Various Forms of Fraud in the Bank Lead to Cyber fraud



As shown in Graph 4.2 above, computer fraud and embezzlement significantly lead to Cyber fraud in the bank (87.5%), followed by falsified financial data (75%), fictitious loans, fake cheques and unapproved loan awards (62.5 %), kickbacks (50%) and waiver of loan interest (12.5%) respectively. From the findings, the prevalent fraudulent acts include; use of fake cheques and dividend warrants, issuing of unauthorized loans, posting of fake credits, defacing of cheques and defalcating, fraudulent transfers and withdrawals, loss of money to armed thieves and outright stealing of money.

4.4.6 Rating of Severity of the Fraud

The respondents were asked to rate the severity of the forms of fraud which led to Cyber fraud in the bank. A 1-5 Likert scale was used to interpret the results whereby a mean score of 1 represent very small extent, 2 represent small extent, 3 represent moderate extent, 4 represent large extent and 5 represent very large extent. The study findings are presented in Table 4.9.

Table 4.9: Severity Rating of Fraud

Forms of fraud	Very Small Extent	Small Extent	Moderate Extent	Large Extent	Very Large Extent	Weighted Average
	F	F	F	F	F	
Embezzlement	-	-	-	3	5	**4.6**
Fake cheques	-	1	5	2	-	**3.1**
Falsified financial data	-	-	1	2	5	**4.5**
Computer fraud	-	-	-	1	7	**4.9**
Unapproved loan awards	-	-	1	4	3	**4.3**
Kickbacks	-	-	-	2	6	**4.8**
Waiver of loan interest	-	-	2	4	2	**4**
Fictitious loans	-	-	1	4	3	**4.3**

(Weighted average= $\frac{\Sigma WnFn}{\Sigma F}$ where $\sum$ is the summation of variables given, *W* is the weight given by our rating scale 1 to 5; *n* is the category to which each rate is allocated to e.g. very small extend, very large extend; *F* is the frequency given by number of respondents.)

NB: Weighted mean has been rounded off to the nearest 1.

The findings in Table 4.9 show that the respondents rated embezzlement, falsified financial data, computer fraud and kickbacks were the most severe forms of fraud that led to Cyber fraud crime. This was followed by unapproved loans awards, waiver of loan interest and fictitious loans with the least severe being fake cheques. In summary other forms of banking fraud led to Cyber fraud crime incidents, they create loopholes that the hackers end up using to steal money from the bank.

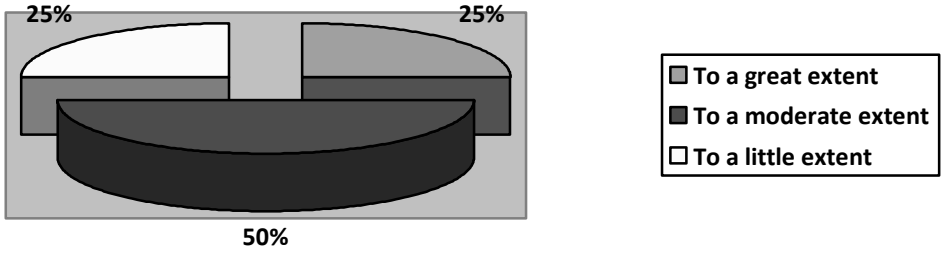
4.5 Challenges Faced in Managing Cyber Fraud

The study sought to establish the challenges faced by commercial banks in managing Cyber fraud fraud. With respect to Chase Bank, the respondents were required to indicate the extent to which commercial banks face challenges in managing Cyber fraud fraud. Mean and standard deviations have been used to present the findings.

4.5.1 Extent Commercial Banks Face Challenges in Managing Cyber Fraud

The respondents were asked to rate the extent commercial banks face challenges in managing Cyber fraud fraud. The respondents indicated their perception in regard to this question. The results are presented in Figure 4.2.

Figure 4.2: Extent Commercial Banks Face Challenges in Managing Cyber Fraud



The results show that majority of the respondents (50%) indicated that the bank faced challenges in managing Cyber fraud fraud to a moderate extent. However, 25% of the respondents revealed that the bank faced the challenges to a little extent, while another 25% indicated that the bank faced the challenges to large extent.

