EFFECT OF CYBER SECURITIES STRATEGIES ON IMPLEMENTATION OF ONLINE BANKING: A SURVEY OF COMMERCIAL BANKS IN KENYA

BY

ODHIAMBO MOSES OLUOCH

A RESEARCH PROJECT REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION, SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI

2018

DECLARATION

This Research is my original work and has not, wholly or in part, been presented for an award of a degree in any other university.

Signature:______________________________ Date:________________________

ODHIAMBO MOSES OLUOCH

D61/85765/2016

This project has been presented for the purpose of examination with my approval as University of Nairobi Supervisor.

Signature:______________________________ Date:________________________

DR. KENNEDY OGOLLAH

Department of Business Administration,

School of Business,

University of Nairobi

ACKNOWLEDGEMENT

I would really like to return honor and glory to the Almighty God for granting me the strength and opportunity to pursue this course. It is through his mercies and kindness that has seen me throughout the entire research project.

I sincerely want to admit that this project would not have been a success ,were it for the support of my supervisor Dr. Kennedy Ogollah for his continues guidance, dedication, overwhelming support and advice, am really thankful.

My appreciation also goes to lecturers and Nairobi University Fraternity for offering me this opportunity and molded me through the knowledge they impacted that has saw me to the end. To My parents, words are not enough to describe my indebtedness to my parents who have sacrificed so much and inculcated a sense of achievement in me at a very early age providing the foundation of what has helped me become and placed on the path where I am today.

Last but not least I owe my deepest gratitude to my wife Mary Apondi, my daughter Michelle and my friends for their patience, continued love and sacrifice throughout the course and for offering unconditional love and support every minute.

DEDICATION

First and foremost, I dedicate this project to one and Almighty God, without whom this research would have been impossible to conduct.

Secondly I dedicate this research with a lot of love to my parents and family, who gave me total support during this research period.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

ATM:	Automated Teller Machines
CIS:	Computer Information Security
EN:	Enterprise Network
FATF:	Financial Action Task Force
IT:	Information Technology
ICT:	Information Communication Technology
KBA:	Kenya Bankers Association
OCC:	Office of the Controller of the Currency
PIN:	Personal Identification Number
PC:	Personal Computer
TAM	Technology Acceptance Model.
WAN:	Wide Area Network

ABSTRACT

The advancement in technology has led to a swift in the way banking sector operates. Clients no longer need to visit banking hall to transact but instead conduct their transaction at the comfort of their homes using online banking services. On the other hand, these developments have been accompanied by increase in cybercrime committed through these channels, hence the need to conduct a study about the effects of cyber security strategies on online banking implementation. A cross sectional survey of 41 Banks in Kenya was done. The research study was motivated by the need to establish the cyber threats facing the commercial banks in Kenya, countermeasures being adopted and how effective these strategies are in managing the cyber threats faced by commercial bank in Kenya. Banking sector in Kenya are under intense pressure to offer their customers quality products and convenience. In order to achieve this, they have adopted new technologies such as online banking to meet increasing customers need and improve on convenience. With the adoption of these new innovations commercial banks have become more vulnerable to cyber-attacks resulting to huge losses of their capitals through online theft and systems hacking. This increasing trend has triggered the need to investigate the causes and the strategies than can be used to curb these types of online fraud. The aim of this study was to establish the effects created by cyber security strategies on online banking implementation within Commercial Banks in Kenya. A cross sectional survey targeting ICT officers and staffs managing online transactions was carried out in 41 commercial banks in Kenya selected randomly from a population of 41 Commercial Banks in Kenya. Out to 41 commercial banks, we managed to get feedback from 31 respondents who managed to completed survey questionnaire giving a response rate of 75.6%. The main instrument for the survey was a questionnaire. The form data analysis used was descriptive statistics. The research study conducted to assess the effect of cybercrime security strategies in commercial banks in Kenya. To achieve this several variables were analyzed such as risk management systems, ICT infrastructures and level of employee awareness and competence handle cybercrime. Others aspects analyzed included regulation in terms of bylaws, policies, staff training among others. IT department was identified as the key areas data collection. Most of the information gathered directly touched on the policies, controls and security strategies employed by ICT departments. The study proposed several security areas that commercial banks need to improve on. These include access permission control mechanisms. Commercial banks should only give access once proper authentication has been done. Secondly, commercial banks need to be on the forefront in conducting security training within internals staffs and external client as well. Finally the study recommends that keen attentions should be taken when handling social engineering issue since threat is the areas that most hacker finds it easy access into the organizations systems.

CHAPTER ONE: INTRODUCTION

The chapter discusses the advancement in technology which has led to a swift in the way banking sector operates. Clients no longer need to visit banking hall to transact but instead conduct their transaction at the comfort of their homes using online banking services. On the other hand, these developments have been accompanied by increase in cybercrime committed through these channels, hence the need to conduct a study about the effects of cyber security strategies on online banking implementation.

1.1 Background of the Study

Technology is rapid becoming a very powerful means of promoting growth, innovation, developments and improving competitiveness (Kamel, 2005). Information Communication Technology (ICT) developments has enhanced innovation and created customer reactiveness and convenience in the banking industry (Loonam & O'Loughlin, 2008). These advancements in technology have seen financial institutions invent and adopt new systems that maximize the use of modern technology such as electronic transaction (Amboko & Wagoki, 2012).However, these new advancements in technologies come with challenges such as increase in cybercrime which is rampant in the banking sector.

This is due to systems vulnerabilities which permit unlawful access and modification, compromising of reliability, accessibility and privacy of the ICT systems. It is therefore sensible that conscientiousness and due care be observed to guarantee proper national information security management (Kitheka, 2013).Cybercrime security issues is currently a major global concern given the huge economic losses companies incur worldwide as a result of the cybercrime and mores on the digital platform.

This research was anchored on game theory, Diffusion innovation theory and Technology acceptance theory. Game theory argues that in order to achieve fully reliable security solution there need to allow the decision taken by one component to consider the policies of all the other components in the network (Njiru, 2013). This concept is widely applicable when designing securities software. Diffusion of Innovation theory is applied in information systems to explain to what extend and level the users are willing to take up new technologies. This model was developed by Davis in 1989, has contributed to a better understanding of behavioral alteration, including the deviation in rates of adoption of innovations in this case online banking (Rogers, 1995).

Cybercrime securities issues are currently a major global concern given the huge economic losses incurred worldwide more so on the digital platform. Thus the study intends to establish the cyber securities strategies to be adopted by the commercial banks in Kenya to help them monitor electronic-transactions from cyber related thefts. The study will also help to bring to light how such strategies impacts on implementation of online banking within commercial banks in Kenya where a more theoretical approach was be taken into consideration during the process of the study.

1.1.1 Cyber Security strategies

The International bodies in charge of communication posits that cybercrime safety strategies are the joint implementation of security procedures, plans, threats management devices, vital practices and proficiency that can be adopted to safeguard the information system.(International Telecommunication Union, 2004). Cyber security entails security of internet security, computer networks and electronic systems (Olayemi, 2014). To prevent the loss of data and uphold integrity, robust cyber-security measures such as early discovery, deterrence and systems ability to continue with its operations during and even after attacks (French, 2009). These are important factors to be considered in mitigating the impacts from cyber-crime and formation of strategy.

System vulnerability occurs when systems are not properly protected. This creates leeway for criminals to find their way into the system and access information illegally.(Tarimo, 2006). Cyber control measures in banking industry should therefore be proactive and reactive at all times. Sole dependence on one precautionary measure for example firewalls and antivirus cannot adequate manage cyber theft. More cyber securities need to be implemented to safeguard information. Modern based technology should be able to detect, deter and eliminate malware and virus before it gets into the system. (Hatfield, et al., 2001).

1.1.2. Online Banking

Online banking is one of the forms of electronic banking platform whereby consumers, retailers and intermediaries can perform several financial transactions as well as consume numerous banking services in an implicit environment (Bradley & Stewart, 2003). Online banking provide electronic consumer interface and presents alternate channel of distribution which allows customers transact through the use of internet (Atanassov, Nanda & Seru, 2007). Electronic transactions through online banking are the application of internet setups to provide numerous services to supplement their products their clienteles (Steven, 2002).

Online form of transaction (online banking) has numerous services such as online screening of account information and report information, payment of bills, transferring funds between accounts, setting up routine periodic payments such as rent and/or loan payments, paying bills, viewing account balances, paying mortgages, inter account transfer, purchase drafts and buying financial apparatuses and offers documentations of deposits, interbank transfers, salary processing, (Kariuki, 2014; Sathye, 1999, Okiro & Ndungu 2013). The advancement of secured transaction technologies using e- banking as a major strategy to aid transactional in banking sector. This online strategy has enabled users to perform ordinary banking services for instance writing bills, paying suppliers, moving funds, printing account reports and getting account balances among many more via online platforms. (Acharya & Kagan (2004)

1.1.3 The Banking Sector in Kenya

Commercial banks operate under the Corporations Act known as Company act supplemented by other acts including the Banking Act, the CBK act provides guiding principles and supervised a single controlling body all under CBK. The banking industry became operational in 2005 and exchange controls elevated. CBK work together with the Ministry of Finance and is in charge of framing and applying fiscal rule and developing the cash liquidity frameworks, solvency programs and suitable working of the monetary system.

CBK is mandated to establish a clearly outlined risk management frameworks in individual financial institutions as a strategy to control cybercrime. CBK has also joined the Anti-Money Laundering Groups (ESAAMLG) in order to fight illegal vices for cleaning illegal funds and funding of terror campaign in Kenya. These bodies work in partnership with FATF, World Bank, UNODC,UK and USA governments (CBK, 2008).

Statistics show that in Kenya, criminals targeted financial institutions and siphoned away an estimated Kshs. 456.3 million in 2009 and attempted to steal close to Kshs 186.7 million in the same period (Okoth, 2009). In 2008, Kshs. 913,154, 000/ = was lost in local currency in addition to the equivalent of USD 291, 000/= in foreign currency in the same year. These losses were attributed to weak computer controls in banks which could easily be overridden. Inadequate laws could thus contribute to the growth in cybercrime cases of fraud and money washing despite the passing of law touching on money washing whose effect is still yet to be felt (Salifu, 2008).

1.2 Research Problem

Cybercrime committed on financial institutions are rapidly and steadily becoming more sophisticated and more widespread. The rise in occurrence and extent of cyber-attacks can be linked to a number of factors, such as ineffective risk management systems within banking sectors, ICT technological infrastructure and staff competency and awareness about cybercrimes attacks. As a result of the vulnerabilities in the systems, organized criminals take advantage to breach financial institution's systems to steal money (Ngalyuka, 2013).

Several researches have been conducted worldwide on cyber safety, cyber threats and effects on online banking. In United States, Vatis (2009) carried out a study on trends in cyber weaknesses, threats and countermeasures. He proposed the need to foster superior security of networks so that they are less susceptible to cyber-attacks. In Germany, Leder (2009) and Australia, Heidi (2009) both of their studies focused on the proactive botnet countermeasures an offensive approach and on social engineering through social media. They commonly recommended an approach that combines both defensive and offensive measure to curb the attacks.

In Kenya, organizations depend heavily on the use of ICT systems which are linked to the internet. As a result, most organizations have become more vulnerable to cyber-attacks. Njiru (2013) carried out a research on a framework to monitor security information inventiveness in banking sector. The found out that the biggest threat to information systems security is human beings. Kitheka, (2013) also conducted a study concerning data safety in public institutions of higher learning in Kenya. This study showed that the information safety controls in public owned universities were not resilient enough to ensure effectively control of information security threats (Kitheka, 2013). Ngalyuka (2013) too did investigate the link between ICT utilization and fraud losses within banking sector in Kenya.

From the above reviews, there exists a knowledge gap on the effects of cyber securities strategies in Kenya are touching on implementation of online banking. This study sought to fulfill this gap. It sought to provide comprehensive solutions to the questions: what are the effects of cyber securities strategies on the implementations on online banking at the Kenya's commercial banks.

1.3 Research Objective

The purpose of the study was to establish the level effectiveness of cyber security strategies on online banking implementation within the commercial bank in Kenya.

1.4 Value of the Study

This research sought to adds to the existing knowledge about effects of cyber security strategies on implementation of online banking. It would avail written materials on the concepts of cyber security strategies and how they influence online implementation. The study is also expected to equip cyber security development engineers with better answers to take care of the worries and necessities of their clients.

To the Top management within the banking industries, the study would be of importance in appreciating the need for having proper control measures in place. They would understand the importance of allocating enough budget and resource to the ICT department to ensure proper security control are adhered to. This could be achieved through hiring ICT staffs, buying and installing security and continuously conducting security trainings and awareness through workshops. To researchers and academicians, this research study would be essentials in the proposition of areas for further research in enhancing the topics of cyber safety in commercial banks in Kenya. This would help to create more insights related areas of study that would have been overlooked. Furthermore, the outcome of this study would provide vital foundation of reference to scholars and researchers planning to undertake similar studies.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This section discusses literature analysis on online banking, cyber threats and cybercrime. The literature is reviewed from journals, reports, periodicals and books. Literature review provides basis and insights into relevant previous research and developing trends. (Saunders, Lewis & Hill, 2000). It present theoretical views and ideas of the earlier research that has been done in the same field.

2.2 Theoretical Literature Review

This segment provides insights about theoretical foundation and models that support the study. This study will use game theory, diffusion of innovation and technology acceptance theory as a basis of analysis. These theories and model will provide clear link connecting dependent variables and independent variable as earlier researched by scholars.

2.2.1 Game Theory

This theory was introduced by Neumann and Morgenstern, (1944).The theory further states that in order to achieve fully dependable security system, there need to permit decision taken by a single component to consider the policies of all the other related mechanism in the network. It was later advanced by Osborne and Rubinstein, (1994) to incorporate multi-agent decision making. Most researchers have applied a stochastic means to prototype network security situations to develop security frameworks (Lye 2005), formation of strong network systems (Wu 2010), and intrusion discovery schemes (Alpcan, 2006).

Game theory comes in handy when model and analyze search large space which involve numerous challenging scenarios. This theory has the ability to examinea thousands of possible circumstances before engaging in favorable action; henceforth, it can complicate the decision making process of the network administrator to a huge scope. (Shiva and Sankardas, 2010).

This theory is relevant to the study since it can be used to the analyze multi scenarios by systems administrators, managers and network experts to formulate strategies and control measures protecting the systems and reducing system vulnerability. Game theory alone cannot be used to analyze the entire security issue since it majorly focuses on network system hence the need to focus on other theories such as Diffusion of innovation theory.

2.2.2 Diffusion of Innovation Theory

This theory was originated by Rodgers in 1962 after empirically analyzing more than 508 studies on technology diffusion across various fields. In line with this theory, the decision to take up innovations is determined by five issues regarding the features of the innovation. These are the perceived usefulness, matching needs, intricacy, testability and visibility with the social system adopting the technology (Rogers (2005, 2003).

According to Rogers (1962) the Diffusion of Innovations (DoI) Theory was as a result of contributions from the pioneering efforts in the implementation of innovations. The theory also holds that the adopters can be clustered into several categories namely innovators, early adopters, early majority, late majority and laggards. Importantly, the theory holds that customers in the innovation adoption phases differ dramatically in their features.

In the initial stages of diffusion, the invention typically takes an S shape. The phases alongside the innovation route are associated by the determinations of the innovator to acclimate a technological development for conversion into an innovation product.(Easing wood, 1988).According to Rogers' adopters of any fresh idea could be classified as innovators, primary adopters, early mainstream majority, late majority and laggards.

In the proposed study how the bank managers, employees and customers perceive the five salient features identified to indicate reliable determinants of acceptance and use of electronic banking in local banks. Further, within the banks in Kenya not all banks adopt the e- banking technology and those that adopt do not adopt at the same time as per the theory. In-line with this theory, the decision to take up innovations is determined by five issues regarding the features of the innovation. These are the perceived usefulness, matching needs, intricacy, testability and visibility with the social system adopting the technology.

2.2.3 Technology Acceptance Model (TAM)

TAM was originated by Davis (1989).The theoretical perspective proposes that the connection between users' acceptance of any innovative and the users' supposed ease of use and convenience of such innovation. The TAM perspective suggests that for any new technology, several issues determine the decision about how and when the technology will be used. These issues include the perceived usefulness and how easy to use is it perceived. (Davis 1989). TAM was developed after several tests by Venkatesh and Davis (2000).

Legris, Ingham & Collerette (2003) did prove that TAM is a theoretical model that can help explain and predict user behavior of information technology. Sabi (2014) also found out that the TAM theoretical perspective is a reliable and was the most applied theory as evidenced by thirty one articles or sixteen percent out of the one hundred and eighty eight articles reviewed. In the context of the study, the theory is relevant because it's a factor by which the adoption of e-banking by local banks can be rationalized. User behavior on newly introduced information systems is a key factor in its adoption. In this study we shall conduct a research to find out the percentages of customers enrolled for online banking in Kenya this will determine the association between the expediency of information systems and the users' perceptions.

TAM theory is relevant because it's a factor by which the adoption of e-banking by local banks can be rationalized (Sabi, 2014). User behavior on newly introduced information systems is a key factor in its adoption (Legris, Ingham & Collerette 2003). In this study we shall conduct a research to find out how acceptance to new technologies my exposed banks to cyber theft in Kenya.

2.3 Cyber Securities Strategies and strategy implementation

Cybercrime committed on financial institutions are rapidly and steadily becoming more sophisticated and more widespread. The rise in occurrence and extent of cyber-attacks can be linked to a number of factors, such as risk management systems within banking sectors, ICT technological infrastructure and staff competency and awareness about cybercrimes attacks. As a result of the vulnerabilities in the systems, banks have been forced to adopt strategies such as risk management system, information and communication technology infrastructure, and staff competency and awareness on online banking implementation. The three components are discussed:-

2.3.1 Risk management system and online Banking implementation

Due to increasing level of cybercrime in the banking sectors due innovation, banks been forced to adopted risk management systems to control these activities. Effective risk management system is considered essential for creating information security in banks and on e-transactions (Bulgurcu et al., 2010). Management performs an oversight role as far as risk management is concerned. Guidelines provided with ISO27001:2013, and Corporate Information Security Policy (CISP), dictates that the managerial should be entire in charge system security. Key stakeholders such as senior managers, systems developers, systems designers, the administrators and security team members are at the core of formulating key strategies and framework for risk management (Bulgurcu et al., 2010).

These control mechanisms are critical and failure to abide and conduct thorough due diligence can lead to greater damage both on reputational and financial loss. Phishing scams and malware are methods that criminal commonly use to illegally gain access to the system and steal information. It is important to effectively manage the mails. Mail filters is a security control strategy that is implemented in a wide range of experimental processes on mail headers. Organizations tend to form situational consciousness in numerous means, and hence able to distinguish threats and damages (Bulgurcu et al., 2010).

