MEETING THE CHALLENGE OF CYBER THREATS IN EMERGING ELECTRONIC TRANSACTION TECHNOLOGIES IN IN KENYAN BANKING SECTOR

BY

JAMES ONYANGO NYAWANGA

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

OCTOBER, 2015

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.

James Onyango Nyawanga (D61/72752/2012)

Signed: ________________________ Date: __________________________

This Research is the candidate's original work and has been prepared with my guidance and assistance; it is submitted with my approval.

DR. NJIHIA JAMES MURANGA

Supervisor

Signed: ________________________ Date: __________________________

Senior Lecturer, Department of Management Science

School of Business

University of Nairobi

ACKNOWLEDGMENTS

My heartfelt sincere gratitude is to the almighty God for giving me good health and a sound mind to handle this project to its conclusion.

I am also very grateful to my supervisor Dr. Njihia James Muraga for dedicating his valuable time and energy to ensure that I remained focused to finish the project. This project would not have been possible without his constant commitment and guidance to ensure that we achieve the best out of it.

I also would like to thank my wonderful parents Mr. And Mrs. Tobias Nyawanga for their invaluable support, prayers and love. They provided consistent encouragement without which I would not complete this project

Last but not least I thank my friends, fellow MBA students, workmates, other lecturers and everybody else who in one way or another contributed ideas towards the improvement of this project. Their outstanding advise has seen me reach this far. Thank you all.

DEDICATION

I dedicate this work to my parents, Mr. And Mrs. Nyawanga

ABSTRACT

The purpose of the study was to investigate how to meet the challenges pf cyber threats in the emerging electronic transaction systems in the Kenyan banking sector. The study addressed the following objectives: To establish ICT security threats facing electronic transactions in the cyber space, to establish factors that influence Cyber security threats on Electronic transaction and finally to establish a cyber-security model for adoption of ICT security on Electronic transaction by the banking sector in Kenya. The research design used was descriptive. The results showed data was collected from 41 ICT experts. To select the respondents for this study, random sampling technique was used. Primary data was first edited, coded and then analyzed using Microsoft Excel and SPSS computer packages. The interpreted data was grouped into common themes and was presented in the form of pie-charts, percentages, figures, tables and bar graphs. The study found out that the cyber-crime rate has increased in the past 12 months with most 80% of attacks originating from China and Kenya itself. The study also found out that cyber-crime is mostly perpetrated by one of the bank staff knowingly or unknowing. Thus the need for cyber training for most if not all the banking staff. The study also finds that weak systems and ICT security structures and policies are another causes of penetration and cyber-attacks.

TABLE OF CONTENTS

CHAPTER ONE: INTRODUCTION

1.1 Background

Information and Communications Technologies (ICTs) are vital tools in any information and knowledge based societies. Today's information society is driven by new technologies, new procedures and new expertise, the use of which is improving the welfare of citizens, changing our way of interaction and social participation, and promoting equality and democracy. These new technologies improve the productivity and competitiveness of companies and open up new markets while creating new business opportunities.

When reviewing information and research regarding electronic transaction security the phrase "information security" is often mentioned. While the phrases are distinct they do harbor similarities and are correlated. By definition, information security is "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" (White 2014). Information security comprises an enormous range of importance processes that many casual users tend to overlook or, often to their detriment, choose to ignore. In a digitally connected world where technology abounds in all forms, ignoring the importance of information security is akin to willingly putting one's personal and financial information at risk. Risk, in this sense, refers to a breach in security that may result in financial ruin, personal and/or professional embarrassment, theft of trade secrets and other serious consequences (Pete, 2001).

However, these new technologies continue to be exploited by malevolent users and the phenomenon is becoming intrinsically linked to organized crime on the Internet and internal malpractices that take advantage of weaknesses within information systems. Vulnerabilities in software applications are purposely sought after in order to create malware that will enable unauthorized access and modification, thus compromising integrity, availability and confidentiality of the ICT networks and systems. Other threats to information security include breaches of personal privacy, e-mail spam, industrial espionage, piracy computer viruses, cyber terrorism and electronic warfare. Any of these can spread worldwide in an instant through information networks. With the increasing sophistication of malware, these threats cannot be overestimated and they could have awful consequences on the critical information infrastructure of any country. It is prudent therefore, that due diligence and due care are implemented to ensure proper national information security management (Sans, 2002).