The respondents were further asked to indicate the challenges the bank managers faced in the management of Cyber fraud. The respondents indicated the

following challenges bank managers face in the management of Cyber fraud ; continuous changes in technology, complexity in detecting fraud on time, insider collusion/collaboration, minimal workforce, high cost of anti-Cyber fraud detection systems, limited technical tools, legal support, global interconnectivity and lack of understanding and support from management when implementing mitigation measures. Inadequacy of resources to keep abreast of advanced technology and lack of knowledge and awareness on Cyber fraud are major problems. Digital investigative challenges have been identified coupled with lack of Cyber fraud detection tools and technologies, and qualified personnel to carry out the investigations. There is insufficient legislation and law enforcement to address and tackle Cyber fraud cases.

From these results, a strong system of internal control is the most efficient way of fraud prevention. Cyber fraud mitigation efforts within many businesses are hampered by a combination of limited board and top management engagement in addressing Cyber fraud security, Cyber fraud challenges, limited resourcing, Cyber fraud capabilities, limited investigation and reporting of Cyber fraud incidents.

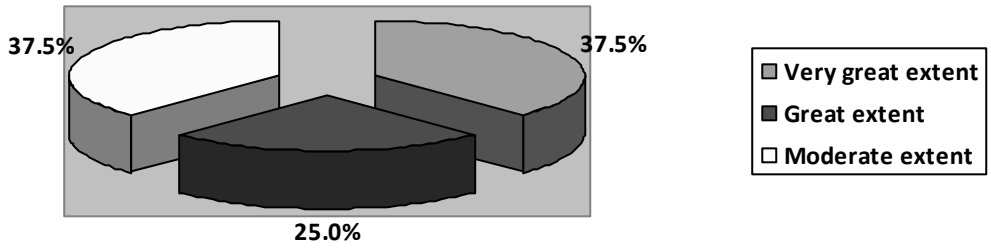
4.6 Impact of Technology in Preventing Fraud

This section covered the questions posed to the respondents on the impact of technology in prevention of fraud in the bank. The respondents were required to indicate the extent to which technology contributes to the rise of Cyber fraud in the bank. The respondents were also asked to rate the impact of technology in management of Cyber fraud.

4.6.1 Extent Technology Contributes to the Rise of Cyber Fraud in Commercial Banks.

The study also sought to establish the extent to which technology contributes to the rise of Cyber fraud in the bank. The findings are presented in Figure 4.3.

Figure 4.3 Extent Technology Contributes to the Rise of Cyber Fraud in Commercial Banks.



The study findings in Figure 4.3 show that 37.5% of the respondents indicated that technology contributed to the rise of Cyber fraud in commercial banks, to a very great extent. This was supported by 25% who indicated to a great extent. However, 37.5% of the respondents indicated technology contributed to the rise of Cyber fraud in commercial banks to a moderate extent. Fraud instigators are using technology to further fraudulent schemes and as it continues to advance unfortunately, the fraud then takes on many forms to be handled with any single application or approach. As technology becomes more advanced, fraudulent schemes will become more complex, while more sophisticated fraud solutions will be developed to combat hacker's best efforts.

4.6.2 Impact of Technology Management of Cyber Fraud

The respondents were asked to rate the impact of technology management of Cyber fraud. Mean was used to analyze the results. A five point Likert scale was used where 5 represents strongly agree, 4 represents agree, 3 represents not sure, 2 represents disagree and 1 represents strongly disagree. The findings are shown in Table 4.10.

Table 4.10: Impact of Technology in Management of Cyber Fraud

Statements	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree	Weighted Average
	F	F	F	F	F	
Technology has brought about challenges of online fraud and increased money laundering.	-	-	-	3	5	**4.6**
The technological surveillance systems are costly for the banks in management of fraud.	-	-	1	4	3	**4.3**
Implementation of advanced technological systems would save the cost of operations of banks.	-	-	-	5	3	**4.4**
The quality technology within commercial banks is a factor that may determine the level of security in terms of encryption as well as internal controls	-	-	-	1	7	**4.8**

(Weighted average= $\frac{\Sigma WnFn}{\Sigma F}$ where $\sum$ is the summation of variables given, *W* is the weight given by our rating scale 1 to 5; *n* is the category to which each rate is allocated to e.g. strongly disagree, ..strongly agree; *F* is the frequency given by number of respondents.)

NB: Weighted mean has been rounded off to the nearest 1.

As shown in Table 4.10, majority of the respondents strongly agreed that technology had brought about challenges of online fraud and increased money laundering; they further revealed that they strongly agreed that implementation of advanced technological systems would save the cost of operations of banks; and also that the quality of technology within commercial banks is a factor that may determine the level of security in terms of encryption as well as internal controls. Moreover, the respondents agreed that technological surveillance systems are costly for the banks in management of fraud.