Risk assessment within the organization is very vital since it aids in the identification of gaps in institution`s risk prone areas and to decide on the appropriate actions to fill in the identified breaches. These risk management strategies tend to help in informed decision on how to invest on time, funds and human resource and avoid wasting of resources. It further involves several overall steps according to IT governance website, the first step would be to identify the various information assets that could be affected by risk, then to identify the risk that could affect the identified assets (Hatfield, et al., 2001). A risk evaluation and prioritization is done on the identified risks, then controls and policies are put in place to manage the identified risks finally monitoring review of the controls is done.

2.3.2 Information and Communication Technology infrastructure on online banking implementation.

According to Rex white and George (2007) technological infrastructure are perceived as tools and models that aid efficient knowledge management from various sources. ICT is one of the key elements of Management information security within the organizations' system. The banking sector employs Basel III strategy help them to curb operational risks.(Locher, 2005).Munir & Manarvi (2010) posits that ICT need to be consolidated together with operational risk administration to enhance real security management within e-banking systems.

ICT security framework have a significant impact in enhancing cyber related attacks within the commercial banks. These security strategies have helped to guarantee satisfactory security level. However, these strategies are not able to guarantee 100% security level (Susantoet al., 2011). Siddique and Rehman (2011) recommended three security precautionary measures. These include banks putting in place protection programs which have power over cookies. Secondly, it is essential to have the most current and up to date software with the most up-to-date patches. Finally, they recommend that all banks should have a firewall which is defined as a form of controls access to a secured network (Limited, 2011).

A firewall should be plugged in all systems in case any request to access from unrestricted network is logged in to the secured network, it needs pass through the firewall, thereby reducing chances of unauthorized users protruding into the organizations systems. To supplement this, a network security policy must also be clearly defined and put in place. These security controls measure helping organization in outlining the resources that need protection. (Firewalls & Virtual Private Networks, 2009).

Systems customization, access controls, software updates and escalation matrix are key a strategies used by ICT departments as a control mechanism. ICT framework, models and internal network security measures need to be regularly reviewed and new control mechanisms adopted. It’s recorded that Banks are continuously conveying data over networks needs to adopt encryption mechanisms to secure their data from criminal intruders as well as use virtual private network and IPsec protocols to enhance data security being transferred from one point to another (Siddique & Rehman, 2011).

2.3.3 Staff competency and awareness on online banking implementation.

Cyber related crime not only aims at vulnerabilities in technology but the vulnerabilities caused by staff behavior. Despite having robust measure in place, most organization still falls victim of these attacks. Most of the cybercrime are committed by insiders more precisely employees (Panel, 2006). As a result, prudent measures such as vetting needs to put in place (Panel, 2006).

Insider related threats, Social engineering, Cyber Espionage among others are the key channels through which organizations' systems get hacked. Insider threats which is the deliberate activities committed by the existing employees. Cyber Espionage which is the stealing of secrets stored in digital formats. Chaula, (2006) presents key security control strategies mostly touching on human behaviors. These include maintaining robust security values. Chaula, (2006) identified the following countermeasures that most banks needs to implement. These include oversight role, extensive awareness creation, risk orientation campaigns, compliance to lay down securities procedures and paying attention to customers details.

Training and creating awareness for all staffs is the most fundamental security control strategy. Training should be conducted regularly with staffs kept abreast on evolving trends of threats (Tendulkar, 2013). Awareness creation about cyber-related risks is slowly increasing. Policymakers around the world and experts have admitted that cybercrime is a phenomenon and is affecting most economies in a greater extend. A result security experts are keenly and openly elevating cybercrime as a national concern. The environment of low awareness and transparency could exacerbate the impact of cyber-attacks (Jain, 1994).

2.4 Empirical Review & Research Gaps

From reviewed relevant journals, thesis and literatures, it was quite clear from several writers like; French (2012), Nikhita and Gander (2012), Jassal and Sehgal (2013), Faheem (2013) that emerging technologies have become more innovative especially in electronic. The increase in innovation in areas of electronic transaction technologies leads to increase in sophistication of the cyber threats targeted to these technologies. However, they have commonly agreed that there is no a clear framework to completely eradicate cyber threats and attacks.

Research on Pakistani commercial banks discovered that suitably formulated security controls measures are in place; however people cultures supporting information security was completely left out (Munir & Manarvi, 2011). Similarly, Ngwenya and Malufu (2012) support the same on their study on Zimbabwean commercial banks, which in most instances they failed to meet behavioral security standards. Okere, Van Niekerk and Carroll (2012) applied Schein's (2013) 3-stage model of organizational' s culture as a foundation for evaluating information safety methods concluded that none have adopted the formal assessing methods of utilizing an established assessment framework. Ibikunle and Eweniyi (2013) on his study focused on challenges and explanation to cyber safety issues in Nigeria. Their finding and recommendation were, there was a greater need of addressing ICT networks vulnerabilities, therefore the need of cultivation a strong cyber security traditions and deriving partnership in cyber security between private and public organizations.

Hussein and Khalid (2016) did a survey on cloud computing security challenges. The study projected model to be used for cloud computing measures which is made up of 3components. The initial component is user's recognition, the second component rely on data detection and the last component is cryptography (encryption) procedure is used to protect the transmission of the data. This model could help to control and manage cyber securities issues.

A study by Deshpande and Sambhe (2014), and Deore and Waghmare (2016) in India on cyber security by focusing on the strategy to security challenges and cyber security automation for regulating data distribution respectively their finding were more like the same, users need to protect personal computers as well as other electronic devices. Firewalls can be employed to protect all personal devices. Cyber security performs important function in information system as well as data distribution and specific developed software needs to be developed using different mechanisms developed and used by scientist for the guarding of information from attacker.

Kreicberga (2013) in Sweden did a study on internal security threat to information safety countermeasures on human factors in small enterprises. The findings were that formal policies lacked appropriate safe guarding and awareness means hence do not affect employee behavior, while casual norms within organization have the greatest control on information security behavior. These strongly support the need to undertake the proposed in order to fill the gaps identified.

Scholars such as Nyambura (2015), Gichengo (2010), and Target (2014) did agree that innovation has greatly enhanced electronic transactions but slightly differed on the approach to mitigate the cyber threats they suggested that the cyber threats could be completely eliminated and this could be done using a particular cyber-security model framework while the focusing on ICT security as a whole. Wechuli (2014), Makumbi et al (2012) and Nyamongo (2012) did a research on cyber security assessment framework Kenyan's government ministries by analyzing the restraining factors affecting these frameworks, assessment of IT technology security related practices within small enterprises in the financial Sector in Kenya and information systems security management on private chartered universities in Kenya respectively.

Their objectives were to establish factors affecting cyber securities within government ministries, the level of dependence on Kenyan SMEs are on ICT and to find out how Kenyan small enterprises and medium enterprises are safeguarding their systems and networks from data theft respectively. The three studies reach a consensus that awareness and training in organizations and institution about security information should be prioritized and a robust strategic security measures needs to be adopted in managing cybersecurity. The studies recommend that, organizations must employ countless securities strategies in place such as separation of functions, security access controls measures and investments on IT assets and finally awareness campaigns for users to sensitize them on ICT security (Makumbi, 2012).

Njiru (2013) supplemented on what other scholars have done by conducting a research on framework guide to information security creativities for accessing banking information systems, a situation on Kenyan banking sector. His key objective was to identify common vulnerabilities affecting the banking information systems and frameworks used to evaluate security programs in banking systems.(Njiru, 2013). The findings were that people are the largest threat to information security and lack of proper training and awareness by staff and customers are the major obstacles to security effectiveness. This has been supported by both Local and international studies reviewed.

The study have identifies some gaps relating to contextual, conceptual and methodological used hence the need to conduct the research on cyber security strategies on online implementation within Commercial Banks in Kenya.From both international and local literature reviewed, there is a mutual agreement that banks are increasing facing cyber-attacks from fraudsters. There has been a substantial rise on cybercrime pursuing human actors to perpetrate crime through internal staffs and outsider.

These reviews establish that technological component only cannot manage the allied cybercrime risks. Rather, researchers universally agree that employment of all-inclusive tactic to ascertain highest level of security is required. Schein, (2009) discovered that present approaches of evaluating security culture have considerable vulnerabilities, such as adopting questionnaires to evaluate culture. Schein, (2009) argued that the use of questionnaires assess culture do not disclose how cultures impacts but only review shallow characteristics of the culture (Schein, 2009). Therefore, it quite clear that there is a strong case to conduct a research on the cyber securities strategies touching on socio-technical aspects on online banking implementation.

Several approaches to risk assessments have typically followed this autonomous dimension solely focusing on the components rather than holistic issues. To incorporate these aspects, an all-inclusive approach is needed and therefore this research evaluated Soft Systems Methodology (SSM) which involved a component of human activity' (Reviewer1, 200x:x). Checkland's (1999) defined SSM as a problem-solving methodology for complex and disorganized situations by creating a variety of models to represent each particular situation(s). SSM is not only appropriate in carrying out security analysis but also to bring on board key stakeholders and identify potential culturally practicable solutions.

Despite there being local studies conducted in the area of information systems security, they have not clearly addressed the subject matter with a focus on cyber security strategies on online banking implementation within commercial banks in Kenya. Therefore there exists a knowledge gap on how commercial banks in Kenya are managing cyber security hence the need for this research to find answers to the questions: What cyber security strategies have been put in place by commercial banks in Kenya to counter cyber-attacks committed on online platform and the perceived effectiveness of the countermeasures these organizations have put in place in countering cyber security threats.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter contained the methods that were used to collect and analyze research data. It further contains sub-sections; research design, study population, the cross section procedure, and procedures for data collections and data analysis methods. This chapter provided study framework on the key areas under focus.

3.2 Research Design

A research design is defined as method of careful selection of methods used to answer the research questions and solve the research problem. According to Creswell et al (2007), research designs are the procedures for collecting, analyzing, interpreting and reporting data in research studies. This study will adopt a cross-sectional survey across the commercial banks in Kenya and the data obtained will be used analyzed in line with the objectives of the study. A cross-sectional survey as a research design will be used to observe a defined population at a given time (Malhotra, 1996). In the study the researcher will obtained data from 41 commercial banks. A questionnaire will be administered to the ICT heads and online banking managers.

Cooper and Schindler (2003), described descriptive design on the basis on univariate hypothesis where it seeks to assess the state of the current associations amongst variables, with the attempts to seek to provide answers to questions such as who, where ,why, what, and how. This form of research design is suitable in giving an account of the effects the cyber securities strategies on online banking implementation within commercial bank in Kenya. The independent variables are risks management systems, ICT framework and, staffs competence and awareness.

3.3 Population of the Study

The population of the study represents the entire data set that the researcher wanted to study and where inferences are made (Cooper & Schindler, 2003). The targeted population was of the study was the 41 commercial banks in Kenya who have adopted online banking services. A total of 31 responses were received from out of 41 Commercial Banks in Kenya.

The study majorly targeted ICT departments and online Banking departments. Individual target respondents for this study comprised of ICT Officers and Online banking managers who deals with cyber securities issues within organizational setup. i. e commercial banks in Kenya. Response rate of 75.6% per cent was recorded with 31 out of 41 submitting back their questionnaires. One person was chosen to represent each bank.

3.4 Sampling Procedure and Sample Size

There will be no need to sample since the study population is small (only 43 banks). Therefore census method would be used for this study whereby all the licensed commercial banks will be included in the study. Coming up the suitable and manageable data size is important. Inadequate data size may results into getting outcome that are statistically insignificant, hence may not be used to deduced to generalize conclusion about the entire population (Kitchenham & Lawrence, 2002).

A cross sectional survey targeting ICT officers and staffs managing online transactions was carried out in 41 commercial banks in Kenya selected randomly from a population of 41 Commercial Banks in Kenya. Out to 41 commercial banks, we managed to get feedback from 31 respondents who managed to completed survey questionnaire giving a response rate of 75.6 percent.

3.5 Data Collection

The study used primary as well as secondary data. Primary data was arrived at through administering structured questionnaire both by self and via email. Secondary data on the other hand was obtained from review of organizations' profiles, journals, books, magazines and past research findings among others. Data was then collected using a structured questionnaire developed from the research question. Some of these questionnaires was self-administered while other were shared on the emails and shared with respondents in two different ways. The interview targeted one Information security experts and or one head of Online banking channel in each of the Commercial Banks.

The data collection tool used was questionnaire which was composed of four parts. First part being demographics, cyber securities threats, cyber securities strategies and countermeasures to curb these threats. It was further segmented into two major sections; section. One of the sections contained general questions to help the researcher to get overall information on the respondent while the other remaining sections contained closed ended questions.

3.6 Validity and Reliability of Research Instrument

The interview guide was designated from the researchers own knowledge of information and cyber security management. It has been subjected to validity and reliability testing by conducting mock interviews with acquaintances who are currently working or have previously worked in the banking industry in Kenya. The responses and contributions have helped refine the interview guide and structure to meet the objectives of the research. Therefore the research instrument used in this study is valid and reliable.

To ascertain the validity of the research instrument, the study sought after opinions of those with skills precisely the researchers and lecturers working under the department of project management (Cooper & Schindler 2003). The opinions and ideas gained will be used to enhance the validity of the data collected. This data will make it possible to conduct necessary fine-tuning of the research instrument.

3.7 Data Analysis

Data analysis entails several stages. First, it began with data preparation which is the obtaining of information from the data which was collected. This was then followed by data editing used adjust data to ensure that omissions, accuracy and consistency are maintained. This is then followed by data coding. This is identification and assigning statistical scores on the data that was being edited. For clarity purposes, the researcher contacted the respondents on several occasions where researcher needed to seek deeper understanding. Transcriptions of data was done and transferred to excel and SPSS. Data was then analyzed using inferential statistics as well as descriptive statistics. The output of data analysis from Excel depicted a strong relationship between the stated variables. The findings and outcome from data analysis was presented in table and figures.

3.8 Chapter Summary

This chapter discussed in details the methods that were employed to bring together, organize and scrutinize the data collected from the field. It also looked at the design of research adopted, study population, sampling procedures, methods of data collections and finally data analysis. The data used for analysis was collected form 31 respondents out of the target of 41 Commercial Banks, One IT expert or online banking manager was required form each banks. Data collection tool was developed from the research question. Data analysis was achieved by the use of excel as well as by the use of SPSS. These methodologies highlighted above aided data presentation and the findings were presented inform of charts, graphs and tables.

CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSIONS

4.1 Introduction

This chapter provides the study findings. The analyzed data has been presented using figures as well as tales. Data collection tool used was thereafter analyzed using descriptive statistics. The questionnaires administered were mainly completed by either ICT security officers, chief information officers, ICT managers, IT Managers, ICT officers, ICT directors who are basically the staff charged with cyber security issues in the organizations. Some of the questionnaires were administered by self, other were sent via email and internet link where response were channeled back for analysis using the same channels.

4.1.1 Response Rate

Thirty one(31) responses were received out of 41 commercial banks that were targeted. This implied that a response rate of 75.6% percent was recorded while 24.4% per cent failed to return their questionnaires. A response rate of above 60 is considered as good for the study (Mugenda & Mugenda 2003). From this result we can deduce that the study was justified in terms of validity and reliability of data collected. These findings are well illustrated in the Figure 4.1.

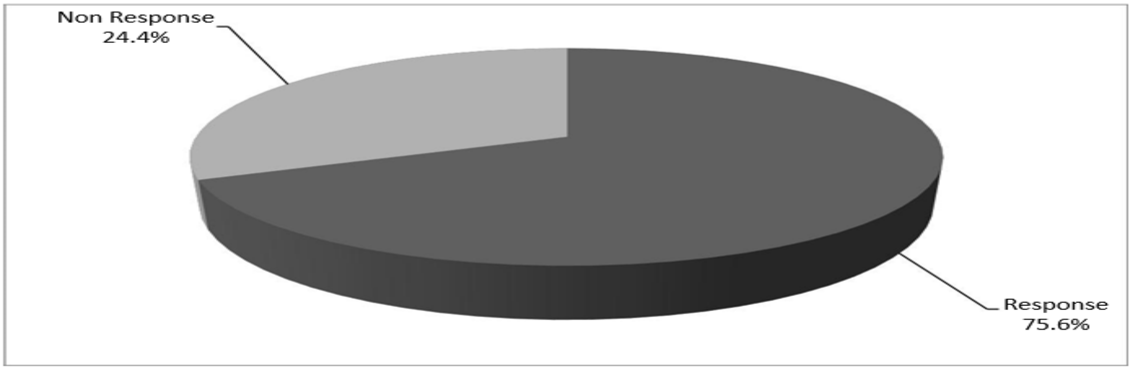


Figure 4.1: Response Rate

Source: Research Data (2018).

4.2 Demographic Information

The sought to find the demographics information of those who participated in the interview so as to rationalize the validity of data collected from 31 respondents for substantiation purposes. It contained respondents' facts as captured on the questionnaires regarding risk managements, staff competencies and ICT infrastructure strategies with regards to cyber security measures. In order to show the effectiveness of cyber securities strategies verses online banking implementation in Kenya, demographics information was considered important.

4.2.1 Gender of Population

This study wanted to find out the gender of those who participated in the interview. The findings are shown in Figure 4.2. There were 11 female respondents and 18 male respondents translating to 59.5% male and 40.5% females while 2% opted not to disclose their gender. It can be concluded that this industry is male dominated. This is clearly highlighted on the figure below.

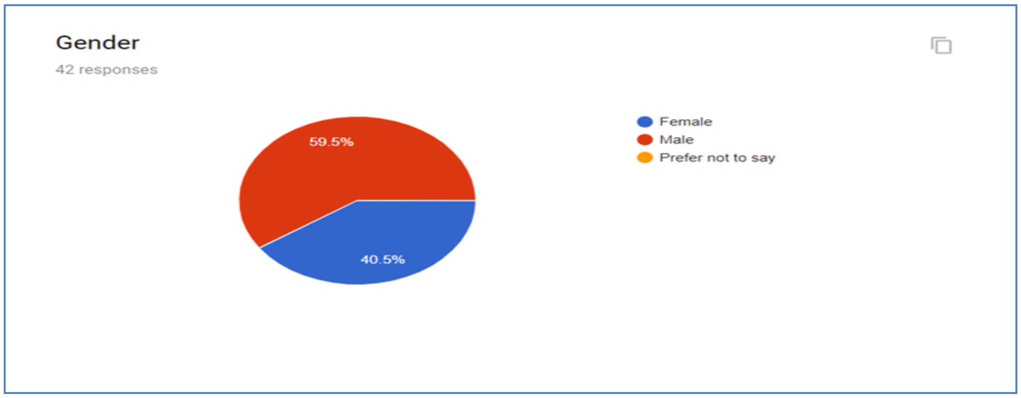


Figure 4.2 Gender of the populations

Source: Research Data (2018).