Organizations are becoming increasing reliant on Information technology to perform most of the basic functions and the complex and manual functions are becoming automated. This reliance leads to dependence on information technology which in turn leads to increase in the value of ICT. The Kenyan cyberspace has seen key emerging technologies over the coming years the growth of the cyberspace has been characterized by several innovative technologies especially in the financial sector domain and specifically in the money transfer, electronic transaction, mobile money transfer, internet and web transaction. The Kenyan financial Market has grown tremendously with the transaction shift from the traditional face to face transaction to the e-commerce transaction. There are over million e-transaction in a single day with this increased transaction the Kenyan market becomes a target for cybercrimes and fraud.

Information security is the protection information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. It is in this regard that the Ministry of Information and Communications Technology whose mandate is to provide strategic and technical leadership, overall coordination, support and advocacy on all matters of policy, laws, regulations and strategy in all matters of ICT in consultation with various stakeholders has developed a National Information Security Strategy to address the information security issues at national level. Information technology security is often the challenge of balancing the demands of users versus the need for data confidentiality and integrity. For example, allowing employees to access a network from a remote location, like their home or a project site, can increase the value of the network and efficiency of the employee. Unfortunately, remote access to a network also opens a number of vulnerabilities and creates difficult security challenges for a network administrator.

Thus with the above discussion on information technology security the study intends to establish the ICT security Threats that are being faced by the electronic transactions in the cyber space, also to form factors that facilitate ICT security threats on Electronic transaction and ICT security policies that have been employed by different institutions finally the study will establish a cyber-security model for adoption of ICT security on Electronic transaction by the banking sector in Kenya where a more theoretical approach will be taken into consideration during the process of the study

1.1.1 Electronic Transaction Technologies

Electronic transaction can use several technologies several types of electronic transactions Technologies with the most commonly recognized being credit cards, direct deposit, direct payments, and funds transfer. Although most people are familiar with the use of credit card there are emerging technologies which have proven to be convenient to consumer. Mobile banking involves the use of mobile technologies to help you check your account balance, transfer funds to a different account and deposit and withdraw funds from your account to mobile.

HFC bank in India is an example of a bank which has applied mobile banking. Internet or online banking is another Transaction technology French (2013) defines it online banking as an electronic payment system that enables customers of a financial institution to conduct financial transactions on a website operated by the institution. Other transaction technologies include such method that the credit card processing software (or app) with an optional card reader from companies like Square.com and PayPal, Both programs operate similarly in that the user can sell goods or services and process payments using only a smart phone by simply installing the pay application. Electronic transactions technologies face many types of threats including threats that first come in the form of possible risks where risk becomes a threat.

1.1.2 Cyber Threats

Cyber-attack is any type of aggressive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system. These can be labeled as either a Cyber campaign, cyber warfare or cyber terrorism in different context. Cyber-attacks can range from installing spyware on a PC to attempts to destroy the infrastructure of entire nations. Cyber-attacks have become increasingly sophisticated and dangerous as the stuxnet worm recently demonstrated (Karnouskos, 2011)

Forms of cyber security threats are; Insider Threats, VoIP PBX Fraud, Mobile Money Fraud, Cyber Espionage, Denial of Service attacks, Cyber Crimes, Data Protection, Spam, Cyber Attacks. Every business connected to the internet can expect to fall victim to cyber-crime at some point as criminals expand their ability to steal money directly or to turn stolen data into money. The losses which cost 445 billion dollars yearly are both direct and indirect, with many businesses citing downtime or lost productivity as a costly side-effect of some cyber-criminal activity.