In order to enhance management of Cyber fraud the respondents were of the opinion that constant training and update of the banks systems should be done daily as the attacks are sporadic, increased sensitization of staff and clients (to keep their PIN secret and never access their bank online platforms on any public WiFi's), embrace Cyber fraud systems, adopt best practices on IT security systems (COBIT) and continuously invest on research and development of robust systems to safe guard Cyber fraud fraud.

On what should be done to enhance management of Cyber fraud, the respondents suggested that employees in all departments to be conversant on set procedures, rules and guidelines in fraud mitigation in order to ensure cases of fraud are zero; the Bank should have a fraud risk officer who will be responsible of interpreting fraud and anti-money laundering policies to the employee so as to ease their understanding on the policies; the institution should have a framework that can facilitate information sharing between as it may assist in improving the recruitment of staff and also identify and lock-out blacklisted

employees form employment opportunities in the sector and the Bank should conduct adequate auditing on the system so as to mitigate risk.

Staff appraisals should consider fraud in measuring staff performance and rewards where staff members are made to understand the importance of controlling fraud to the overall performance of the organization. The Bank should also adopt advanced technology that would help in the deterrence and detection of fraud.

Utilize the youth and their ingenuity when it comes to technological advancements. Visits to Ethical Hacking forums and I-Hub can be eye openers. Instead of relying on reactive measures like whistleblowing, banks can and should take a more hands-on approach to fraud detection. By leveraging the power of data analysis software, banks can detect fraud sooner and reduce the negative impact of significant losses owing to fraud. Applications like splunk and SIEM Tools are examples of neural network setups with huge databanks of information for picking up trends. Usually such applications of neural networks systems involve knowing about the previous cases of fraud, to make systems learn the various trends.

4.7 Discussion

The study findings show that commercial banks in Kenya experience Cyber fraud to a significant level. The study found out that the major Cyber fraud experienced by the bank were phishing fraud, Cyber fraud spams, and password sniffers and fake copycat web sites. These findings conforms to those of Longe & Chiemeke (2008) who posited that add on to the list of Birbal and Taylor, (2005) acts such as Phishing, Cyber fraud

terrorism, Electronic spam mail, Cyber fraud stalking, and Copy-cat websites . The study further established various forms of fraud in the bank that led to Cyber fraud ; these include computer fraud, embezzlement, falsified financial data, fictitious loan, fake cheques and unapproved loan awards. These prevalent fraudulent acts and practices in the banking industry are similar to those noted by, Owolabi (2010), who set out the several types of fraudulent practices in the Nigerian industry. These include use of fake cheques and dividend warrants issuing of unauthorized loans posting of fake credits defacing of cheques and defalcating, fraudulent transfers and withdrawals, loss of money to armed thieves and outright stealing of money.

On the systems that the bank had put in place to prevent and manage Cyber fraud crimes, the study established that the bank was auditing of the systems to identify any vulnerability. The banks also sensitized the staff on Cyber fraud , procured versatile IT securities infrastructures and also used CAPEX requirements and review policies on security. These findings are in agreement with those of Beck et al. (2009) who found out that fraud Detection technology was on demand among institutions as banks invest in new systems and processes that make it difficult for criminals to target them. An example is the Anti-Money Laundering (AML) technology solution. These findings are also supported by Stafford (2013) who noted that banks across the globe are installing systems and technologies in response to Cyber fraud -attacks. The bank further implemented the central bank policy guideline to counter Cyber fraud fraud. The CBK Anti-fraud policy supported by other internal measures helped greatly in prevention and detection of fraud.

On the challenges facing the bank in dealing with Cyber fraud crimes, the study found out that the bank faced challenges in managing Cyber fraud to a moderate extent.

These included: continuous changes in technology, complexity in detecting fraud on time, insider collusion/collaboration, minimal workforce, high cost of anti-Cyber fraud detection systems, limited technical tools, legal support, global interconnectivity and lack of understanding and support from management when implementing mitigation measures. The above findings are in agreement with those of Muthukumaran (2008) who revealed that technological resources (systems) required for anti-Cyber fraud detection are very expensive and can increase the cost of operations for a business. These findings are also supported Shandilya (2011) who indicated that lack of resources especially for banks in developing nations is a great challenge, as massive resources are required to protect against Cyber fraud -attacks. According report by Kenya Cyber fraud Security (2016) also cited insider threat is the main cause of direct losses in Cyber fraud crime in Kenya.

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS.

5.1 Introduction

This chapter depicts the summary of the data findings on the effect of fraud risk management on performance of deposit-taking micro finance institutions in Kenya, the conclusions and recommendations are drawn there to.