4.2.2 Age of Respondents

This study sought to find out information about the age of the respondent representing the entire population. The findings were Twenty three percent (14.3%) of the interviewee recorded that they were below 25 years old, while forty eight percent (45.2%)were falling in between 26 to 30 years and 35.7% recorded that their ages were between 31 years to 35 years and three percent (3.8%) were in between 36 to 40 years. Figure 4.2.2 clearly highlights these statistics. It can therefore be concluded that majority of the responded were falling between 26years old to 30years old while minority are falling between 36 years old and 40 years. This industry is dominated by young population.

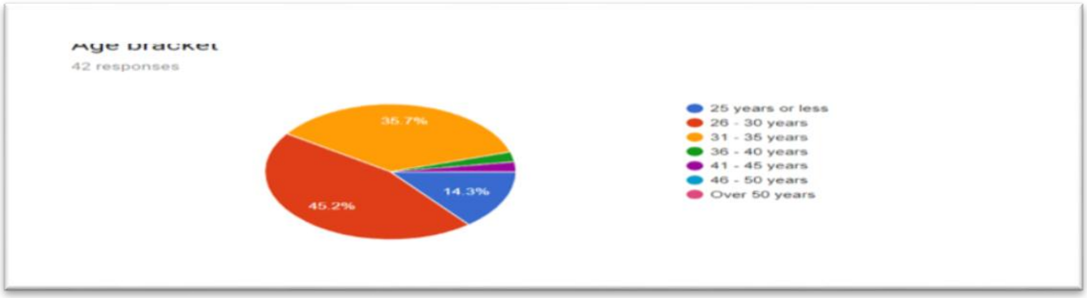


Figure 4.3: Age of the respondents
Source: Research Data (2018).

4.2.3 Highest Education Level

This study sought also to find education level of the respondent. This was considered a critical component as it impacted on directly on the research topics. It was also used to gauge whether the respondent were able to read, comprehend and responds to the research questions accordingly. The finding were Eighty five point seven (85.7%) of the respondents were graduate, 14.3% were holding postgraduate qualifications and negligible percentage holds diploma qualifications. Figure 4.4 clearly represents this in form of a diagram. This showed that there is high level of literacy amongst those who responded meaning that they were able to read, understands and respond appropriately as per their knowledge.

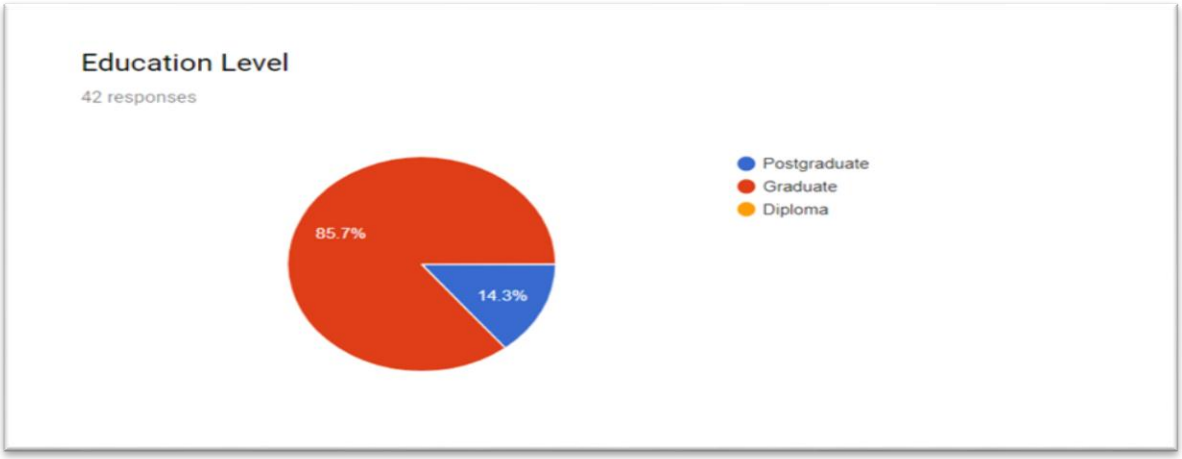


Figure 4.4: Highest Level of Education

Source: Research Data (2018).

4.2.4 Position held in the Bank

This study sought to understands different opinions and views of those who are charged with upholding and managing security issues within the banking sectors. The study majorly targeted the one ICT staffs and/or Channel managers heads in each of the 41 Commercial banks out of which 31 responses were received. The positions held by those who responded are clearly highlighted figure 4.5

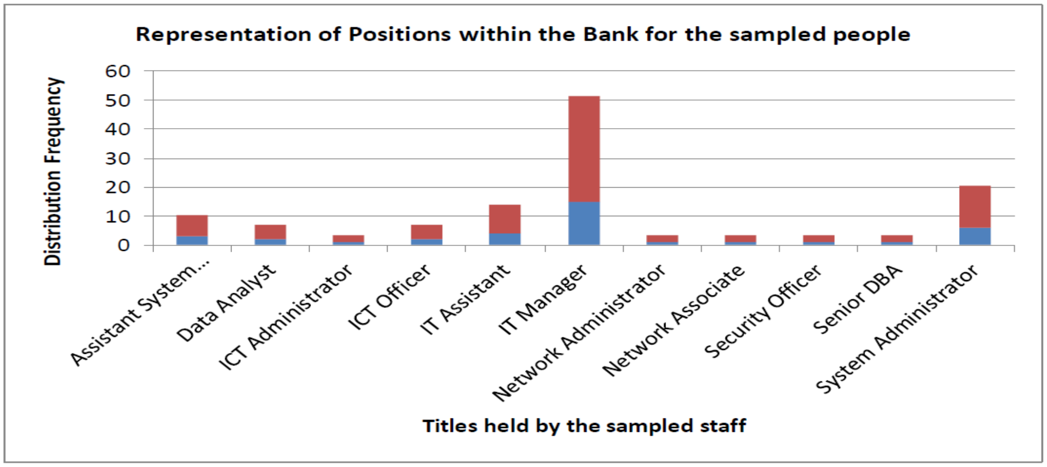


Figure 4.5: Ranks (position) held by the respondents.

Source: Research Data (2018).

4.2.5 Years of Experience

The study looked at the age of the responded with respect to understanding how this affects cyber safety measures. The findings from the study reported aSixty four point three per cent (64.3%) of the response indicated that they have less than Five years on their current job, while 23.8% indicated that their experience falls between 6 years and 10 years and 11.9% of the remaining respondents indicated that their experience is over 10 years. The responses from the respondents are shown on a figure labeled 4.6.

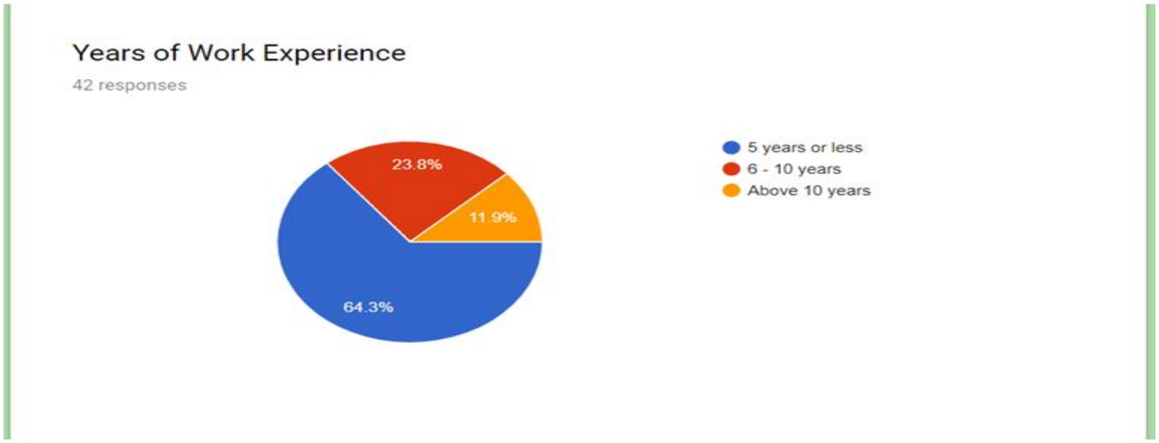


Figure 4.6 Years of experience

Source: Research Data (2018).

4.2.6 Statistics about the Employees

The study intended to establish statistics of staffs that are employed in commercial banks. The findings from the study were 71.4% per cent of the respondents recorded that the total number of employees in their organizations fall above 1000 while 26.2% per cent of the respondent indicated that the employees in their organizations falls in between 101 and 999. The remaining 2.4% per cent indicated that those employed in their institution were 1000 and below. This is clearly represented in Figure 4.7

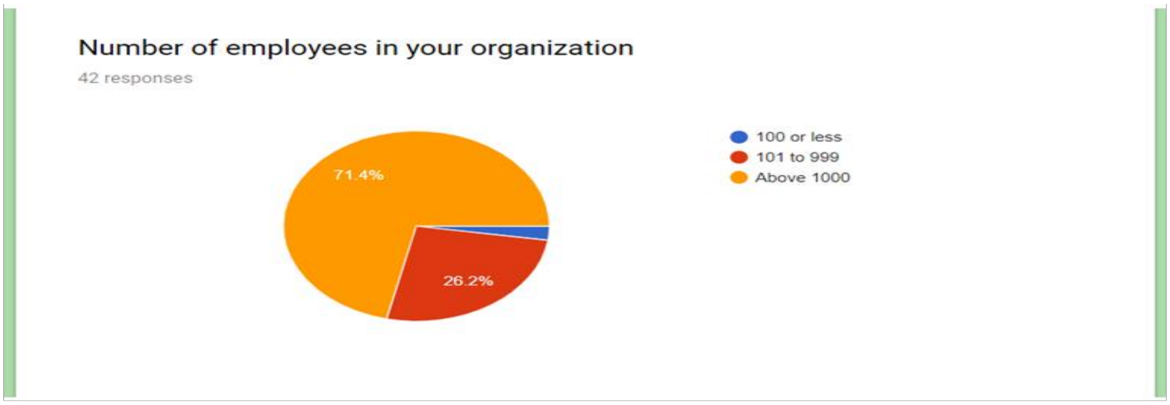


Figure 4.7 Number of employees

Source: Research Data (2018).

4.2.7 Asset base and Ownership

The study also sought to establish the asset base within the organization and the ownership whether locally internationally or both. The findings from the study were 78.6% per cent of the respondents recorded that their organization owns assets worth KES 10 Billion and above while 9.5% per cent of the other respondents stated that that their organizations owns approximately in between KES 5 Billion and 10 Billions. On ownerships, Fifty eight per cent (58%) of the other respondents indicated that their companies are locally owned while 2% said their companies are foreign owned. This implies that most commercial banks are owning an assets above KES 10 billion and more than 50% of those commercial banks are locally owned. Figure 4.8 clearly represent the information in a diagram form.

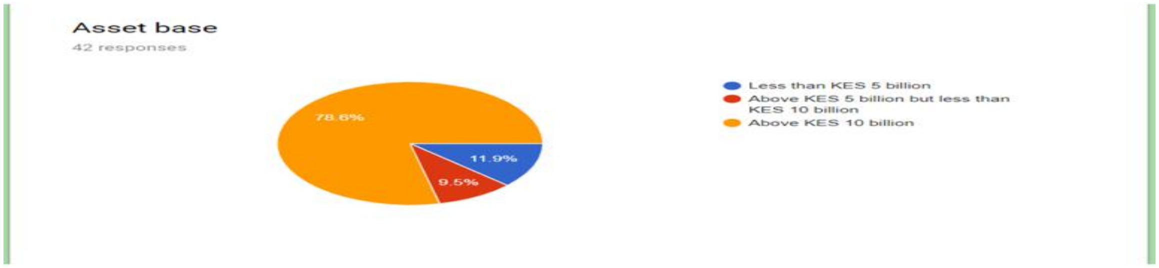


Figure 4.8 Assets based and ownership.

Source: Research Data (2018).

Tables 4.1 Summarized Data on asset base, ownership and Account holders.

LIST OF COMMERCIAL BANKS IN KENYA	Asset Base	Duration in Kenya	Owner Ship	Account holders subcribed to online Banking
Bank of Africa Kenya Ltd	<10	30	BOTH	20000-50000
Barclays Bank kenya Ltd	<10	89	FOREIGH	20000-50000
CFC Stanbic Holdings Limited	<10	30	BOTH	20000-50000
Chase Bank Kenya (Under Receivership)	*<10*	30	BOTH	20000-50000
Citibank N.A Kenya	<10	26	LOCALLY	20000-50000
Consolidated Bank of Kenya Ltd	*<10*	*100*	*LOCALLY*	*<50000*
The Co-operative Bank of Kenya Ltd	<10	122	LOCALY	<50000
Credit Bank Ltd	<10	38	LOCALLY	<50000
Diamond Trust Bank (Kenya) Ltd	BTWN 5B-10B	30	BOTH	20000-50000
Ecobank Kenya Ltd	<10B	35	BOTH	20000-50000
Equatorial Commercial Bank Ltd	<10B	107	FOREIGN	20000-50000
Equity Bank Limited	<10B	59	LOCALLY	20000-50000
Family Bank Limited	<10B	30	LOCALLY	20000-50000
GT Bank Ltd	<10B	36	LOCALLY	20000-50000
Giro Commercial Bank Ltd	<10B	59	LOCALLY	20000-50000
Guaranty Trust Bank Kenya	<10B	32	LOCALLY	20000-50000
Guardian Bank Ltd	<10B	45	LOCALLY	20000-50000
Gulf African Bank Limited	<10B	47	LOCALLY	BWTN 5001-20000
Housing Finance Company of Kenya	<10B	40	LOCALLY	0-5000
I &M Holdings Limited	<10B	59	both	<50000
Jamii Bora Bank Limited	BTWN 5B-10B	47	LOCALLY	5001-20000
Kenya Commercial Bank Ltd	<10B	59	both	<50000
K-Rep Bank Ltd	<10B	59	LOCALLY	20001-50000
National Bank Of Kenya Ltd	<10B	30	LOCALLY	<50000
NIC Bank Limited	<10B	40	LOCALLY	5001-20000
Prime Bnak	<10B	27	BOTH	20000-50000
Spire Bank	<10B	59	BOTH	<50000
Sidian Bank	<10B	42	BOTH	20001-50000
Stanbic Bank	<10B	40	BOTH	<50000
Standard Chartered Bank Kenya Ltd	BTWN 5B-10B	31	LOCALLY	5001-20000
Trans-National Bank Ltd	<10B	47	LOCALLY	BWTN 5001-20000

Source: Research Data, (2018)

4.2.8 Statistics about the account holders enrolled in online banking

The study intended to establish the statistics of clients' account especially those enrolled in online banking services. The study revealed the thirty eight percent (38%) of those who took part in the interview recorded that 50,000 and above accounts have been fully enrolled in online banking while twenty eight percent (28%) indicated that those that have enrolled in electronic banking range between 5001-20,000 of the account holders; 18% of the those who responded to that question said that accounts between 20,000-50,000 are enrolled and using electronic banking services to carry out their transactions. These results implies that majority of the commercial banks in Kenya are using online banking services to carry out their transactions. This is represented in the figure labeled 4.9

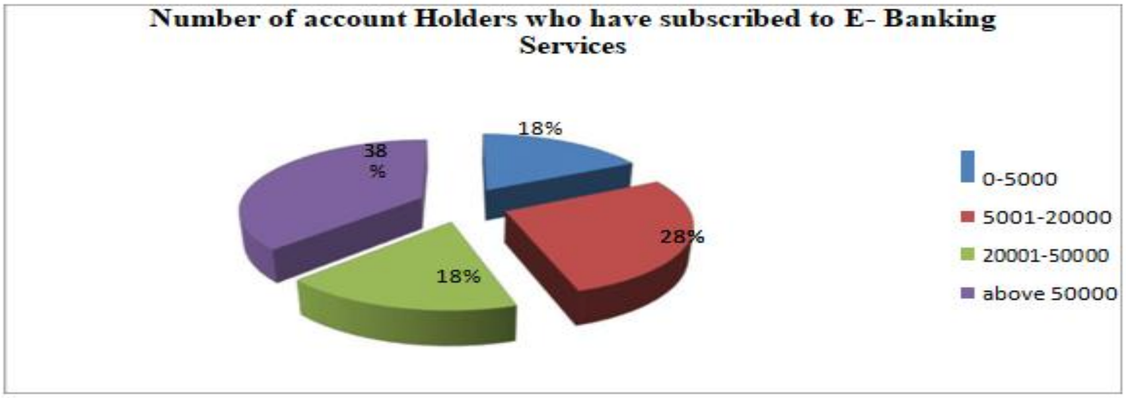


Figure 4.9: Statistics about the account holders enrolled in online banking

Source: Research Data (2018).

4.3 Factors Contributing to the Incidences of Cyber related crime (threats) on Electronic Banking in Kenya banking sector.

This study was carried out to establish the factors associated with the incidences of cybercrimes committed through online banking platform. This information was considered to be key in revealing the gaps and loophole that attackers use. It also helped in formulation of countermeasures to minimize or completely block cybercrime incidences. Below are the key factors leading to the incidences of cybercrime committed on online platform within commercial banks in Kenya and discussed in details?

4.3.1 Security compromise through employees accidentally committing mistakes

The research was conducted to find out opinions of the respondents about the employees intentionally or unintentionally committing mistakes that may lead to cyber-attack. Fifty Eight (58%) of the respondents indicated that this contributes in little extend while 39% of the respondents indicated they that this does not at all contributes to the cybercrime and 3% agrees that this contributes moderately to cybercrime. This is information is represented in the below diagram labeled 4.10.