1.1.3 Banking Sector in Kenya

Kenyan Banks have realized tremendous grow in the last five years and have expanded to the east African region. The banking industry in Kenya has also involved itself in automation, moving from the traditional banking to better meet the growing complex needs of their customer and globalization challenges. These increase in competition have spill over from local banks to the international banks, some of which are new players in the country. This has served the Kenyan economy well as the customers and shareholder are the ones who have benefited the most. Kenyan banks are growing at three times the rate of economic growth. This is the highest multiple in the region, and could be at least partly due to the influential role that mobile payment platforms have played, incorporating growing number of adults into the banking network. The banking industry in Kenya is regulated by the Central Bank of Kenya act, Banking Act the Companies Act among other guidelines issued by the Central Bank of Kenya (CBK). The industry has over the past few year enjoyed exponential growth in deposits, assets, profitability and products offering mainly attributed to automation of services and branch network expansion both locally and regionally.

The growth has brought about increasing competition among players and new entrants into the banking sector. Thanks to the stiff competition, banks are now focusing on the diverse customer needs rather than traditional banking products such as over the counter deposits and withdrawal. CBK requires financial institutions to build up their minimum core capital requirement to Kenya shillings 1 Billion by December 2012. The Global crisis is one of the issue being experienced affected banking industry in Kenya and more so the mobilization of deposits and trade reduction. Interest margins declines have also affected the banking industry in Kenya and finally with the new digital age threats, cyber threats are becoming a major issue to the banking industry. One of the biggest areas of concern remains online and mobile banking. A decade ago, these platforms were used by a limited number of early adopters, but have since evolved into a mainstream service in Kenya. (Kangondu, 2015).

1.2 Statement of the Problem

Cyber-attacks against financial services institutions are becoming more frequent, more sophisticated, and more widespread. Although large-scale denial-of-services attacks against major financial institutions generate the most headlines, community and regional banks, credit unions, money transmitters, and third-party service providers (such as credit card and payment processors) have experienced attempted breaches in recent years.

The rise in frequency and breadth of cyber-attacks can be attributed to a number of factors. Unfriendly nation-states breach systems to seek intelligence or intellectual property. Hackers aim to make political statements through systems disruptions. Organized crime groups, cyber gangs, and other criminals breach systems for monetary gain—i.e., to steal funds via account takeovers, ATM thefts, and other mechanisms. As the cost of technology decreases, the barriers to entry for cybercrime drop, making it easier and cheaper for criminals of all types to seek out new ways to perpetrate cyber fraud. A growing black market for breached data serves to encourage wrongdoers further (Margaret, 2008).

According to a research done by Reddy (2014) and Gander (2014) on cyber security challenges and its emerging trends on latest technologies they clearly state that Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. They also propose that there is no perfect solution for cyber-crimes but we should try our level best to minimize and manage them in order to have a safe and secure future in cyber space. Even though this is true but there is need to create a model a benchmark strategy that can be used as a minimum requirement for Cyber security solution.

Another research by Tagert (2010) on cyber security challenges in developing nations found that a common approach and proposed frameworks for developing nations have shortcomings and it further develops and informs how developing nations could better approach their cyber security problems. It finds that developing nations have been trying to imitate what is being done in the developed world, which the research concludes is not a good approach. The researcher reiterates that better approach starts by identifying the different challenges between the developing nations and the developed nations and how this differences impacts the national strategic approach. The researcher studied the cyber security situation by analyzing the cyber threat, cyber defense approaches and strategies in both developed and developing nations of which he concludes while the physical hardware and software may be the same, the circumstances in a developing nation are different, which necessitates a customized solution and strategy.

Another research paper on Internet Banking and Commerce E-Banking and Cyber Security by French (2012) the paper bring a new factor that organizations, online banking in particular, are spending the majority of their efforts on external security without properly assessing the importance of internal security. With internal security being of a higher risk than external security, these additional security measures give users a false sense of security. The study tries to addresses the need for increased awareness of internal threats through security measures such as security awareness, policies, practices, and procedures. Online banks and other organizations should evaluate every aspect of security bearing in mind the user security as the final objective. According to the researcher, while security is important, organizations should balance the need for increased security with the desire to make systems easy to use and useful to the consumer and not prohibit them from accessing their information. Although the researcher has indeed raised pertinent issues in regards to online security but banking institution have been taking into consideration internal threats with a lot of keenness and are spending a lot of their time and money analyzing internal threats. Further the study is only limited to internet banking which is quite a closed research as there are other emerging technologies which are intertwined with internet banking which are also affected with security threats.