5.2 Summary of the Findings

This section gives a summary of the findings on management of Cyber fraud in commercial banks in Kenya where the focus was on Chase Bank. The objectives of this study were to find out the forms of Cyber fraud commonly practiced in commercial banks; to establish the challenges faced by commercial banks in managing Cyber fraud; to evaluate the impact of technology in preventing fraud in commercial banks; and to determine the role of Cyber fraud fraud on management of Chase Bank.

The study found that commercial banks in Kenya experience Cyber fraud to a significant level. From the study, anti-fraud policies are supported by effective procedure for prevention and detection are key weapons for the financial sector firms in the fight against fraud. Chase Bank experiences Cyber fraud spam, phishing fraud and password sniffers to great extents while the Bank experienced fake copy-cat web site fraud to a moderate extent. It is clear that there are a high number of Cyber fraud to Kenyan financial institutions due to the rising utilization of technological transactions that constitute internet banking, mobile banking, mobile transaction and cloud expansion.

The study also found that computer fraud, falsified financial data, fake cheques and fictitious loans influenced management of Cyber fraud in Chase Bank to great extents. In addition, embezzlement, waiver of loan interest, unapproved loan awards and kickbacks influenced management of Cyber fraud in Chase Bank to moderate extents. The study found that commercial banks face challenges in managing Cyber fraud to a great extent. From the study information infrastructures, internal control, government role and structural challenges affect the management of Cyber fraud in Chase Bank to great extents while fraud detection and corporate governance challenges the management of Cyber fraud in Chase Bank to moderate extents.

The study found that technology contributes to the rise of Cyber fraud in commercial banks to a great extent. From the study, the quality technology within commercial banks is a factor that may determine the level of security in terms of encryption as well as internal controls, the Institution has a technological mechanism for monitoring transactions on a daily basis to detect occupational fraud, technology has also brought about challenges of online fraud and increased money laundering and the technological surveillance systems are costly for the banks in management of fraud.

5.3 Conclusion

The study concludes that commercial banks in Kenya face various forms of Cyber fraud. These Cyber fraud include phishing fraud, Cyber fraud spams, password sniffers and fake copy-cat web sites. These fraud have increasing due to the rising utilization of technological transactions that constitute internet banking, mobile banking, mobile transaction and cloud expansion. The Cyber fraud are executed in

various ways such as embezzlement, fake cheques, falsified financial data, computer fraud, unapproved loan awards, kickbacks, waiver of loan interest and fictitious loans.

The study concludes that a strong system of internal control is the most efficient way of fraud prevention. This is an implication that Cyber fraud mitigation efforts are hampered by a combination of limited board and top management engagement in addressing Cyber fraud security and Cyber fraud challenges, limited resourcing and Cyber fraud capabilities, and limited investigation and reporting of Cyber fraud . The study deduces that technology has a major impact on prevention of Cyber fraud.

5.4 Recommendations

This study recommends that banks should implement systems and structures that reduce the opportunities for fraud. In addition to strengthening internal control systems and structures, banks can use ICT tools to reduce opportunities or instill punitive measures for employees engaging in fraud and fraud related incidences.

In addition, this study recommends that banks should strictly adhere to due diligence rules and regulations imposed by the CBK on customers and employees. This will allow banks to have background knowledge on employees and customers. Where regulations on due diligence are not available, banks should develop custom made bank specific rules and regulations. In addition, these rules must be applied without exemption. This study further recommends that banks should engrain in their organizational culture: ethical practices in employees.

To reduce the cases of fraud in banks, this study recommends that ICT should be utilized as it is easy to track, easy to use and useful. The use of ICT will enhance accountability and transparency of employees as access to the system is tracked and recorded. Therefore cases of fraud are easily identified and culprits prosecuted. Indeed, ICT could be the cure to fraud in the banking industry. This could inform the rush by most banks to upgrade their core banking systems and card management systems.

In addition, this study recommends utilization of the youth and their ingenuity when it comes to technological advancements. Visits to Ethical Hacking forums and I-Hub can be eye openers. Instead of relying on reactive measures like whistleblowing, banks can and should take a more hands-on approach to fraud detection. By leveraging the power of data analysis software, banks can detect fraud sooner and reduce the negative impact of significant losses owing to fraud. Applications like splunk and SIEM Tools are examples of neural network setups with huge databanks of information for picking up trends. Usually such applications of neural networks systems involve knowing about the previous cases of fraud, to make systems learn the various trends.