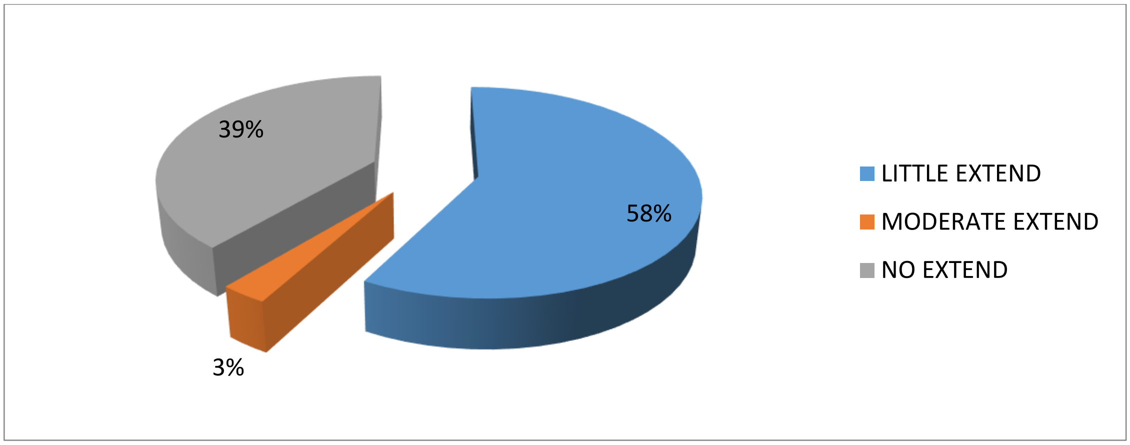


Figure 4.10: Security compromise through employees accidentally committing mistakes

Source: Research Data (2018).

4.3.2 Employees being misled by External Parties to give out login credentials

This study was conducted to try and establish the respondents' knowledge about employees being misled by External Parties to give out login credentials. The results showed that (51.6%) of the respondents indicated that this contributes in little extend while 48.4% of the respondents indicated they that this does not at all contributes to cybercrime. This is represented in figure 4.11 below

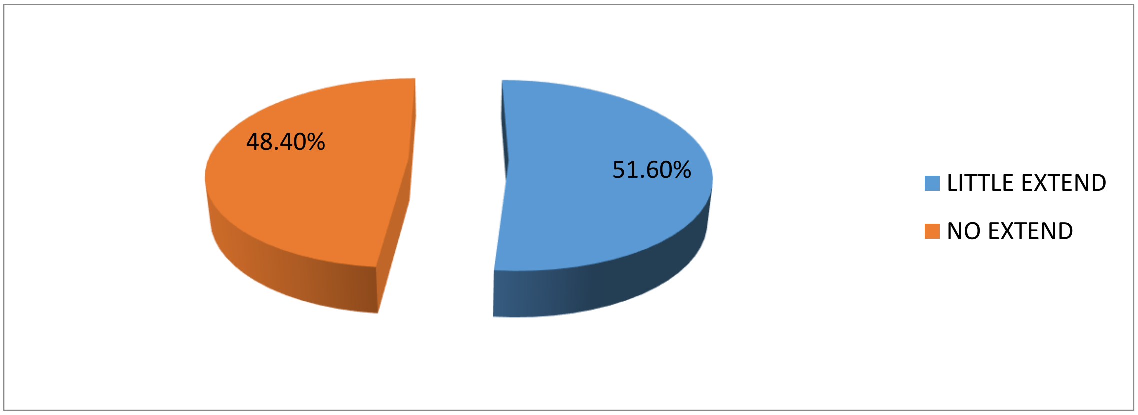


Figure 4.11: Security compromise through employees accidentally committing mistakes

Source: Research Data (2018).

4.3.3 Authorized users such as IT experts attacking the systems

The study conducted to find out unravels if the authorized IT experts contribute to the cybercrime by attacking the systems. Forty one point nine (41.9%) of the respondents indicated that this contributes in little extend while 48.5% of the respondents indicated they that this does not at all contributes to the cybercrime and 9.6% agrees that this contributes moderately to cybercrime. This data collected is depicted in figure 4.12 below.

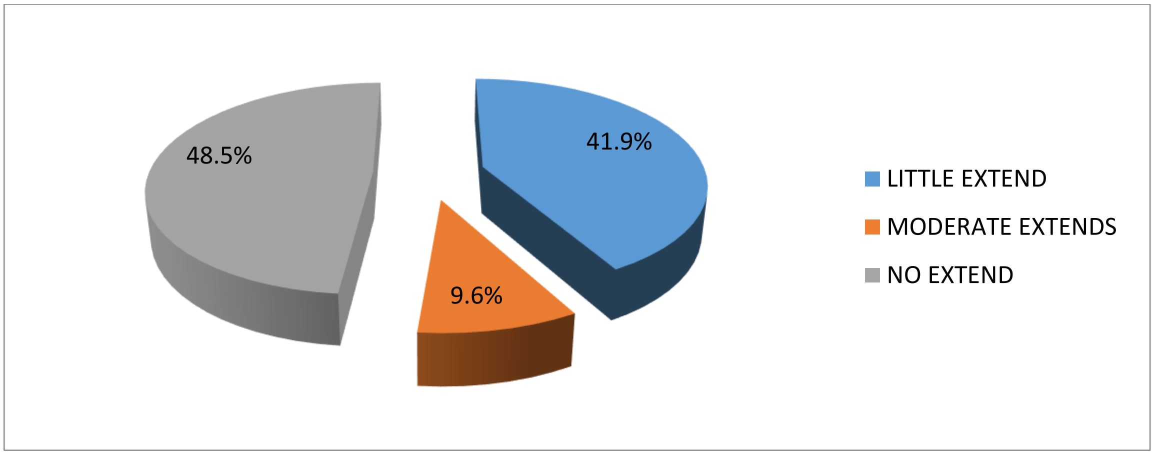


Figure 4.12: Graphs showing how authorized IT experts attacks systems

Source: Research Data (2018).

4.3.4 False offers on the internet to share the credential

The study intended to establish to what extend respondents receive false to avail their credentials to the third party via social websites and its impacts. The findings were. Sixteen Percent (16%) of the respondents indicated that this contributes to a large extend,39% of the respondents indicated they that this contributes to a little extends, 10% of the respondents indicated they that this contributes to a moderate extends and 35% states that this does not contribute at all to the cybercrime. Shown in Figure 4.13.

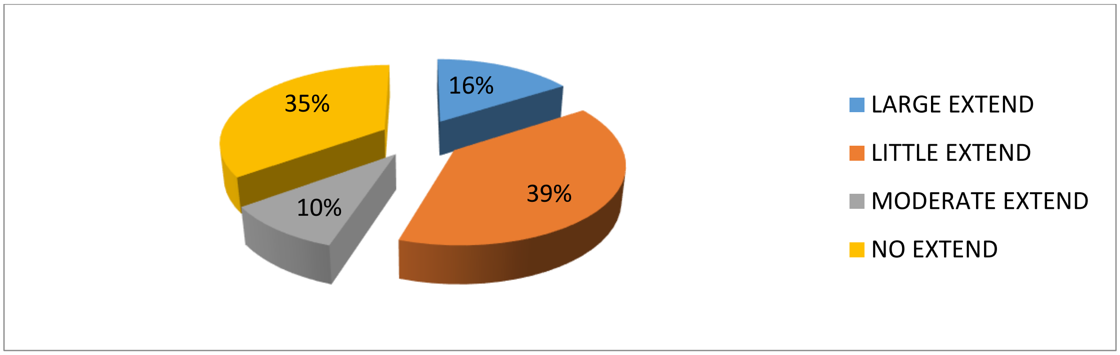


Figure 4.13: Graphs showing how false offers on the internet to share login credentials

Source: Research Data (2018).

4.3.5 False application that appears to be integrated with social network trickling users to install them hence stealing of user access credentials.

The study was carried to know if employees (staffs) receive false applications that appear to be integrated with social network trickling them to install them. Three point two (3.2%) of the respondents indicated that this contributes to a large extend, 51.6% of the respondents indicated they that this contributes to a little extends, 3.2% of the respondents indicated they that this contributes to a moderate extends and 42% states that this does not contribute at all to the cybercrime. This is depicted in graph labeled 4.14 below.

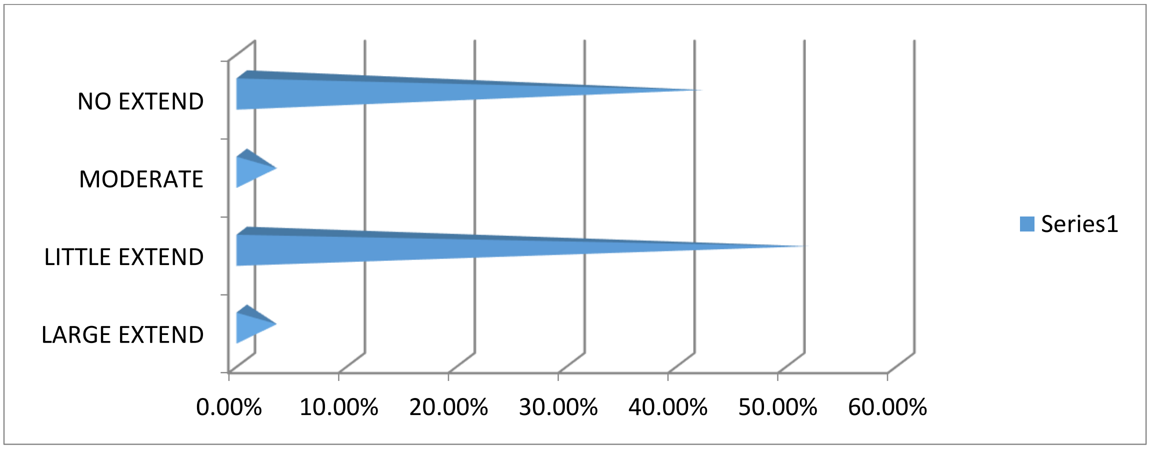


Figure 4.14: Showing how false applications that appears to be integrated in the social networks to share login credentials

Source: Research Data (2018).

4.3.6 External parties hacking into the systems and making calls through them and Denial of Service.

The study wanted to know how accessible is the organizations systems easily protruded by external hackers and making calls through it hence denying them access. The finding were forty five point two per cent (45.2%) of the respondents indicated they that this contributes to a little extends, 3.2% of the respondents indicated they that this contributes to a moderate extends and 51.6% states that this does not contribute at all to the cybercrime. This is depicted in figure labeled 4.15.

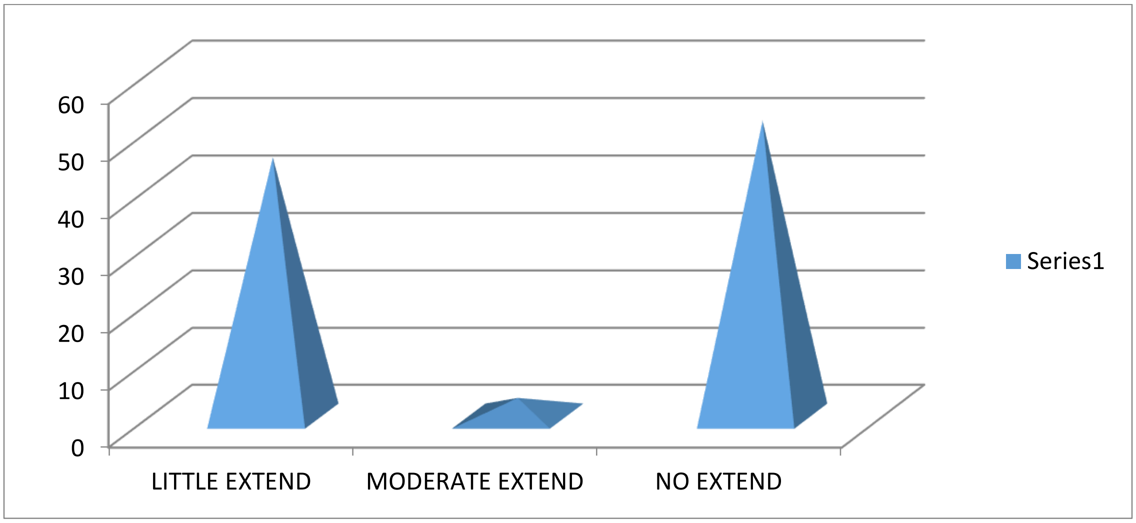


Figure 4.15: Graphs showing how external parties hacking into the systems making call through it and denial of service.

Source: Research Data (2018).

4.3.7 Attempts to access secrets and confidential information stored in the organization's computer and or ICT networks by illegal users.

The study was conducted to investigate from the respondents if there has been an attempt to access secrets and confidential information by unauthorized users. Fifty Eight (58%) of the respondents indicated they that this contributes to a little extends while 42% states that this does not contribute at all to the cybercrime. This is shown in figure labeled 4.16.

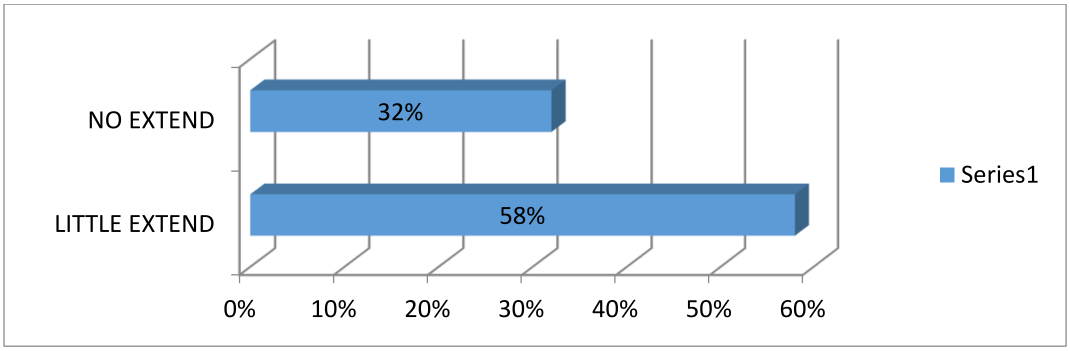


Figure 4.16: Attempts to access secrets and confidential information stored in the organization's computer and or ICT networks by unauthorized users.

Source: Research Data (2018).

4.3.8 Existence of Network Security Policy

The study carried out to find out to ascertain whether the commercial banks had in place a policy touching on network security within the organization. As shown in Graph 4.3.3. The statistic form the research showed that 92.7% of those interviewed indicated that their organization had in place as strong network security policy while a small percentage of about 7.3% indicated they are not sure whether they have that policy of not. The table below shows this representation in form of diagram.

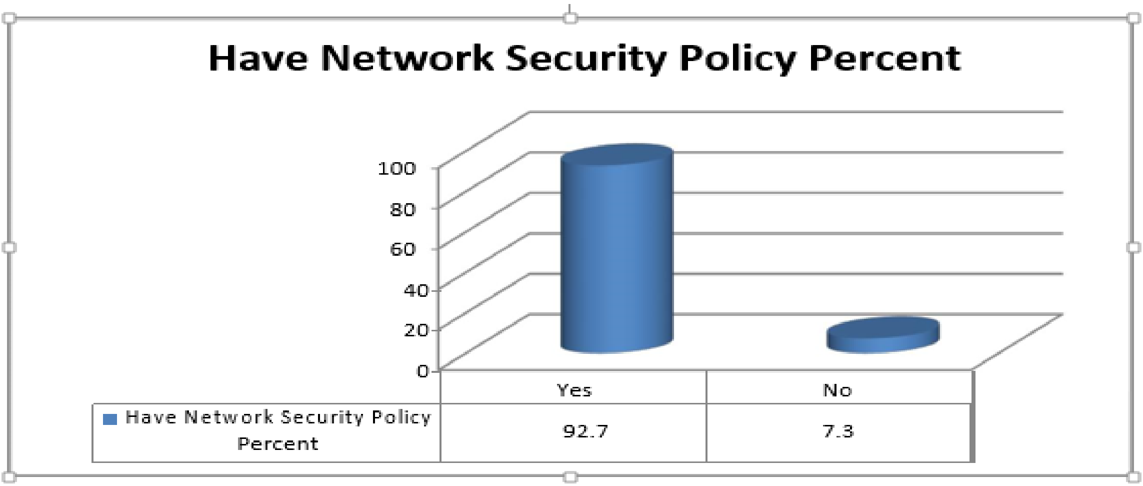


Figure 4.17: Existence of Network Security Policy

Source: Research Data (2018).

4.3.9. Bank use of Antivirus as security control measure

The study was conducted to find out whether commercial banks in Kenya have installed antivirus in their computers to protect from Trojan and malwares. The finding were 95.1% of those interviewed reported that their bank have installed antivirus while four point nine percent 4.9% reported that their individuals banks do not have antivirus installed in their systems. Figure 4.3.10 presents these diverse opinions from the respondents.

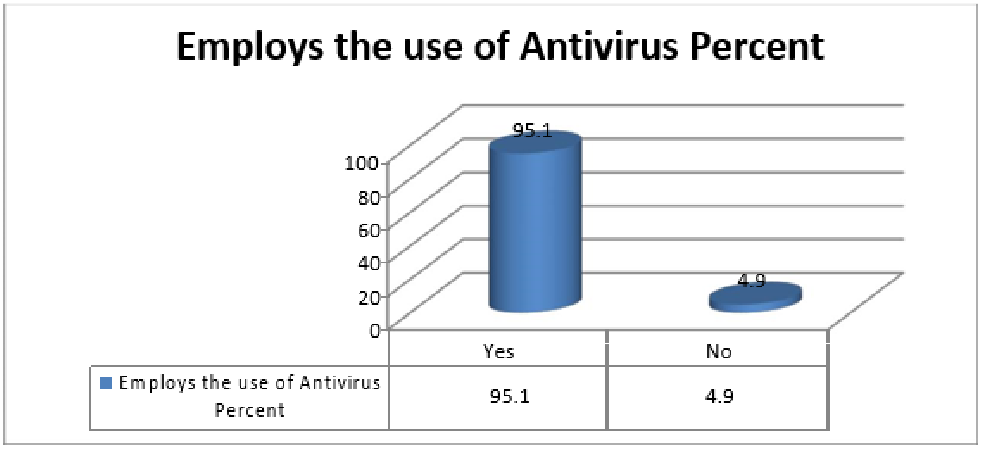


Figure 4.18 Bank install Antivirus as a security control mechanism

Source: Research Data (2018).

4.3.10 Existence of a Firewall

The study also was conducted to assess the level of systems protection through firewalls. The outcome showed that 96.6% of those responded to that questions expressed that their individual banks had strong firewalls while a small percentage of about 2.5% of the reported that they are not sure whether their individuals banks had installed firewalls.

This is represented diagrammatically on Figure 4.19.