Locally a research by Nyambura (2013) on her research work on Factors contributing to the occurrence of cybercrime on E-banking in commercial banks in Kenya, necessary policies have been formulated and documented and that commercial banks understand what cyber-crime is and the effect of the vice in the baking industry, and insists that commercial banks need to guard themselves against cyber-crime. Indeed the banks have taken necessary precautions and installed proper technology to guard against cyber intrusion at the internet level by installing firewalls and training of ICT staff but there is need to also install antivirus at the PC client level. The study further reveals that although there are spirited efforts by bankers Association to create awareness the commercial banks were aware that there has been an increase in the cases of cybercrime. However the reporting of the same to the authorities was at a minimum and for the cases which were reported, these are subjected to the same process as theft as the Kenyan legislation is yet to establish laws which deal with these cases as they should.

According to another research on Information Technology threats in Electronic Transfer in commercial banks in Kenya which focused on determining the extent of EFT threats, and establishing the EFT security measures undertaken to counter the threats and the challenges in enforcing the measures in commercial banks in Kenya. The researcher’s findings indicated that the main security threats in the country were Card skimming, Social engineering, Virus, Phishing and Worms. The main measures of countering the threats were firewalls, Use of easy and confidential system for staff to report any abnormal behavior, Consistent enforcing of policies and controls, Enforcement of separation of duties and least privilege, application of Role Based Access Control and use of data encryption are among others. The findings further showed the greatest challenges circulated on high cost of purchasing, licensing and maintenance of security solutions. The management was non-committal when budgeting for IT security department, providing limited budget fund for the department.

From the foregoing review of relevant literature, it is evident that research in the area of cyber security in Emerging technologies has been done but not in a comprehensive approach. All the literature reviewed indicates that previous researchers only concentrated on a few variables of Security and how they affect emerging technologies while this study covers additional important variables that were omitted by previous studies like electronic funds transfer systems, mobile banking, point of sale terminals and mobile transactions. From further survey of relevant literature, it has been found that there are few studies specific to Kenya on the issues of emerging technologies, cyber security and the factors increasing ICT security on the emerging technologies. This study therefore intends to fill these pertinent gaps in literature by studying the effects of Cyber threats on electronic transactions on cyberspace, factors facilitating these threats, and cyber- security models for adoption ICT security.

1.3 Research Objectives

The objectives of this study were:

i. To establish ICT security threats facing electronic transactions in the cyber space.

ii. To establish factors that influence Cyber security threats on Electronic transaction.

iii. To establish a cyber-security model for adoption of ICT security on Electronic transaction by the banking sector in Kenya.

1.4 Value of the Study

The findings of the study are important to the following groups:

Government national cyber policy makers will find the study useful in identifying the shortcomings of the implementation procedures they used and to recommend improvements where necessary. Thus the need to revisit the national Cyber policies and to include all stakeholders.

Top management of the banking industries to understand the importance of allocation of budget and resource to the ICT department specifically security department to be able to invest on latest technologies to combat cyber-crimes. Top management have been known to prioritize ICT security as low as possible, through this sensitization we increase the involvement of management in ICT security matters.

The general public on the importance of personal cyber security practices to avoid issues and cases of cyber-crime. By educating and creating awareness to the general public and the users we reduce the cyber-crime rates. The best way to reduce cases of cyber fraud is to sensitize and educate the users on common best practices, how to detect cyber frauds and how to protect oneself from cyber fraudsters.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

Electronic transaction has become a very important technological advancement for changing business practices presently (David et al., 2008). Electronic transactions especially in banking sector has seen tremendous growth and has evolved from the traditional banking practices to the current electronic transactional banking (Gonzalez et al., 2008). The literature review is a critical evaluation of existing related literature review on the challenges of cyber threats in the emerging electronic transaction in the banking sector, which serves as the background of this study. It also highlights concepts of innovation verses cyber security especially in the electronic transaction and the risks associated with Electronic transaction in the banking sector as well as the objective of the study. A cyber-attack is an attack initiated from a computer against a website, computer system or individual computer (collectively, a computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it. A cyber-attack takes many forms, gaining unauthorized access, unwanted disruption or denial of service, installation of malicious code among others. (Practical Law Company, 2011)

2.2 ICT Security Threats and Electronic Transactions in Cyber Space

According to (Kissel, 1994) information technology security is "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity, and availability" the definition is arguably the most recently and commonly used within the financial sector.