5.5 Suggestions for Future Studies

This study focused on investigating management of Cyber fraud in commercial banks in Kenya where the focus was on Chase Bank. To validate the findings of this study, this study recommends that future studies be replicated in different banks or financial institutions. This could be undertaken in a large bank especially the top 5 banks in asset size in Kenya or the East African region.

Furthermore, a similar study using multiple banks could also provide substantive literature for comparison. This could provide literature for comparison to the findings of this study.

In addition, this study recommends research on the impact of Cyber fraud on bank performance. Though it is generally perceived to be negative, the magnitude or extent of the impact has not been examined and this could provide literature on how Cyber fraud affects various performance indicators of the Bank.

Finally, this study recommends a research on the impact of Cyber fraud management policies on bank performance. The Central Bank of Kenya, Kenya Bankers Association and the International Financial Reporting Standards all impose regulations on the type, form and frequency of reporting of banks. This has led to the reduction of Cyber fraud management. These regulations could have a positive effect on bank performance. Furthermore, the introduction of these policies could lead to the reduction of other forms of Cyber fraud.

REFERENCES

Albrecht, W.S., Albrecht, C.O., Albrecht, C.C., & Zimbelman, M.F. (2009). *Fraud Examination (3rd ed.)*. Nashville, TN. South-Western College Pub.

Albrecht, C., Turnbull, C., Zhang, Y., & Skousen C.J. The relationship between South Korean chaebols and fraud: *Management Research Review* 33 (3) (2010), 257-268.

Beck, T., Demirguc-Kunt, A., & Levine, R. (2009). Financial institutions and markets across countries and over time - data and analysis. *Policy Research* (Working Paper Series 4943).

Birbal R., & Taylor M. (2005). *Log on to IT for CSEC*. England. Pearson Education Limited.

Braga Anthony A. Setting a Higher Standard for the Evaluation of Problem-Oriented Policing Initiatives: *Criminology & Public Policy* 9 (1) (2010), 173-182.

Cameroon, D. (2011) Cyber fraud costs UK 27 Billion pounds, *Reuters media briefs*.

Central Bank of Kenya- CBK. (2017). *Draft guidance note on Cyber fraud risk*. Nairobi, Kenya.

Central Bank of Kenya- CBK. (2013). *Supervision Annual Report*. Nairobi, Kenya.

Chase Bank Limited (IR). (2017). About Chase Bank Kenya Limited. Retrieved from https://www.chasebankkenya.co.ke

Cohen J., Ding Y., Lesage C., & Stolowy H. Corporate Fraud and Managers' Behaviour: Evidence from the Press. *Journal of Business Ethics* 95 (2) (2010), 271-315. Springer, Netherlands.

Cooper D. R. & Schindler P.S. (2006). *Business Research Methods*. McGraw-Hill Irwin. Pennsylvania. Crane, D. (Producer), & Kauffman, M. (Producer). (1994–2004). *Friends* [Television Series]. Burbank, CA: NBC.

Davis, J.H., Schoorman, F.D., & Donaldson, L. The Distinctiveness of Agency Theory and Stewardship Theory. *The Academy of Management Review* 22 (3) (1997), 611-613.

Donaldson, L., & Davis, J.H. Stewardship Theory or Agency Theory: CEO governance and shareholder returns. Australian Journal of Management 16 (1) (1991), 49-64.

Douglas, T., & Loader B. Cyber fraud crime: Law enforcement, security and surveillance in the information age. *Journal of Social Policy* 30 (1) (2000), 300.

Eisenhardt, K.M. Agency Theory: An assessment and review. *Academy of Management Review* 14 (4) (1989), 532-550.

Fatima, A. E-Banking Security Issues: Is there a solution in biometrics? *Journal of Internet Banking and Commerce* 16 (2) (2011).

French, A. (2009). Cyber fraud crime: Conceptual Issues for Congress and U.S. Law Enforcement (CRS Report R42547. Washington, DC)

Greenberg, D.F., & Roush, J.B. The Effectiveness of an Electronic Security Management System in a Privately Owned Apartment Complex. *Evaluation Review* 33 (1) (2009), 3-26.

Gottschalk, P. Categories of Financial Crime. *Journal of Financial Crime* 17 (4) (2010), 441-458.

Guillaume, L.F., & Fortinet, F. (2009): *Fighting Cyber fraud crime: Technical, Juridical and Ethical Challenges*. Virus Bulletin Conference Genève - Switzerland, 2009.

Halder, D., & Jaishankar, K. (2011). *Cyber fraud and the Victimization of Women: Laws, Rights, and Regulations*. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.

Hankin, A., Hertz, M., & Simon, T. Impacts of Metal Detector Use in Schools: Insights from 15 years of research. *Journal of School Health* 81 (2) (2011), 100-106.