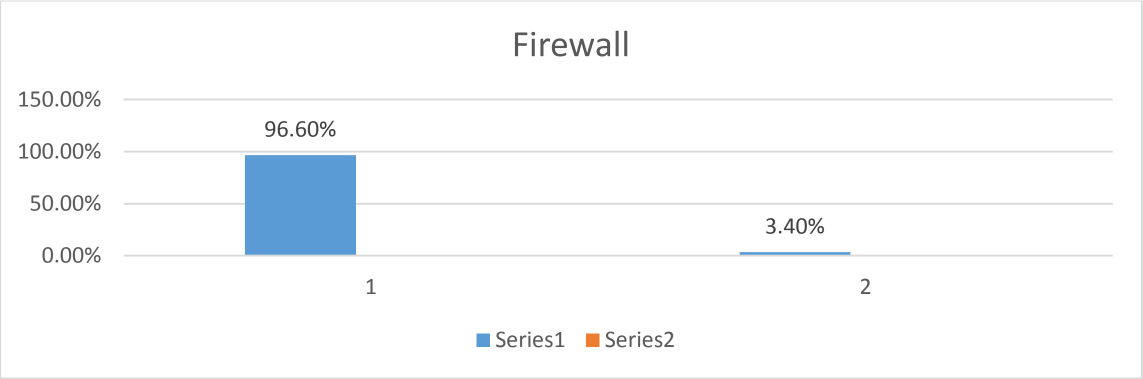


Figure 4.19: Existence and use of Firewalls

Source: Research Data (2018).

4.3.11 The frequency of reviewing Firewall Configurations

The study wanted to investigate how often commercial banks tend to review firewall configuration within their organization. The finding showed fifty two percent (52%) of those who participated in the research reported that they review their firewall often, i.e. within six to eight months; while 43% reported that they review their firewalls very often i.e. within a period of one to three months. The remaining 5% reported that it usually takes time and usually reviewed after one or more than one year (sometimes).

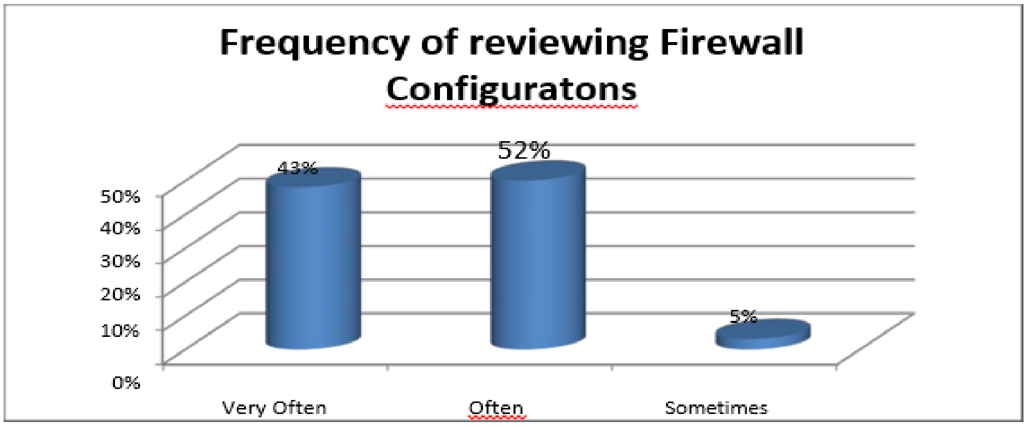


Figure 4.20: Depicts the frequency level of Reviewing Firewall Configurations within the organization

Source: Research Data (2018).

4.3.12 Staff training on Cyber Security

The study wanted to investigate whether ICT staffs have been taken through training regarding cybercrimes. The response were that 75% percent of those interviewed stated that they fully agree that their ICT staffs have undergone security training internally as well as externally; 14.6% on the other hand reported that they strongly agreed that there has been training and campaigns in their organization about cybercrime while 9.8% of the remaining felt that no training has been conducted on cybercrime related issue hence disagreed. This has been represented on figure 4 21.

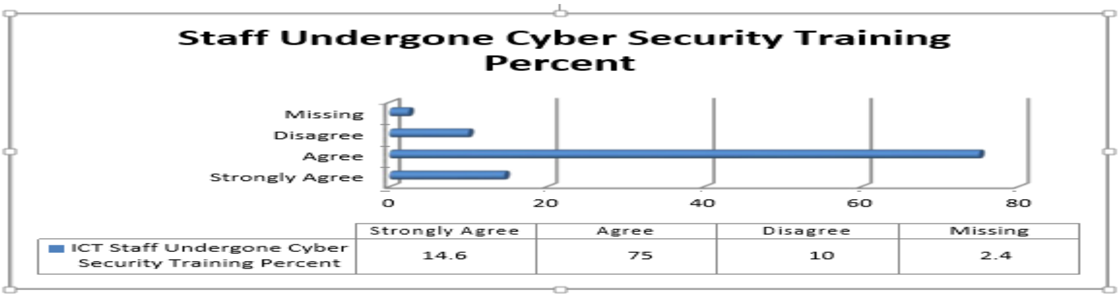


Figure 4.21: Staff training on Cyber Security

Source: Research Data (2018).

4.3.13 Form of customers' authentication: use of passwords

The study was conducted to verify if their banks use any form of authentications. The finding clearly portrays that eighty two point nine percent (82.9%) confirmed that their individual banks use password as form of authentication to access network while seventeen point one percent (17.1%) of the respondents indicated other forms of authentications such as biometrics and staff identification cards.

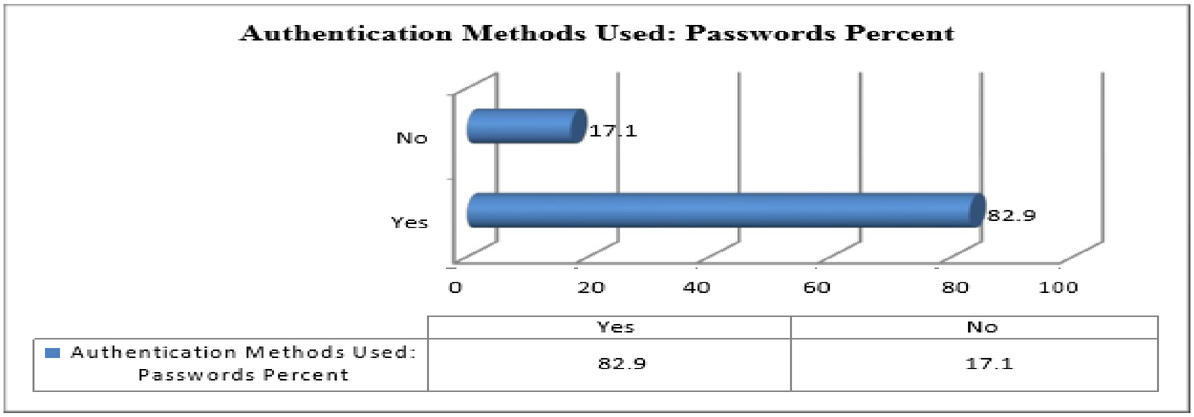


Figure 4.22: Form of customers' authentication: use of passwords

Source: Research Data (2018).

4.3.14 Form of customers' authentication: use of Biometrics

The study was conducted to verify if their banks use any form of authentications. The finding clearly portrays that fifty eight point five percent (58.5%) confirmed that their individual banks use biometrics as form of authentication to access network while thirty nine percent (39%) of the respondents indicated other forms of authentications such as password and staff identification cards while the remaining 2.4 % failed to respond to that questions.

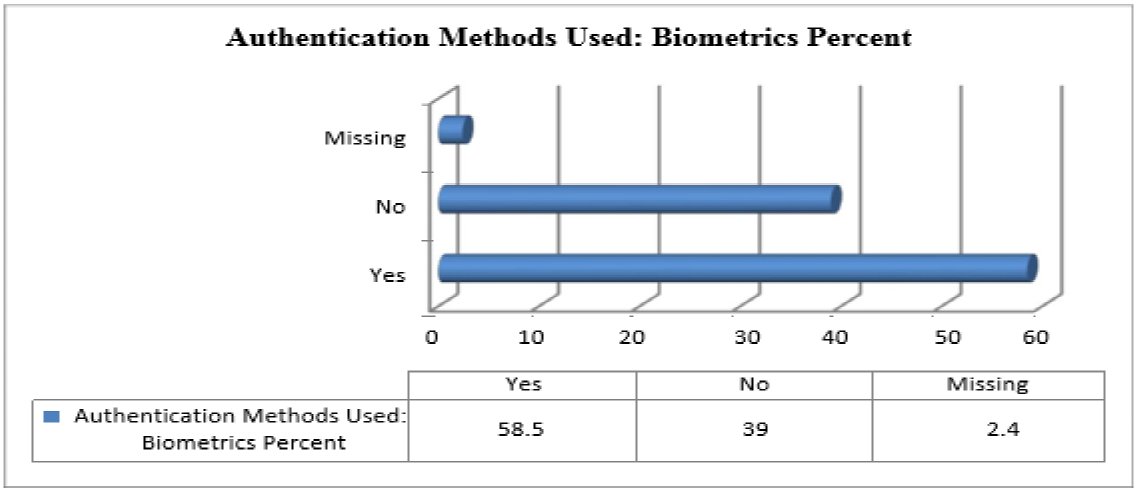


Figure 4.23: Form of customers' authentication: use of Biometrics

Source: Research Data (2018).

4.3.15 Form of customers' authentication: use of staff identification cards

The study was carried out to ascertain if their banks use any form of authentications. The finding clearly portrays that sixty three point four percent (63.4%) confirmed that their individual banks use staff identification cards as form of authentication to access network while thirty six point six percent (36.6%) of the respondents indicated other forms of authentications such as password and biometrics.

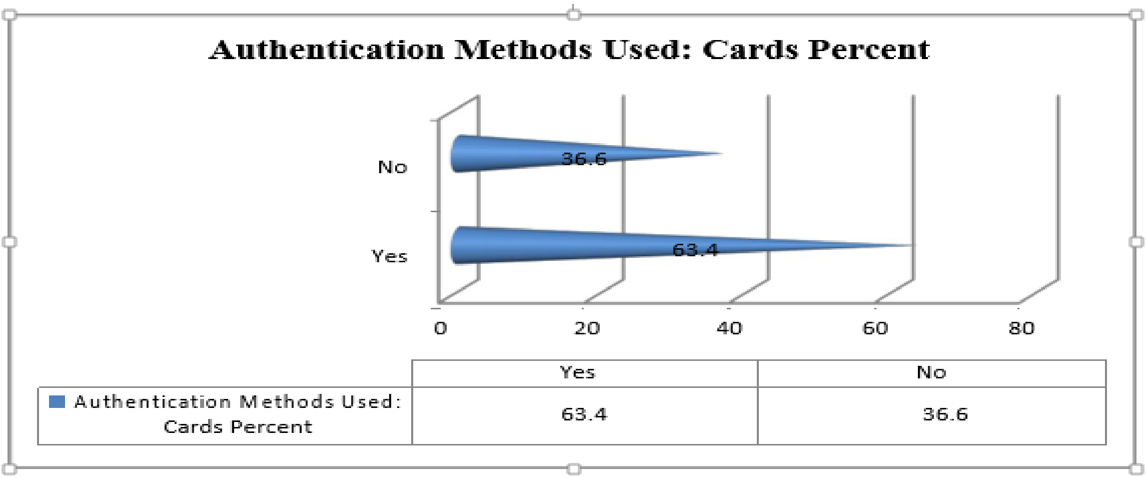


Figure 4.24: Form of customers' authentication: use of staff identification cards
Source: Research Data (2018).

4.3.16 Continues Monitoring of inbound network traffic load on firewalls and systems resources

The study was conducted to investigate if the commercial banks have deployed an invasion discovery system for monitoring of inbound network traffic load on firewalls and systems resource theft. Figure labeled 4.3.16 depicts this form of relationship through the diagram below which shows the respondents responses. 64.5% of those responded expressed agreement to a very large Extend that their banks employed the use of intrusion detection systems, 3.2% of the respondents moderately agrees, 9.7% of the respondents said that this applies to a little extend and 22.6% of the respondents expressed that this is applicable to a large extend on the use of invasion discovery system.

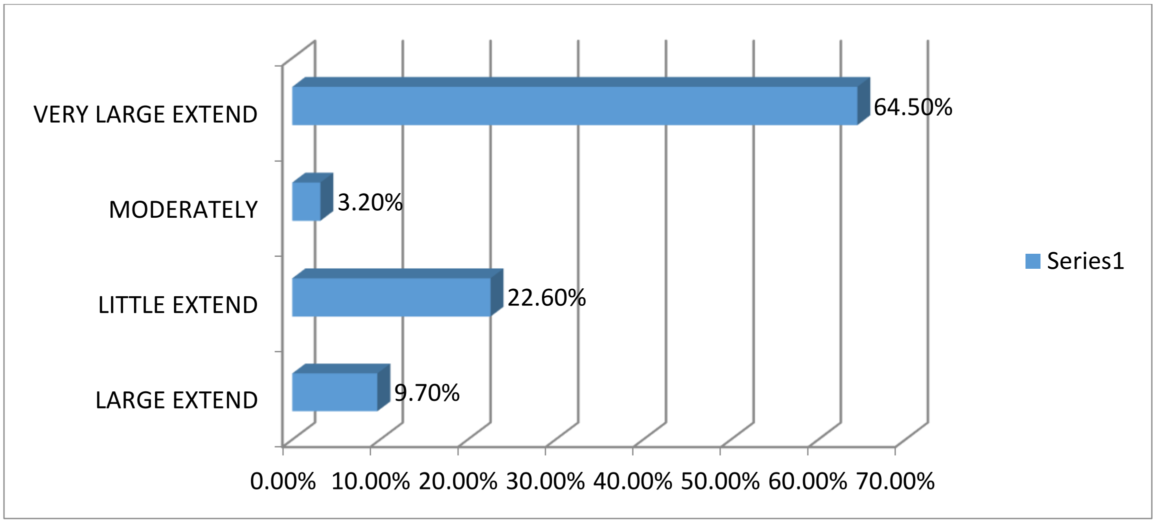


Figure 4.25: Continues Monitoring of inbound network traffic load on firewalls and systems resources

Source: Research Data (2018).

4.3.17 Forms of data storage and transmission

The study was carried out to investigate various forms the banks store and transfer their data in, whether encrypted or not. Seventy one percent (71%) of the respondents expressed agrees to a very large Extend that their banks stores data in a encrypted format, 16,10 % of the respondents agrees with this to a little extend, 6.5 % moderately and 3.2% of the respondents expressed that this is applicable to a no extend or Strongly disagree.

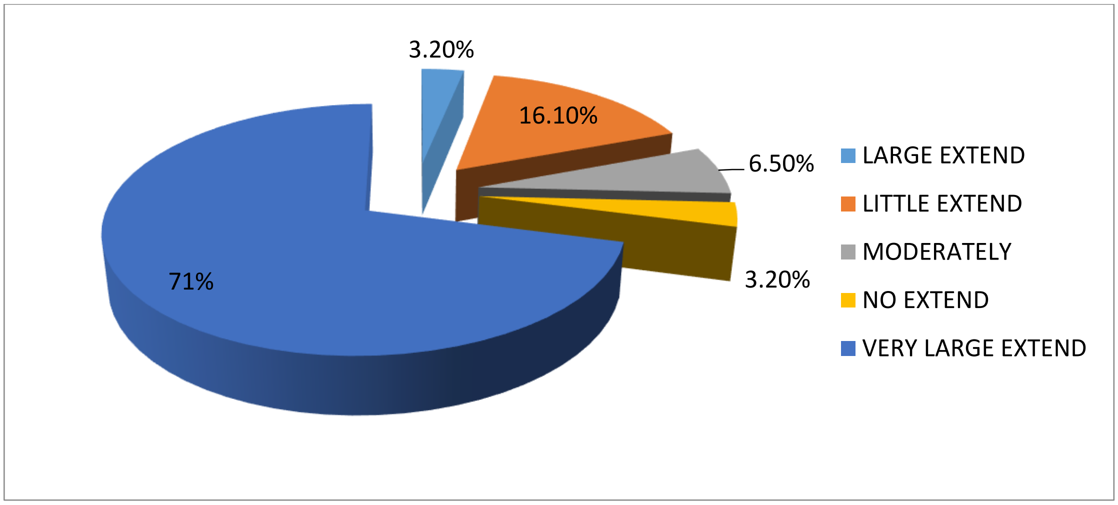


Figure 4.26: Forms of data storage and transmission

Source: Research Data (2018).

4.3.18 The frequency of updating and patching of organizations' software

This research wanted to investigate how often bank updates their software as a cyber-security prevention strategy. The outcome was shown on the figure labeled 4.27 which showed that74.2% of those who responded recorded that they update their software very often, to a very a large extend between, 19.3% or the respondents expressed that they update frequently but not very often and 6.5% of the respondents expressed that they update relatively often.

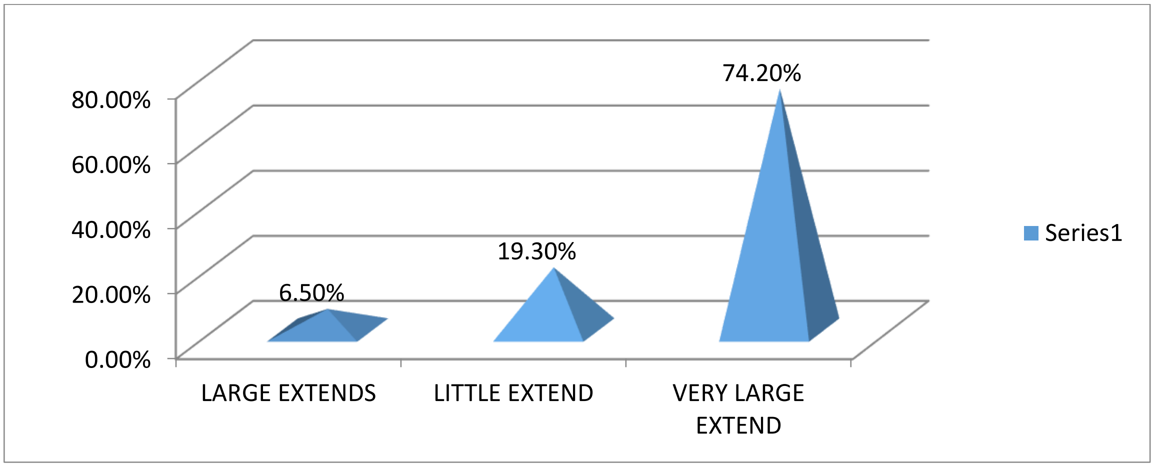


Figure 4.27: The frequency of updating and patching of organizations' software
Source: Research Data (2018).