Electronic transaction are ever evolving to cope with the customers demand for convenience in transaction of their business. With this dynamic evolution so does the threats grow in sophistication. According to the Kenya Cyber security strategy released in 2014 we are highly susceptible to attacks from all over the world as we mature to an information society (Kenya Internet governance Forum, 2015). For a business to remain profitable embracing of the new Transaction technologies should be deemed as one of the strategic priorities. In the wake of these technologies customers do not feel secure in transacting business through electronic and online payment systems this is mostly due to the perceived and indeed a possibility of security risk. (McNichol, 2001)

There are arguably several risks which eventually translate to threats that surround the electronic transaction systems, access to sensitive customer information such as account details, pin numbers etc. This is especially in VISA Card transaction especially internet payment systems insertion of malicious code to read the card details as the customer enters the details during the transaction is one of the common threats even though efforts have been made to ensure confidentiality and integrity is maintained by embedding secure chip ability on the cards, the PC used could be compromise leading to the question of totality in security. Operational risks are also viewed as part of the threats associated by electronic transactions; these include access control, firewalls, cryptographic techniques, public key

Encryption, and digital signatures. The deficiency of the systems are majorly part of threats associated. According to the Kenya Cyber security report (2014) there are several threats to the electronic transactions, Insider Threats is the quite common especially in the global banking sector. Singer and Friedman (2103) defines it as deliberate malicious activity by current employees where privileged users probed systems for unauthorized access, co-opted other user’s access privileges and attacked systems for several reasons including competitive advantage, disgruntlement and most common blackmail . The figure has risen in the past few years as the perpetrators are mostly young employees who are techno-savvy who are on the forefront of the vice. According to a security expert the internal fraud is difficult to spot because it tend to be complex than the external threats due to the fact that the culprits are quite conversant with system and are better placed to understand the systems weaknesses and exploit them. (Njoka, 2014)

Mobile Money transfer and mobile money payment is a system which has been embedded to our banking and transaction domain with every payments and transactions now can be done by access to just an application. In Kenya the likes Mpesa, Mkesho, Mobile banking, Airtel money, have since been used as payment platforms for different transactions. According to (collymore, 2014) the M-revolution has grown where 80% of the Kenyan population have subscribed to the mobile money transfer and this has become an essential part of the lives. Since the launch of mobile money in 2007 reports of fraud have emerged with fraudster emerging with new, innovative and sophisticated ways of finding loopholes in the new controls implemented by banks, merchants and consumers (Kenya Cyber security Report, 2014). These crimes are estimated to have affected 20 million users inclusive of banking institution and individual users. According a report done by McAfee (2014) it is estimated that the cost of cybercrime globally stands at $445 billion annually, cybercrime is also believed to have affected 800 million people during 2013. Further on financial losses resulting from cybercrimes could have caused the loss of jobs for 150,000 Europeans.

Cyber espionage is another threat that takes precedent within the Electronic transaction, according to PC encyclopedia cyber espionage is the unauthorized spying by computer. The term generally refers to the deployment of viruses that clandestinely observe or destroy data in the computer systems of government agencies and large financial enterprises. In the US the senate banking committee decided to call a hearing in regards to protecting the financial industry against Cyber threats this was after a series of massive cyber-attacks directed towards JP Morgan Chase and other several banks who revealed that 76 million household and 7 million business accounts had been compromised. The US government showed great concerns claiming that there could be foreign state sponsoring of the cyber espionage (Fortune, 2014). Recently there was a group of 77 Chinese cyber-espionage who were arrested in Kenya who had sophisticated communication equipment and they were targeting Kenya’s communication system as well as the banking data and ATM machines they were also suspected to be involved with manufacturing of ATM cards and internet fraud (SC Magazine UK, 2014).