Hier, S.P. Risky Spaces and Dangerous Faces: Urban surveillance, social disorder and CCTV. *Social and Legal Studies* 13 (4) (2004), 541-554.

Holt,T.J., & Lampke, E. Exploring Stolen Data Markets Online: Products and market forces. *Criminal Justice Studies* 23 (1) (2010), 33-50.

Hutchinson, D., & Warren, M. Security for Internet Banking: A framework. *Logistics Information Management* 16 (1) (2003), 64-73.

Jensen, M.C., & Meckling, W.H. Theory of the Firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics (JFE)* 3 (4) (1976), 151-174.

Kagwe, M. (2016). The Proposed Cyber fraud Security and Protection Bill. Kenya Law

Kelly, P., & Hartley C.A. Casino Gambling and Workplace Fraud: A cautionary tale for managers. *Management Research Review* 33 (3) (2010), 224-239.

Khanna, A. & Arora, B. A study to investigate the reasons for bank fraud and the implementation of preventive security controls in Indian banking industry. *Int. Journal of Business Science and Applied Management* 4 (4) (2009).

Kimani, J. (2011). Fraud Risk Assessment Plan for Barclays Bank of Kenya. Bachelor's Project. Tampere University of Applied Sciences.

Klein, P.G. Opportunity Discovery, Entrepreneurial Action and Economic Organization. *Strategic Entrepreneurship Journal* 2 (3) (2008), 175-190.

Kochems, A. & Keith, L. Successfully Securing Identity Documents: A Primer on Preventive Technologies and ID Theft. *Backgrounder.* The Heritage Foundation. (No. 1946) (2006), 1-8.

Kshetri, N. Diffusion and effects of Cyber fraud in developing economies. *Third World Quarterly* 31 (7) (2010), 1057-1079.

Lawson, J. (Ed.), Jarvis. A., Blundell P., & Reid M.K.. (2004). Software Development with Java. For the e-Quals IT Practitioner Diploma- Level 2. Oxford. Heinemann Educational Publishers.

Ledgerwood, J., & White, V. (2006). *Transforming Microfinance Institutions: Providing full financial services to the poor*. World Bank. Washington DC.

Litan, A. (2004). *Phising attack victims likely targets for identity theft*. Available: http://www.gartner.com

Littman, J. (1997): *The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Paulsen.* Boston: Little Brown.

Longe, O.B., & Chiemeke, S.C. Cyber fraud crime and Criminality in Nigeria: What roles are internet access points in playing? *European Journal of Social Science* 6 (4) (2008), 132- 139.

Long, P., Millbery, G., & Stuart, S. (2008). *OCR ICT for AS (1st ed.).* London. Hodder Education.

Maat, S.M. (2004). Cyber fraud Crime: A comparative law analysis. Master's Project. University of South Africa.

Mazerolle, L.G., Kadleck C., & Roehl J. Controlling drug and disorder problems. *The role of place managers* 36 (2) (1998), 371-404. McCarthy, B., Hagan, J., & Cohen, L. E. (1998). Uncertainty, Cooperation, and Crime: Understanding the Decision to Co-offend. *Social Forces*, *77*(1), 155–176.

McGuire, M. (2012). *Organized Crime in the Digital Age*. Detica/ BAE and John Grieve Centre for Policing and Security. London.

Merchant, K.A., & Van der Stede, W.A. (2007). *Management control systems: Performance Measurement, Evaluation and Incentives (2nd ed.).* England. Pearson Education Limited. Moran, R. (1996). Bringing Rational Choice Theory Back to Reality. *The Journal of Criminal Law and Criminology (1973–), 86*(3), 1147–1160

Mugenda, O., & Mugenda, A. (2003). *Research Methods Qualitative and Quantitative Approaches*. Nairobi. Acts Press

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

Neuman, W.L. (2006). Social research methods. *Qualitative and quantitative approaches (6th ed.).* Boston: Allyn & Bacon.

Opromolla G., & Maccarini, M. The Control System in the Italian Banking Sector: Recent changes in the application of legislative decree no. 231 of June 8, 2001. *Journal of Investment Compliance* 11 (2) (2010), 16- 22.

Outa, G., Etta, F., & Aligula, E. (Eds.). (2006). *Mainstreaming ICT: Research Perspectives from Kenya*. Nairobi, Kenya. Mvule Africa Publishers.

Paternoster, R., & Pogarsky, G. (2009). Rational Choice, Agency and Thoughtfully Reflective Decision Making: The Short and Long-term Consequences of Making Good Choices. *Journal of Quantitative Criminology, 2*, 103–127.