4.4 Assessing the level of effectiveness of Prevailing cybercrime Regulation

4.4.1. The level of reporting cases of cybercrime attacks successful blocked

The research intended to investigate if Kenya commercial banks reported upsurge instances of successfully blocked cybercrime attacks. Fifty Eight percent (58%) of the respondents stated that they strategies worked efficiently and to a very large Extend while 42% of the respondents stated that the strategies contributed greatly to a large extend on the successfully blocked attempts. Above statistics is represented on the figure labeled 4.28

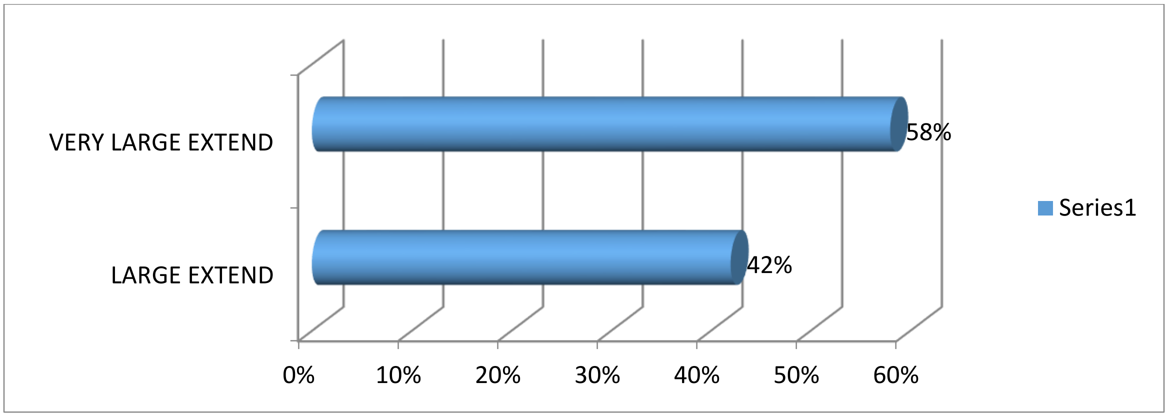


Figure 4.28: The level of reporting cases of cybercrime attacks successful blocked

Source: Research Data (2018).

4.4.2 The frequencies of Firewall policies review

The research was carried out to investigate the duration upon which commercial banks in Kenya review their firewall policies. The finding from the research showed that 68.1% of the respondents indicated they reviewed their firewall policies between 1-6 months (very large extend), 28.9% of the respondents indicated they reviewed their firewall policies ranging in between 8-24 months (large extend), 3% of those who responded expressed that their individual banks reviews their policies regarding firewalls in spread of more than two years and above which is Moderately.

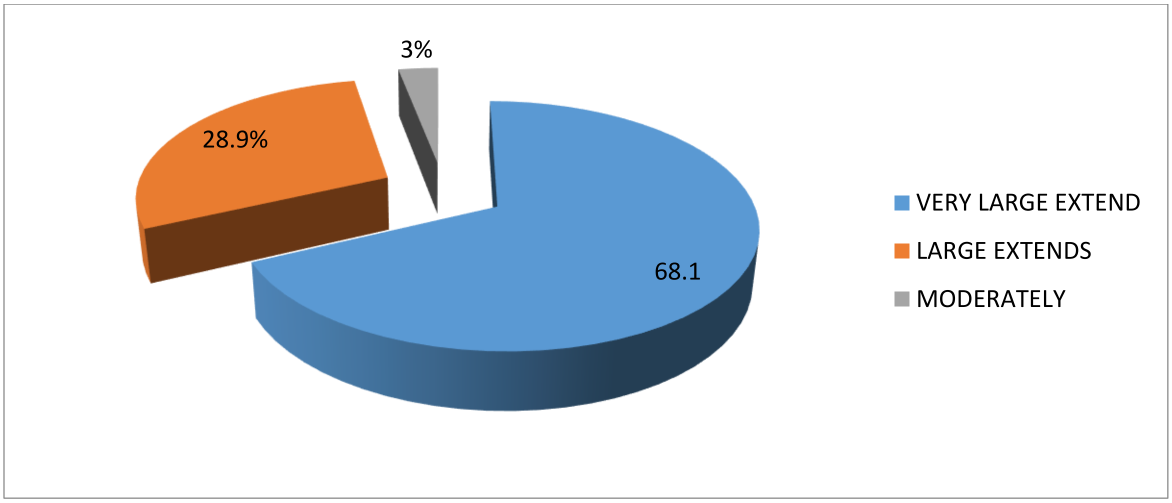


Figure 4.29: The frequencies of Firewall policies review

Source: Research Data (2018).

4.4.3 Existence of Security Policy within the Bank

The study sought to if the bank is operating under cyber-security policy as a mechanism of curbing cybercrime incidences. Out of 42 of those who responded, ninety three percent 93% admitted that they there exist a policy governing cybercrime, 4% disagreed and said that haven't come across such policy touching on cybercrime, the remaining 3% of the respondent were not sure if the cyber security policy was in place or not.

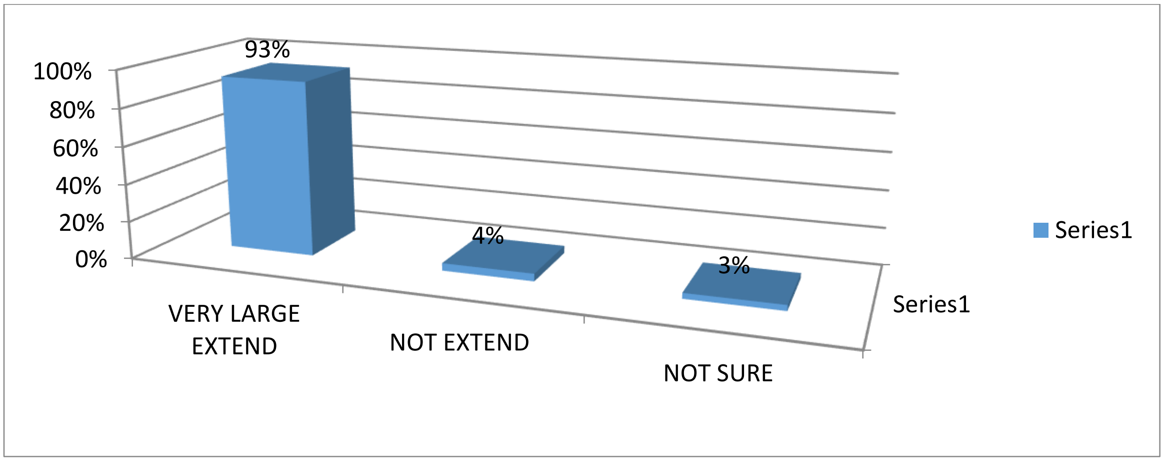


Figure 4. 30: Existence of Security Policy within the Bank

Source: Research Data (2018).

4.4.4 Maintenance of confidentiality of the privileged information stored in the organizations computer of ICT Network.

The study was conducted investigate to what level are the employees aware of the policy concerning confidentiality about the privileged information stored in the organizations computer of ICT Networks. The findings were that 67.5% of those who responded expressed greater level of knowledge about this policy. However thirty one point seven (31.7%) of those who took part in the survey said that they were not aware of this policy concerning protection of confidentiality of organization information.

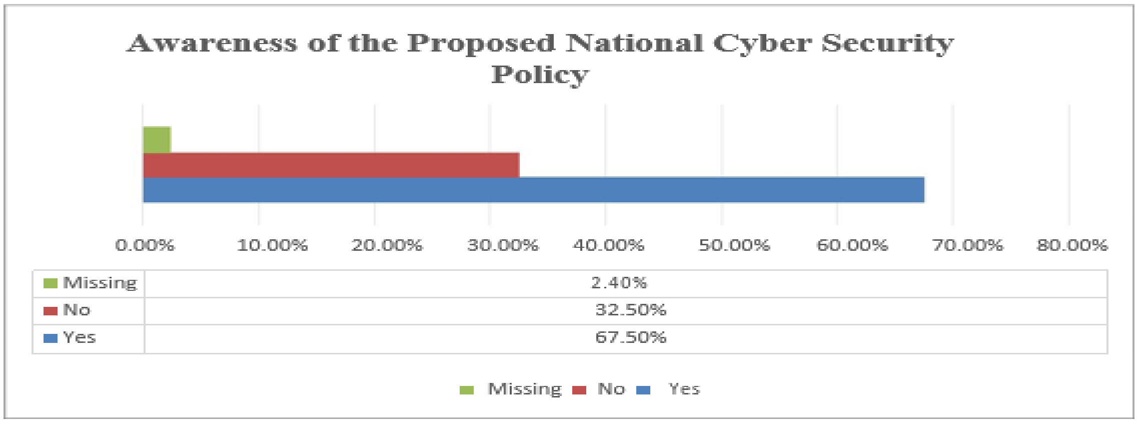


Figure 4.31: Maintenance of confidentiality of the privileged information stored in the organizations computer of ICT Network

Source: Research Data (2018).

4.4.5 Maintenance of integrity of information stored in the organizations' computer or ICT Network.

The study was conducted to investigate how employees maintain integrity when it comes to protecting organizations' data as well and network system. The outcome was that sixty eight point four 68.4% of those who responded respondents agreed with this to a very a large extend networks and data from the organization as protected and employees upheld their integrity, 15.6% of them but just on a large extend. 15.9% of the respondents expressed that they disagreed showing no extend at all

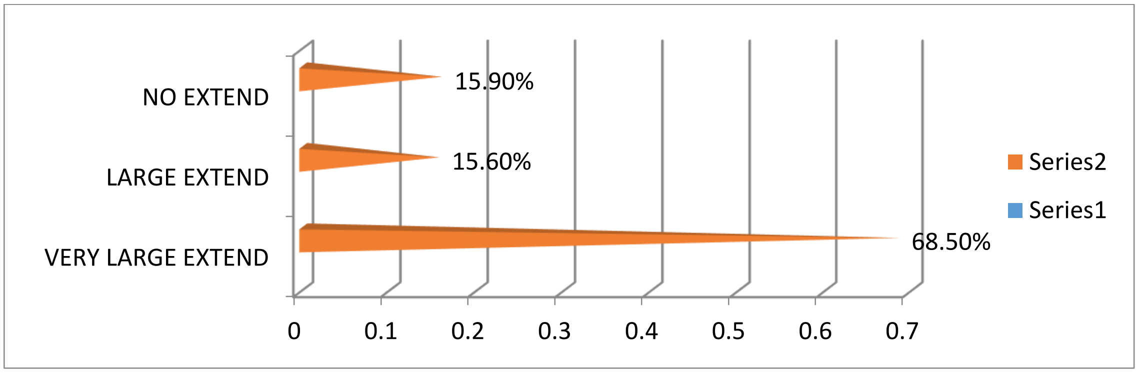


Figure 4.32: Maintenance of integrity of information stored in the organizations' computer or ICT Network.

Source: Research Data (2018).

4.4.6 Staff education by banks on the importance of protecting themselves against cyber related crimes.

The study carried out to evaluate if the banks has conducted staff educations on the importance of protecting themselves against cyber related crimes. The results showed that Fifty four point two Percent (54.2%) of those who responded agreed to a very large extend21% however strongly disagreed, 12.8% disagreed to a little extend that they had educated staffs and finally 12% of the respondents indicated that they strongly agreed to a large extend their staffs were well educated to enable them protect themselves from cyber-attacks.

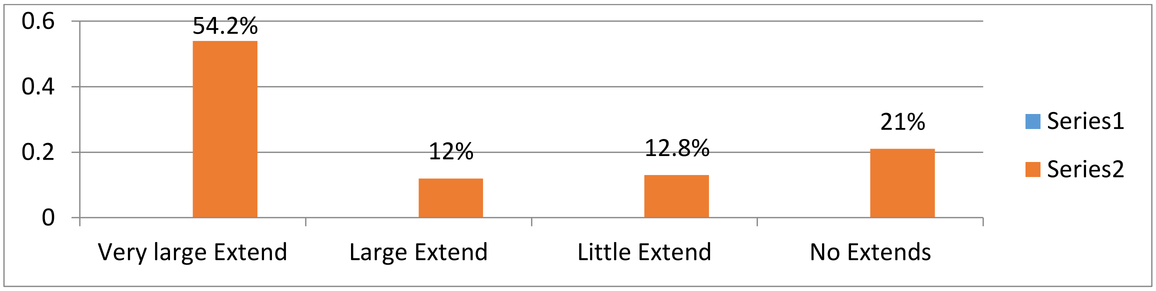


Figure 4.33: Staff education by banks on the importance of protecting themselves against cyber related crimes

Source: Research Data (2018).

4.4.7 Knowledge about social engineering by staffs

The study was conducted to assess what level staff understands social engineering and its linkage to cybercrime. The findings were 51.5% of the respondents stated that they agreed to a very large extend meaning that banks employees were well educated and equipped with knowledge about social engineering; 34.2% of those who responded strongly disagreed indicating no extend at all. 10.1% of the remaining responded moderately agreed that the institutions employees had been educated to recognize social engineering and finally 4.2% of agreed to a large extend meaning that banks staffs had been trained about social engineering and its impacts on organization

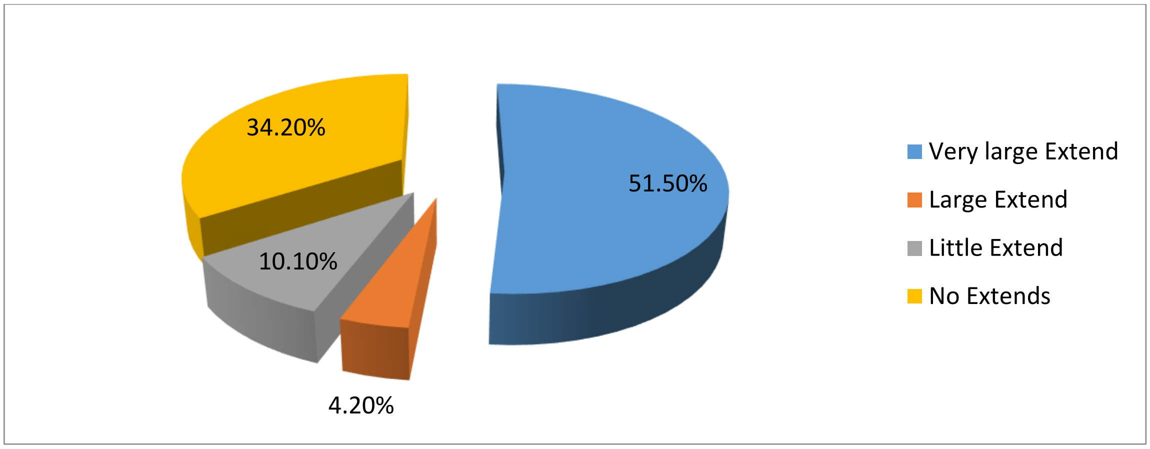


Figure 4.34: Knowledge about social engineering by staffs

Source: Research Data (2018).

4.5 Discussion of the findings

This section basically provides meaning about the results and the findings from the study. This study examined cyber securities strategies in relation to the online banking implementations within commercial banks in Kenya. The Key variable that was analyzed was the ICT frameworks and policies in place, staff competencies and security awareness amongst them, and finally risks management systems with the organization. The study sought to highlights gaps in the Kenyan commercial banks pertaining cyber securities strategies with the aim of recommending further areas for study. This study presents countermeasures that need to be employed in the banking sector to help in managing cyber related attacks and put in place means of detecting such attacks so as to ensure that banking sector is safe and if attacked are capable of speedily recovering from an attack.

4.5.1 Determining the Level of preparedness in terms of Cyber related threats in Kenyan banking sector.

This is one of the important concepts that banks need to ensure that enough resources have been invested to secure their systems from cybercrimes. Tendulkar, (2013), further emphasized this by starting that a stout security measures are key in mitigating the effects of cyber-attacks. Findings discussed above clearly supports the arguments where Ninety three Percent (93%) of the responses reported to have strong network security policy.

Security control measures need to be adhered to and often checked, updated and outdated ones replaced. Majority of the respondents acknowledged the need of having strong Firewalls to protect organizations' networks. Organizations' network security framework must be well furnished all the time. Controls such as right of entry and software update should frequently done, regularly reviewing security configuration and installation of new software (Siddique & Rehman, 2011). The findings showed that close to 96.6% of the respondents had their firewalls properly maintained while 3.4% per cent were not fully certain about the status of firewalls in the company. Siddique and Rehman (2011) supported this argument that all request from external networks to the secured network go through a firewall.

The study reports that Fifty four Percent (54%) of the respondents agreed to a very large extend that their staff are well educated to aid in systems protection against systems-attacks/ Twenty one per cent (21%) gave a contradicting opinions that they don't believe that their staffs are well trained to handle these attacks; 13% per cent disagreed to a little extend that their staffs were well educated and another 12% of the respondents indicated that they strongly agreed to a large extend that the organizations that they are working for have fully trained their staff and are able to handle cyber attack whenever it comes.

These findings concur to what Tendulkar, (2013) had stated that Cyber-safety mechanisms are often overlooked especially when the crime is orchestrated by internal employees. Staff Training should be made compulsory given that there are new innovations of cybercrime as the systems change; training is best strategy that needs to be performed keeping staffs well informed about the current development by the attackers.

Control strategies such as internal network control measures must be properly maintained. These access controls and software updates must be updated more frequently installing the most current antivirus and invasion detection applications (Siddique & Rehman, 2011). It is from this study that it was found out of 31 respondents 95.1% per cent reported that their individuals' banks adopted security mechanisms such as antivirus. Furthermore, the sampled 31 banks installed various access control method. Eighty two per cent (82.9%) of the responses showing that their bank widely use passwords as form of authentication methods to access organizations Network. Simmons (2012) also agreed with these securities proposed measures stating that it's critical for organizations to be always on the looks to ensure that both physical security and computer are well protected.

Risks management systems entail comprehensive process with regards to physical, technical and administrative controls. Bhasin (2007) recommended that a comprehensive approach need to be undertaken including technical, human and technological approach in order to controls such kind of risks. From the research, the study showed that Seventy one percent (71%) of the respondents expressed agrees to a very large Extend that their banks stores data in an encrypted format, hence in agreement with Bhasin (2007) who posits that banks who are continually transferring Data across networks must ensure Data Encryption is adhered to as well as policies and measures addressing cybercrime.

Siddique and Rehman (2011), advised on the use of 3 security deterrent procedures. Firstly, the banks are supposed to have a defense package that has control over any cookies, preventing data channeling to other unspecified. Secondly, he advised that it is vital to always use the new developed software updated with the newest patches closing loopholes attackers use to gain access into the systems.

The Findings on how frequently organizations patch their software reported that that74.2% of the responses expressed that they update their software very often, to a very a large extend between, 19.3% or the respondents expressed that they update frequently but not very often and 6.5% of the respondents expressed that they update relatively often. The findings indicated tha 65.9% per cent of the respondents acknowledged that the cybercrime committed through social engineering is currently gaining momentum.

4.5.2 Effectiveness of strategies/countermeasures on Cybercrimes in the banking sector in Kenya.

From this research, 93% per cent of the respondents them confirmed that their organizations have policy of cyber security in place. The respondents were asked how secure their information are and how the strategies adopted help to maintain the integrity of the data stored in those systems; Forty four Per cent (44.2%) of the responses stated that their organizations are in the process of implementing such policy governing crimes committed through online platforms. This is in accordance the Kenya Cyber Security strategy was developed and launched in 2014.

According the Research by Wang, (2007), the argued in the sense that current technologies create avenues allowing criminals to develops new crimes. This has resulted into upward trends of such crimes. The new vice is clearly portrayed on this studies under the Kenyan Context, 59.1% of the respondents indicated that there has been an upward trend on cyber related crimes.

Commercial Banks operations have been taken a notch higher to enable customers to operate their bank accounts at the comfort of their homes via electronic means (Rashid, 2011). Kenyan banks revealed compliance to this as 89.1% of the responses interviewed indicated that their banks allow online banking for their customers as well as their internal staffs. Hundred percent (100%) of the responses reported that their banks use of Technology to give efficient service to their clients. The responses gathered from the sample populations on the authentication methods revealed that 92.6% of the respondents indicated their banks uses one form of the other as a security means of authentications.

According to Amoroso (2011), he said that it is essentials to train all the users who make vital decision within the organization. The application of access codes is one such mechanism that is used to authenticate users. He further stated that in order to attain full compliance staff need to be trained and made aware of the associated risks in any form of behavior that portrays may either damage or redeem the image of the organization and leading to loss through security system manipulation.

4.5.3 Employee level of Competence and Awareness

As earlier discussed, most of the cybercrimes are usually committed by the insider or the link between the insider and the outsider. Human beings are usually the weakest link with the organization systems. Failure to manage this weak links may lead to unauthorized in the process of data movement, for example, when transmitting data from one point to another. India (2000) strongly proposed that the use of digital signatures to validate data and documents transmitted by electronic means and application of logon keys to authorize users to encrypt data. Bank should implement security control strategies e.g Data cryptography (Schulz, 2006). This study strongly supports the same where 93.8% of the respondents indicated that in their systems employs cryptography as a security strategy.

The study fully concurs to the notion that staffs need to under thoroughly vetting process prior to being on boarded. Similarly procedures should be undertaken when promoting staffs since they these staffs are prone to accessing sensitive and more confidential data as they gain more responsibilities. Kris’s and Belicove (2012) said that employers are deviating nowadays and tend to overlook work history of their new employees. This study largely concur with the above recommendation in that 68.4%) of all the respondents recorded that they their organizations usually perform thorough check before formally engaging employees into signing contracts.

Verizon (2012) reported that more than three quarter of cyber-attacks in 2012 were committed through social engineering. Seventy six point three (76.3%) of all the respondents reported that they concur with this to a very large extend that the organizations employees had been well trained to distinguish social engineering. This numbers is on a lower end considering the impacts of cyber-attacks in commercial banks. Youga and Singh (2013),strongly proposed that staff needs to be equipped with adequate skills regarding on social engineering in order to be able to identify loopholes that intruders use to gain access into the system.

In spite of the plausible stringent firm's laws regarding network usage policy, some of the employees still goes again these policies and give out their credentials, access unprotected social sites thereby exposing the organizations to cyber-attacks. Those of the different opinion argued that this draconian security tactics are purely fallacies, the real source of risk is untrained human element. Internet Safety (2015) supports this by identifying social sites as the main sites being targeted by criminals. The report states that users must comply with the laid down policies for managing the emails. The research finding went contrary to the above recommendations.

Raval, (2010) stated that over time, as technology increases and new developments and innovation come into play the desire for information is as well increasing at the same rate. There is need for capacity utilization leading to reduction of cost of accessing these services. This therefore results into sharing through virtualization growing and creating a much wider spectrum, called as cloud computing. The study showed that about 61.1% per cent of the responses record that the organization they are working for use cloud computing as safer havens for data storage. (Cadregari, 2011) Despites the positive benefits of this form of data storage, there are a myriad of challenges concerning this argument, there is a greater need to take great care of the potential harm caused by criminals and hackers getting access to this vital information stored in the clouds due to centralizing of information sources.

The study to a greater extend agreed that environment with low awareness and lucidity could intensify the effects of cyber relates attacks. Low awareness level may imply that key players are likely to be misled by a new vices developed finding themselves lacking suitable tools to alleviate such attacks. Furthermore instances where transparency is completely left out there has been increasing cases of cyber-crime (Tendulkar, 2013). This argument is fully in agreement by this study, whereby around 79.7% per cent of the respondents indicated initials cases of cyber crime had rapidly increased due to lack og sharing information within the organization setup.

4.5 Chapter Summary

In summary, the study was conducted to investigate the effect of cyber security strategies on online banking implementation within commercial bank in Kenya. Data was collected from 31 ICT staffs and staffs in charge on online banking. This study targeted a sample of 41 head of ICT in each bank.

Out of the 31 response received, 23% per cent were falling below 25 years of age, and 48% were in between 26 to 30 years, 26% ranged in between 31 to 35 years and 3 % said that they were between 36 to 40 years. Both genders were fairly represented with a bulk being males, contributing 71% of the total sample size. Ninety Four (94%) of those who responded were graduates while 6% had postgraduate qualification.

The sample population greatly contained ICT staffs in holding various positions within the bank. The demographic data was very important validity and verification purposes. Out of the sampled populations of 42 respondents, 62.6% of those who responded strongly agree to a very large extend that their individuals' banks employed usage of technology to serve their clients.

The study was carried out to find out the respondents knowledge of whether mistakes committed by employees leads to cybercrimes. Fifty Eight (58%) of the respondents indicated that this contributes in little extend while 39% of the respondents indicated they that this does not at all contributes to the cybercrime and 3% agrees that this contributes moderately to cybercrime. Ninety two point seven percent (97.5%) of those who responded expressed that their banks installed strong firewalls, 2.5% however disagreed.

The findings were, fifty four Percent (54%) of the respondents agreed to a very large extend that staffs' knowledge and awareness was very high however 21% of those who gave back their responses recorded that they strongly disagreed, 13% of the responses disagreeing but to a little extend that they had educated staffs and another 12% of the responses received recorded that they are in strongly agreement to a large extend that they had trained staffs to guard themselves from cyber-attacks. As regards to the Data protection and storage, Seventy one percent (71%) of the respondents expressed agrees to a very large Extend that their banks stores data in a encrypted format, 16.10 % of the respondents agrees with this to a little extend, 6.5 % moderately and 3.2% of the respondents expressed that this is applicable to a no extend or Strongly disagree.

From various responses received from those interviewed about cyber security policies, ninety three percent strongly agreeing that their individual banks have in place governing cyber security related concerns, however, 7% disagreed and went further to state that they haven't come across such policies with their organization. On the issue of staff training and awareness campaigns, 75% of the responses strongly agreed that the ICT staff have undergoing training pertaining securities issues affecting their banks more so on e-platform. Fourteen percent (14.6%) showing agreement but not on a large extends, the remaining 9.8% reported their disagreement that their ICT Staff have been taken through series of training concerning cybercrime.

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter looks at the outcome and the findings from the study presented in chapter four. This entails the rationale of the study, research objectives and methodology applied discussed in details. Later in this chapter research summary has been given with the research question given linking key variable discussed in an attempt to answer the question about the effects of cyber securities strategies that affects online banking implementation within the commercial banks in Kenya. Brief discussion conclusion and recommendations for further development are then presented.

5.2 Summary

The main objective of the study was to find out the effects of cyber security strategies on online banking implementation in Kenya precisely on Commercial Banks. The study addressed the objective.

To find out the effects of cyber security strategies on online banking implementation within Commercial Banks in Kenya

The research design used was descriptive in nature. Data was therefore collected from 42 responses from ICT staffs and staff managing online banking. To select the respondents for this study, it was agreed that head of ICT department within each commercial bank was interviewed and where he/she was unavailable, a representative was interviewed. Data gathered from primary sources were edited, assigned codes, analyzed using Microsoft Excel and SPSS software, and finally interpreted into meaning forms. This was then presented in the form of pie-charts, percentages, figures, tables and bar graphs.

The outcome from the study about online banking adoption and implementation within commercial banks in Kenya revealed a 100% usage in carrying out most of their transactions electronically. Out of 31 responses received 93 per cent confirmed that their banks had policy governing cybercrimes issues while 4% of them specified they did not have a cyber-security policy while the remaining 3% of the respondent were not sure if the cyber security policy was in place or not. Close to 95.1% per cent of the responses received indicated that they use an antivirus to secure their systems from external attacks.

The other key finding was on the level of effectiveness of these said regulations. Fifty Eight percent (58%) of the respondents stated that they strategies worked efficiently and to a very large Extend while 42% of the respondents stated that the strategies contributed greatly to a large extend on the successfully blocked attempts. On the national proposed cyber security policy 67.5% per cent of the responses reported that they were fully aware of the national policy on cyber security.

Seventy four point two per cent (74.2%) of the responses expressed that they update their software very often, to a very a large extend between, 19.3% or the respondents expressed that they update frequently but not very often and 6.5% of the respondents expressed that they update relatively often. The other security aspects that was analyzed is on the firewalls and how often their update their software. The findings were Sixty eight percent (68%) of the responses indicated they reviewed their firewall policies between 1-6 months (very large extend), 29% of the respondents indicated they reviewed their firewall policies between 7-24 months (large extend) while 3% of the respondents indicated they reviewed their firewall policies in more than 24 months (Moderately).

The feedback gotten from the third variable about staff competencies and level of security awareness showed that. Seventy Five percent (75%) of the responses strongly agreed that their ICT staffs have undergone training about cybercrimes; 14.6 per cent agreeing to a little extend while 9.8 per cent indicated that they strongly disagreed with the notion that security trainings are frequently done.

5.4 Conclusions

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

The study exposed that policies indeed plays a critical role as far as cybercrime is concerned. Most to the respondent fully agreed that the availability of those properly formulated and documented policies that helped their bank overcome cases of cyber-attacks, the statistics clearly show that commercial banks have a clear understanding the concepts cybercrime and its impacts in the banking industry, and the need to safeguard themselves through their behaviors.

Commercial banks also need to carefully adopt preventive control strategies such as putting strong firewalls in place as well as protecting their electronic gadgets using current and updated antivirus. To supplement this, commercial banks employs access permission control strategies to authenticate all their users. Proper investments and budget allocation should be channeled in training their ICT personnel as well as their staffs on issues about cyber security. It was noted from the findings that training of Non ICT staff and their customers has not been prioritized as compared to that of the ICT staffs. The study also discovered that invasion detection mechanisms as well as cryptography mechanism have not been fully adopted as a key means of protecting of data access from unauthorized people.

5.4.2 Evaluating the Effectiveness of Existing strategies/countermeasures on Cybercrimes within commercial Banks in Kenya.

The study largely reported that commercial banks have embraced to a greater extend the application of technology to perform its day to day operational duties thereby increasing efficiency and accuracy within their transaction. This as a result moves their services closer to their clients through increased working hours, offering self-service machines such as ATM machines, online as well as mobile banking. The study further purported that despite these advantages, commercial banks are fully aware of the increased cases of cybercrime.

The study further exposed that 56% of the staffs knew about the proposed Cyber Security Policy. Despite the upward trend in cybercrime in commercial banks locally and internationally, majority of the respondents showed that they had not reported fewer cases are being reported due the fear of damage and exposure to that organization. This is however contrary to the spirited campaign by the Kenya Bankers Association launched in 2015 to promote awareness to their clients on how to protect themselves from these crimes. Finally this study further showed that commercial banks need to emphasize the need of having well research, articulated and tested policies which detect all forms of unauthorized access and blocking them. Caution should be taken to have in place policies which are able to recognize all failed log on attempts thus reducing the chances of a hacker accessing into the banks systems.

5.4.3 Evaluating Employee Competence and Awareness in Influencing Cybercrime in Banks

The study acknowledged consider able numbers of disgruntled staffs were not properly handled within the organization. Furthermore, the study further agreed that commercial banks scrutinize their employees before bringing them on board and when promoting their staffs. The study proceeds to disclose the attempts that have been put forwards aiming towards educating their employees to appreciate and cautiously handle social engineering. However, the study recommends additional more efforts to be geared towards this course. The other gaps identified are on social media usage. Most of Commercial banks are yet to fully implement policy regulating the use of social media as a communication channel. Whenever using this channel, issue such as monitoring should be properly addressed as they may be able to regulate the level of damage and reverse negative publicity. This was revealed through the study that only few banks complied.

5.5 Recommendation for development

The findings and outcome from the study identified a number of areas that require developments in order to reduce crimes committed on the cyber space. This will also aids in strengthening the cyber securities strategies used in commercial Banks in Kenya. The areas to be improved include risks management system in terms of the level of preparedness to curb incidences of cybercrime, secondly is on use and effectiveness of the existing regulation by ICT infrastructure and lastly on the staff competencies and awareness level about cybercrime related issues. These are discussed below in details.

5.5.1 Risks management systems in terms of Level of preparedness to curb Cyber Security threats on Commercial Banks in Kenya.

From the study that was conducted, it’s therefore recommended that Commercial banks need to improve on their risk management systems through formulation of preventive mechanism for instance having strong firewalls installed and updated frequently. Furthermore, commercial banks need to improve on their access permission control mechanisms for authenticating all their staffs. These forms of risk management system should work on the basis two level approvals, where once the request has been initiated; it has to be approved by a second party. Finally as an oversight role, management need to invest heavily on training and awareness creation on all their employees and well as extend awareness campaigns to their esteemed clients. Invasion detection mechanism should not as well be forgotten but instead supplemented with other control measures in commercials banks to ensure all their systems are properly secured.

5.5.2 ICT security management systems in terms of effectiveness of existing controls as well as regulation on Cybercrimes in Kenya.

The results from the study showed that most of the commercial banks in Kenya were fully informed about cybercrimes and trained on the need of strictly following the controls measures put in place by ICT department. This is adhered to but not to the satisfactory levels (100%). There its recommended that full compliance must be reported in term of password protection, locking of systems full time, continues reviewing of login credentials and following strictly proposed national security measures governing commercial banks operations. Reporting any form of suspicion to the authorities was also reported to be low. This therefore needs to be improved. The proposed national security policy when adopted will help the entire country as a whole to develop specific policies and measures in line with their operation to safeguard not only individual owned networks but also National networks.

Furthermore, commercial banks through ICT infrastructure should enforce full implementations of access control policies such as monthly or weekly reactivation of individuals staffs profiles as well as resetting of access codes after a specified period has elapsed. Modern intrusion detection devices need to be installing to detect unauthorized attempts to hacks the systems through numerous failed logs on attempts. The blocking features should be fully operational to block users once a number of login attempts have been exceeded.

5.5.3 Determining staffs' Competence and Awareness level to curb Cybercrime in Banks in Kenya

This is an area that cannot be assumed. From the review which was fully supported by the finding from the study showed that ninety per cent of those reported cybercrime were committed through internal staffs as well as outside staffs. There has direct links between internal staffs and outside staffs where internal staffs disclose organization data to the outsider. This created avenues where criminals are able to hacker into customer accounts hence stealing huge amount of money. Other crimes are directly committed by internal staffs by colluding with their partners to defraud banks accounts.

As results of these reported trends crimes being committed through staffs, the study strong recommends that employees should be thoroughly vetted before on boarding them and during promotions since they will handling more sensitive information. There need to be continues training on social engineering as it was reported that criminals use this channels to hack banks systems. Investment in training of staffs may not give immediate reward in terms of profits but will help the organization to protect their systems from external attacks as well as internal attacks.

Staffs should be undertaken through several sequences of training, awareness campaigns on the importance securing their systems and the outcome if systems are not protected from cyber-attacks. Commercial banks need to fully adopt the use of social media as a communication strategy awareness creating as well as employ some staffs to monitor and manage socials sites. This strategy helps to perform damage control or reverse negative publicity caused by disgruntled internal and external clients.

5.6 Limitation of the Study

Although the results can be considered statistically significant, the study had a number of limitations. To begin with, the study was based on the effects of cyber security strategies on implementation of online banking. The study therefore excluded other financial institutions which might have been affected directly or indirectly by the cybercrime within commercial banks in Kenya. The study however considered all the commercial banks since they are the key players in the industry and they were the most hit by the cybercrime. Secondly, the research was carried as a descriptive research design in the banks' head offices in Nairobi, thus the study did not get divergent views from other banks' branches across the country.

The study however countered the limitation by considering the views of the top management personnel from these banks who acted as representatives of the entire banks' position across the country since the introduction of the capping regulation. There were also limitations in getting the respondents because of their busy schedule and due to huge number of clients. Others considered the information sought very sensitive thus they may have responded generally without giving very specific details. To counter this challenge the researcher had to make prior arrangements as well as giving ample time for the respondents to respond to the research instrument. This included extending the data collection period with some days as well as making networks with the target respondents to enhance response rate.

5.7 Recommendations for Further Study

From the analysis and finding from the previous studies, Majority of the banks in Kenya has policies relating to cybercrime but they fully implement them. As a result, there is a dire need to create high level of compliance strictly following institutions' policies and laid down procedures. These policies and processes can only be operational and more effective if they are applied on day to day activities. Another aspect is on the frequency of patching and updating firewalls. From the study, there emerge a gap on how often organization update their firewalls. There is however a greater call to all commercial banks in Kenya to improve how frequent they need to patch and firewall updates their software failures to which will leaves the organizations vulnerable to any attack no matter its magnitude.

To ensure smooth business continuity for any organization in business, there are several steps that the organization clearly needs to undertake after an attack or attempted attacks. This is on disaster recovery mechanisms. This is defined as the section in the business that outlines steps taken towards recovery whenever there is a hitch in the business operation due to either systems failure or cybercrime attacks. It is therefore critical to undertake a study to assess the level of preparation of commercial banks to pull through from a disaster that may be caused cybercrime. The study should entails measures are being taken to ensure seamless flow of operations within the commercials banks. A propose that a study on the impact of socializing staffs about cybercrime awareness new staffs as they are assuming their new role in the bank would change the culture within the banking sector. It would be of great importance to come up with various new ways in which this could be done.

REFERENCES

Acharya, R.N., &Kagan, A. (2004).Commercial B2B Web Site Attributes within the Perishable Sector.*Journal of Internet Commerce, 3(4)* 79-91.

Amaroso, E. (2011).2 Cyber Attacks: Protecting National Infrastructure. Burlington: Elsevier.

Amboko, L.F., &Wagoki, J. (2012).Determinants of Adoption and Usage of Banking Innovations by Consumers for Competitive Advantage: A Case of Banks in Nakuru County. *International Journal of Science and Research (IJSR) 3(10) 1597-1601.*

Atanassov, J., Nanda, V., &Seru, A. (2007). Finance and innovation: The case of publicly traded firms. Working Paper. University of Oregon, Arizona State, and Chicago.