Price Water House Coopers (PWC) (2012). Financial Focus, Risk and Regulation, Available: http://www.pwc.com/ke/FinancialFocus.

Rachna D., Tygar, J.& Hearst, M. (2006): Why Phishing Works in the Proceedings of the Conference on Human Factors in Computing Systems (CHI2006)

Rae, K., & Subramaniam, N. Quality of Internal Control Procedures: Antecedents and moderating effect on organizational justice and employee fraud. *Managerial Auditing Journal* 23 (2) (2008), 104-124.

Saul, H. (2007). Social network launches worldwide spam campaign. *New York Times*

Schmalleger, F. & Pittaro M. (2009) *Crimes of the Internet*. Pearson Prentice hall.

Serianu. (2016). Kenya Cyber fraud Security Report. Serianu Cyber fraud Threat Intelligence Team in partnership with USIU's Centre for Informatics Research and Innovation (CIRI), School of Science and Technology. Nairobi.

Shandilya, A. (2011) Online Banking: Security Issues for Online payment Services. www.buzzle.com/articles

Spira, L., & Page, M. Risk Management: the reinvention of internal control and the changing role of internal audit. *Accounting Audit and Accountability Journal* 16 (4) (2003), 640- 661.

Stafford, P. (2013). Cyber fraud Crime Threatens Global Financial System. Available at: http://www.ft.com/cms/s/0/9804988c-3722-11e3-9603-00144feab7de.html#axzz2tMwSTsmF

Stone, C., & Travis, J. (2011). *Towards a New Professionalism in Policing: New perspectives in policing bulletin.* U.S. Department of Justice, National Institute of Justice, 2012. NCJ 232359. Washington, DC.

Tagert, A. (2010). Cyber fraud security Challenges in Developing Nations. Dissertation. Carnegie Mellon University. Retrieved from: http://repository.cmu.edu

Wada, F. & Odulaja, G.O. Electronic Banking and Cyber fraud Crime In Nigeria - A Theoretical Policy Perspective on Causation. *African Journal of Computing & ICT* 5 (1) (2012), 69-82.

Wall, D.S., ed. (2001). *Crime and the Internet*: Routlege. New York.

Welsh, B.C., & Farrington, D.P. Crime Prevention and Hard Technology: The case of CCTV and improved street lighting. *The New Technology of Crime, Law and Social Control* (2007), 81-102 NCJ-218026. Available at: http://www.criminaljusticepress.com.

Wilhelm, W. K. The Fraud Management Lifecycle Theory: A Holistic Approach to Fraud Management. *Journal of Economic Crime* 2 (2) (2004), 1-38.

Wittek R. (2013). Theory in Social and Cultural Anthropology Publisher: Sage

Wright, R. Developing effective tools to manage the risk of damage caused by economically motivated crime fraud. *Journal of Financial Crime* 14 (1) (2007), 17 – 27.

APPENDICES

Appendix I: Introduction Letter

Dear respondent,

RE: DATA COLLECTION

I am a postgraduate student at the University of Nairobi pursuing a Degree in Master Criminology and Social Order. As a requisite for the degree award, am carrying out a study on **Management of Cyber fraud - Fraud in Commercial Banks in Kenya A Case of Chase Bank.** You and your organization have been selected to participate in this study. The attached questionnaire has been designed to help gather data from respondents. In respect to this you have been identified as one of the respondents.

Therefore, I kindly request you to facilitate the collection of the necessary data by answering the questions as precisely and factually as possible. This information sought is purely for academic purposes and this I assure you of strict confidentiality of the information given.

Yours faithfully

NYAMWARO N. BONARERI

MA Student

UON

Appendix II: Research Questionnaire

This questionnaire consists of two major sections (Sections A and B). Kindly respond to all questions by putting a tick [√] in the box matching your answer or write your answer in the space provided if it is not included in the choices. The information given here will only be used for purposes of academic study and will be treated with utmost confidentiality. Your cooperation will be highly appreciated.

SECTION A: BACKGROUND INFORMATION

1) Gender

Male	[ ]	Female	[ ]

2) Age Bracket

21-30 years	[ ]	31-40 years	[ ]
41-50 years	[ ]	Above 51 years	[ ]

3) How long have you served in the Organization?

Less than 2 years	[ ]	2 – 5 Years	[ ]
6 – 10 Years	[ ]	11-15 Years	[ ]
20 Years and above	[ ]		

4) What is your highest level of education?