Babbie, E. R. (2004). The Basics of Social Research. Wadsworth.

Belicove, M. E. (2012, 10 26). The 10 Dos and Don'ts of Conducting Employee Background Checks. Retrieved from Forbes: http://www.forbes.com/sites/mikalbelicove/2012/10/26/the-10-dos-and-donts-o-conducting-employee-background-checks/

Bulgurcu, B., Cavusoglu, H., &Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness,*MIS Quarterly*34(3), 523-548.

Bhasin, D. M. (2007).Mitigating Cyber threats to Banking Industry. The Chartered Accountant, 1618-1624.

Cadregari, C. (2011). Every Silver Cloud Has a Dark Lining : A Primer on Cloud Computing, Regulatory and Data Security Risk. ISACA JOURNAL Volume 3,1-5.Retrieved from ISACA.org: Dark-Lining.aspx http://www.isaca.org/Journal/archives/2011/Volume-3/Pages/Every-Silver-Cloud-Has-a-

Central Bank of Kenya. (2008; 2013) *Bank Supervision Report*. Nairobi: Central Bank of Kenya.

Cooper, D. R., Schindler, P. S., & Sun, J. (2003). Business Research Methods.

French Aron (2009). Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement (CRS Report R42547. Washington, DC: Congressional Research Service, July 20, 2012. United State

Hatfield, D.E., Tegarden, L.F., Echols, A.E. (2001), "Facing the uncertain environment from technological discontinuities – Hedging as a technology strategy" Journal of High Technology Management Research, Vol. 12, pp. 63-76.

Heidi, W. M. (2015). Countering Social Engineering through Social Media: An Enterprise Security Perspective. Australia: Charles Sturt University.

India, G. o. (2000). Gazette of India Extraordinary. Retrieved 11 15, 2013, from Government of India: http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf

International Telecommunication Union (2004). Understanding Cybercrime: A Guide for Developing Country.

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

Jain, B. &Kini, O. (1994).The post-issue operating performance of IPO firms. The Journal of Finance, 49. No. 5, pp. 1699-726.

Jaffar, M., &Manarvi, I.(2011). Performance comparison of Islamic and conventional banks in Pakistan. Global Journal of Management and Business Research,11(1), 66

Kamel, S. (2005).The Use of Information Technology to Transform the Banking Sector in Developing Nations**.** *Information Technology for Development* 11 (4) 305–312.

Kariuki, J. G. (2014).Factors Influencing the Adoption of Internet Banking In Kenya. Journal of Business and Management 16(9) 60-65.

Kitchenham, B., & Lawrence, S. (2002). Principles of Survey Research: Part 5 Populations and Samples. ACM Sigsoft, 17-20.

Kitheka, P. M. (2013). Information Security Management Systems in Public Universities in Kenya: A Gap Analysis Between Common Practices and Industry Best Practices. Nairobi: University of Nairobi.

Kothari, C.R. (2004), Research Methodology: Methods an d Techniques New Delhi: Kings Mill.

Leder. (2009). Proactive Botnet Countermeasures An Offensive Approach. Bonn: Institute of Computer Science IV, University of Bonn, Germany.

Leder, F, & Martini, W. (2009). Proactive Botnet Countermeasures An Offensive Approach. Bonn: Institute of Computer Science IV, University of Bonn, Germany.

Legris, P., Ingham, J., &Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. *Information & Management*, 40, 191–204.

Lewis, P., Saunders, M and Thornhill, A. (2014)."Developing an Explanatory theory of Reward System Change." Personnel Review, Vol. 33, pp 91-8.

Loonam, M., & O’Loughlin, D. (2008). An observation analysis of e-service quality in online banking. *Journal of Financial Services Marketing, 13(2)*, 164-178.

Malhotra, N. K. (1996). Marketing Research: AN Applied Orientation. Second Edition. New Jersy: Prentice Hall.

Mehta.(2011). Electronic Crime in a Globalized Society. Its impact on the sound development of the State - An Indian perspective. International Journal for business information Technology, 159-164.

Mugenda, O. M. &Mugenda, A. G. (2003).*Research Methods*: Quantitative and qualitative Approaches University Press

Ngalyuka, C. (2013). The Relationship Between ICT Utilization and Fraud Losses in Commercial Banks in Kenya. Nairobi: University Of Nairobi.

Njiru, S. W. (2013). A Framework to Guide Information Security Initiatives For Banking Information Systems, Kenyan Banking Sector Case Study. Nairobi.

Olayemi, O. J. (2014). A socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria, *International Journal of Sociology and Anthropology*, 6(3), 116-125.

Okiro, K., &Ndungu, J.(2013).The Impact of Mobile and Internet Banking on Performance of Financial Institutions in Kenya. *Journal of Business and Management 16(9) 146-161.*

Okoth, J. (2009), *" Fraudsters take home billion s from banks"* .Nairobi: East Africa Standard 17th November.

Rashid, F. Y. (2011, 12 13). Google Removes Malicious cloned games from the android Market.E-Week.

RavalVasant, C. D. (2010). Risk Landscape of Cloud Computing. ISACA JOURNAL Vol 1, 1-5.

Rogers, E.M. (2005). Diffusion of Innovations, New York: The Free Press.

Rogers, E.M. (2003). Diffusion of Innovations, New York: The Free Press.

Sabi, H.M (2014) Research Trends in the Diffusion of Internet Banking in Developing Countries, *Journal of Internet Banking and Commerce*, August 2014, 19, no.2

Siddique, M.I. and Rehman, S. (2011), Impact of Electronic Crime in Indian Banking Sector – An Overview. International Journal of Business & Information Technology, Vol. 1 No. 2.

Salifu, A. (2008), *The Impact o f Intern et C rim e on Development.* Journal of Financial Crime, 15 (4) Pp. 432-443.

Sathye M. (1999). Adoption of Internet banking by Australian Consumers: an empirical investigation. International Journal of Bank Marketing, 17(7), 324-334.

Schulz, G. (3, 8 2006). Top 10 Ways to Secure your Data. Retrieved 11 15, 2013, from ComputerWorld:http://www.computerworld.com/s/article/9002188/Top_10_ways _to_secure_ your_stored_data?taxonomyId=19&pageNumber=2

Steven, A. (2002). Information System: The information of E-Business, New Jersey, Natalie Anderson.

Tarimo, C. (2006): ICT Security Readiness Checklist for Developing countries: A Social-Technical Approach. PhD thesis. Stockholm University, Royal Institute of Technology.

Tendulkar, R. (2013, 7 16). Cyber- Crime, Securities Markets and Systematic risk. Retrieved:http://www.csrc.gov.cn/pub/csrc_en/affairs/AffairsIOSCO/201307/W0 20130 719521960468495.pdf

Vatis, M. (2009).Trends in Cyber Vulnerabilities, Threats, and Countermeasures.

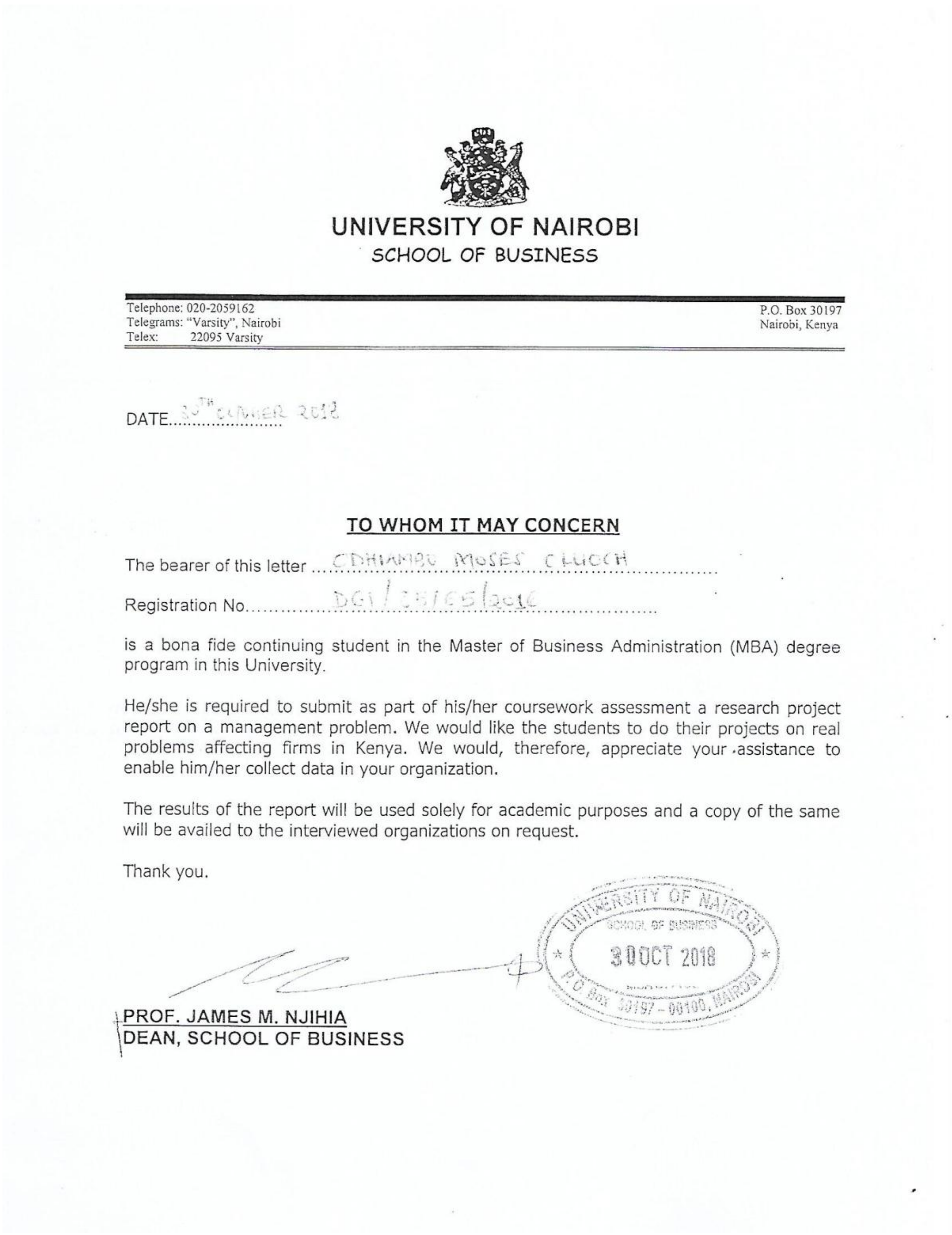
Wei, X. K. (2012). Security Implementation for a VoIP Server.

Wang, S. (2007). Measures of retaining digital evidence to prosecute computer based crimes. Computer standards and Interfaces, 216-223.

Youga, l. J., & Singh, A. (2013). A study of the Cybercrime and Security Scenario in India. International Journal of Engineering and Management Research, 13-18.

APPENDICES

Appendix A: Introduction letter



UNIVERSITY OF NAIROBI
SCHOOL OF BUSINESS

Telephone: 020-2059162
Telegrams: "Varsity", Nairobi
Telex: 22095 Varsity

P.O. Box 30197
Nairobi, Kenya

DATE 30TH OCTOBER 2018

TO WHOM IT MAY CONCERN

The bearer of this letter ODHIAMBO MOSES OLUOCH

Registration No. D61/25165/2016

is a bona fide continuing student in the Master of Business Administration (MBA) degree program in this University.

He/she is required to submit as part of his/her coursework assessment a research project report on a management problem. We would like the students to do their projects on real problems affecting firms in Kenya. We would, therefore, appreciate your assistance to enable him/her collect data in your organization.

The results of the report will be used solely for academic purposes and a copy of the same will be availed to the interviewed organizations on request.

Thank you.

UNIVERSITY OF NAIROBI
SCHOOL OF BUSINESS
30 OCT 2018
P.O. Box 30197 – 00100, NAIROBI

PROF. JAMES M. NJIHIA
DEAN, SCHOOL OF BUSINESS

Appendix B: Questionnaire

This questionnaire is designed to assist in collecting data to determine cyber threats, countermeasures and effectiveness of countermeasures in ISO certified organizations in Kenya. Kindly note that the findings of this research are solely for academic purposes and all the responses will be treated with utmost confidentiality

SECTION A:

(i) Demographic

Information Tick as

appropriate

1. Gender Male □ Female □
2. Age bracket 25 years or less…….. □
   26– 30 years………... □
   31 - 35 years………. □
   36 - 40 years………. □
   41 - 45 years………. □
   46 - 50 years………. □
   Over 50 years............ □
3. Education Level : Postgraduate □ Graduate □ Diploma □
   Other Specify____________________
4. Job Title : _______________________________

5. Years of work experience: 5 years or less □ 6 -10 years □
   Above 10 years □

(ii) Organization Information

1.0 In which industry does your organization operate? Tick as

Financial services…………………………. □

Asset

Based…………………………………

□

Other

Specify__________________________

2.0 Number of employees in your organization (Tick as appropriate)

100 or less...……………………………………………….... □

101 to

999……………..……………………………….…. □

Above

1000…………………………………………….... □

3.0 Asset base

3.1 Less than KES 5 billion……………………………….□

3.2 Above KES 5 Billion but less than KES 10 Billion……..□

3.3 Above KES 10 Billion…………………………………...□

4.0 How long has the organization been operating in Kenya? _________years

5.0 Is the organization locally owned or foreign multi-national subsidiary?

Locally owned…………………………………………….□

Foreign ……………………………………………….... □

Both……………………………………………………….□

SECTION B: Cyber Threats

To what extent has your organization experienced each of the following situations? Tick to indicate using the scale given.

		No Extent	Little Extent	Moderate Extent	Large Extent	Very large Extent
1.	Employees unintentionally or carelessly making mistakes that compromise cyber security					
2.	Employees being tricked by parties external to the organization to give out their security information for example passwords					
3.	Privileged users for example, IT administrators, attacking the organization’s information system for any reason					
4.	Fake offers on the internet					

	to share user security credentials					
5.	Fake plug-ins posing as legitimate extensions that trick users to download and install them leading to infection and stealing of information from the infected machine(s)					
6.	Fake applications, that appear to be integrated for use with a social network tricking users to install them resulting in the stealing of user access credentials					
7.	External parties hacking into your PBX and making calls through it					
8.	An attack that resulted in websites and servers unavailable to legitimate users					
9.	Computers in your organization spamming and or spreading viruses					
10.	Computers in the organization used by third parties to conduct online fraud activities					

11.	Attempts to access your online or mobile banking platform by non authorized users					
12.	Attempts to access mobile money points of service by unauthorized users					
13.	Lost money fraudulently through mobile money service					
14.	Attempts to access secret or confidential information stored in the organization’s computers or ICT network by unauthorized users					
15.	Breach of access to secret or confidential information stored either in the organization’s computers or ICT network					
16.	Confidential information stored in the organization’s computers or ICT network been stolen at any one time					
17.	Other: specify and rate					

SECTION C: Cyber threat Countermeasures

To what extent has your organization implemented each of the following cyber security countermeasures? Tick as appropriate using the scale given

	Countermeasure	No Extent	Little Extent	Moderate Extent	Large Extent	Very large Extent
1.	Cyber security policy					
2.	User awareness training on cyber security issues					
3.	Two factor user authentications					
4.	Maintain staff values and attitudes that align with organizational mission and ethics					
5.	Segregate your voice and data traffic					
6.	Disabling of non-service related or unused open PBX ports					
7.	Call Detail Record (CDR) Monitoring to identify unusual usage patterns					
8.	Policy on how to deal with online social engineering or phishing attempts					
9.	Continuous monitoring of inbound network traffic load on firewalls and system resources (CPUs)					
10.	Segmentation of internal and external networks for critical systems					
11.	Carry out cyber risk assessment on its critical assets					
14.	Legislation					
15.	Carry out cyber security or information security audits					
16.	Constantly scanning and patching for					

17.	software vulnerabilities					
18.	Other : specify and rate					

SECTION D: Effectiveness of cyber threat countermeasures implemented by organization

To what extent has the cyber threat countermeasures applied in the organization been effective in achieving each of the following risk mitigation objectives?

		No Extent	Little Extent	Moderate Extent	Large Extent	Very large Extent
1.	Increased number of successfully blocked cyber attacks					
2.	More uptime of the organization’s ICT system to users					
3.	Maintenance of confidentiality of privileged information stored in the organization’s computers or ICT Network					
4.	Maintenance of integrity of information stored in the organization’s computers or ICT Network					
5.	Maintenance of availability of information stored in the organization’s computers or ICT Network					
6.	Other: Specify and rate					

Thank you for completing the questionnaire

Appendix C: Commercial Banks Registered in Kenya as at 30th January 2018

1. African Banking Corporation Limited

2. Bank of Africa Kenya Ltd

3. Bank of Baroda (K) Ltd.

4. Bank of India

5. Barclays Bank of Kenya Ltd

6. Sidian Bank

7. Charterhouse Bank Ltd

8. Chase Bank Ltd

9. Citibank N.A. Kenya

10. Co-operative Bank of Kenya Ltd

11. Commercial Bank of Africa Ltd

12. Consolidated Bank of Kenya

13. Credit Bank Ltd

14. Development Bank of Kenya

15. Diamond Trust Bank Ltd

16. DIB Bank

17. Ecobank Kenya Ltd

18. Equity Bank Ltd

19. Family Bank Ltd

20. Fidelity Commercial Bank Ltd

21. Fina Bank Ltd

22. First Community Bank Ltd

23. Giro Commercial Bank Ltd

24. Guardian Bank Ltd

25. Gulf African Bank Ltd

26. Habib Bank A.G. Zuric

27. Habib Bank Ltd

28. Imperial Bank Ltd

29. Investment & Mortgages Bank Ltd

30. Jamii Bora Bank Ltd

31. Spire Bank Ltd

32. Kenya Commercial Bank Limited

33. Middle East Bank (K) Ltd

34. National Bank of Kenya Ltd

35. NIC Bank Ltd

36. Oriental Commercial Bank Ltd

37. Paramount Universal Bank Ltd

38. Prime Bank Ltd

39. Standard Chartered Bank Kenya Ltd

40. Trans-National Bank Ltd

41. UBA Kenya Bank Limited

42. Victoria Commercial Bank Ltd

Source: Central Bank Website of Kenya Licensed Commercial Retrieved from Bankshttps://www.centralbank.go.ke/wp-content/uploads/2017/05/Directory-of-Licenced-Commercial-Banks-Mortgage-Finance-Institutions-and-NOHCs.pdf (2018)