Certificate	[ ]	Diploma	[ ]
Bachelor's Degree	[ ]	Masters	[ ]
PhD	[ ]	Others (Specify.....)	[ ]

5) What is your designation?

Functional heads [ ] Deputy HOD [ ]

SECTION B: FORMS OF CYBER FRAUD FRAUD

6) To what extent does your bank experience Cyber fraud fraud?

To a very great extent	To a great extent	To a moderate extent	To a little extent	To no extent

7) To what level has your Bank implemented the Central Bank Policy Guideline to counter Cyber fraud fraud?

To a very great extent	To a great extent	To a moderate extent	To a little extent	To no extent

8) a) In the Cyber fraud crime fraud incidents experienced in this bank, have you experienced any of the following forms of Cyber fraud crime?

Forms of Cyber fraud Fraud	Yes	No
Phishing fraud		
Cyber fraud spasm		
Password sniffers		
Fake Copy-Cat Web Sites		

b) If yes, how do you rate their severity on a scale of 1-5 where 1=very small extent, 2=small extent, 3=moderate extent, 4=large extent and 5 very large extent.

Forms of Cyber fraud Fraud	**1**	**2**	**3**	**4**	**5**
Phishing fraud					
Cyber fraud spasm					
Password sniffers					
Fake Copy-Cat Web Sites					

9) In your opinion, explain how some of the forms of Cyber fraud fraud that have influenced the management of Cyber fraud fraud at your bank? ……

……

……

10) a) Do the following forms of fraud in the bank lead to Cyber fraud crime?

Other forms of fraud	Yes	No
Embezzlement		
Fake cheques		
Falsified financial data		
Computer fraud		
Unapproved loan awards		
Kickbacks		
Waiver of loan interest		
Fictitious loans		

b) If yes, how do you rate their severity on a scale of 1-5 where 1=very small extent, 2=small extent, 3=moderate extent, 4=large extent and 5 very large extent.

Aspects relating to Cyber fraud fraud	**1**	**2**	**3**	**4**	**5**
Embezzlement					
Fake cheques					
Falsified financial data					
Computer fraud					
Unapproved loan awards					
Kickbacks					
Waiver of loan interest					
Fictitious loans					

SECTION C: CHALLENGES FACED IN MANAGING CYBER FRAUD FRAUD

11) With regard to this Bank, to what extent do commercial banks face challenges in managing Cyber fraud fraud?

To a very great extent	To a great extent	To a moderate extent	To a little extent	To no extent

12) In your opinion, what challenges do the bank managers face in the management of Cyber fraud fraud in your Bank? ……

……

……

……

13) What are the other aspects of challenges faced in management of Cyber fraud fraud that you would like to share with us? …….

……

……

……

SECTION D: THE IMPACT OF TECHNOLOGY IN PREVENTING FRAUD

14) With regard to Chase Banks, to what extent does technology contribute to the rise of Cyber fraud fraud in commercial banks?

To a very great extent	To a great extent	To a moderate extent	To a little extent	To no extent

15) What is your level of agreement with the following statements on the impact of technology in management of Cyber fraud fraud? Use a scale of 1 to 5 where strongly agree=5, agree=4, not sure=3, disagree=2 and strongly disagree=1

Impact of technology in management of Cyber fraud fraud	**1**	**2**	**3**	**4**	**5**
Technology has brought about challenges of online fraud and increased money laundering					
The technological surveillance systems are costly for the banks in management of fraud					
Implementation of advanced technological systems would save the cost of operations of banks					
The quality technology within commercial banks is a factor that may determine the level of security in terms of encryption as well as internal controls					

16) What other information would you like to share about management of Cyber fraud fraud in commercial banks in Kenya? ……

……

17) What do you think should be done to enhance management of Cyber fraud fraud in commercial banks in Kenya?

……

……

Thank You for Your Time!

Appendix III: Key Interview Guide

1. What are the forms of Cyber fraud crime fraud you face in the bank
2. How often have you experienced these forms of Cyber fraud crime fraud
3. In your opinion, explain how some of the forms of Cyber fraud fraud has influenced the management of Cyber fraud fraud at chase bank?
4. What mechanisms has the bank employed to reduce the risk of Cyber fraud crime fraud
5. What challenges does this bank face with regard to managing Cyber fraud fraud?
6. With regard to Chase Banks, how does technology contribute to the rise of Cyber fraud fraud in commercial banks?
7. What other information would you like to share about management of Cyber fraud fraud in commercial banks in Kenya?
8. What do you think should be done to enhance management of Cyber fraud fraud in commercial banks in Kenya?

Thank You for Your Time!