In the wake of closing the digital divides so have we been exposed to high number of Denial of Service attacks and Distributed DoS. Distributed denial-of-service attack is an attempt to make a machine or network resource unavailable to its intended users, DDOS is a type of DOS attack where multiple compromised systems which are usually infected with a Trojan are used to target a single system causing a Denial of Service (DoS) attack. (Mirkovic, 2005). Banking institutions have not been left behind with the need to move from the traditional physical servers and data center which requires high maintenance cost to the cloud servers which are operational efficient, low maintenance cost and quite convenient. In the Security summit (2015) in Johannesburg, it was revealed that South Africa is the most targeted country when it comes to denial of service with an increase of more than 150% of DDOS attacks on the continent, with a typical attack averaging 9Gbps. The recent attacks being targeted to South Africa`s financial institutions with the main aim of destabilizing the financial economy.

2.3 ICT security threats in Electronic Transactions

As we embrace the emerging technologies of electronic transaction in the banking sector there are factors that increase susceptibility to security threats these factors are sometimes overlooked by banking institutions and government or some of these factors cannot be fully contained despite the ICT security controls and strategies put in place to overcome these ICT security flaws. According to James R Clapper, Director of National Intelligence cyber threat cannot be eliminated; rather, cyber risk must be managed. Moreover, the risk calculus some private banking sector entities employ does not adequately account for foreign cyber threats or the systemic interdependencies between different critical infrastructure sectors (Economic times, 2015)

Human factors are the major challenges that fuel the security issues ignorance as the key ingredient lack of knowledge on the proper security policies and controls put in place to protect customers is quite rampart especially on mobile money users. Fraudster use this as an advantage to fraudulently access private information and later accessing money from unsuspecting customers mostly posing as the mobile services providers customer care. As part of the survey done by Serianu Limited Information security consultants in 2013, 90% of customers and merchants have fraudulently lost money from their mobile transaction to individuals posing as Mobile service providers and all the customers were not aware of the number the service provider uses for contacting customers.

In June 2013 a law was in co-operated into the communications act by a committee that was tasked to spearhead efforts against cybercrime. Embedded laws included penalties for both individuals and organization committing cybercrimes (Kenya Cyber report, 2014).

Despite all this efforts the ever changing and dynamic cyber world poses more sophisticated and new wave of attacks thus the need to constantly review the laws to accommodate the dynamic nature of cyber-attacks which are rarely undertaken by the government. This has led to less stiffer penalties on quite a large scale attack, this has not discouraged the cybercrime world.

Information security strategies undertaken by the banking institutions and government as a whole has not been of much assistance either. We do acknowledge the efforts previously put in place by the government, the banking institutions and mobile services by creating ICT security policies to combat cybercrime but there is need to constantly review this policies. The creation of the cyber security department by the government in 2013 that falls under the directory of e-government services shows such level of government commitment to combating cybercrime the department is in charge of creating cyber policies among other things (Getao, 2013).

The challenges comes when implementing the cyber policies unfortunately the lack of commitment and the bureaucracy within the government ranks have hampered the policies implementation. In banking institution the balance between innovation and Information Security policies is the main challenge management in banks have been mostly drawn towards innovation, research and development when it came to financial allocation ICT security tend to be allocated quite less. Gartner (2015) poses that, an average of 5.6 per cent of the overall IT budget is allocated to information security which shows how “little of value” security is he further states that Knowing how much is being spent on IT security is an indicator of whether organizations are practicing due diligence in security and related programs. Therefore there is need for information security managers to include estimates of measurable security budgetary allocation for every ICT project undertaken within the banking institutions.

2.4 Cyber-security model and strategy for ICT security in Electronic transaction

Havard Business review (2007) critically defines strategy as a set of guiding principles that, when communicated and adopted in the organization, generates a desired pattern of decision making. Therefore cyber security strategy is an integrated and well calculated approach to cyber security custom made to specific business and risk profile. The adoption of a minimum baseline strategy for government, private institutions and specifically banking institutions should be encouraged by use of an all-encompassing cyber security model. Clarity in setting up objectives and priorities which should include definition of the scope be it private and public institutions. A roadmap should be envisioned by creating milestones to be achieved, implementation strategies, master plan development should be developed. A perfect example is the development of the Government of Kenya national cyber security strategy (2014) of which its purpose is to clearly define Kenya’s cybersecurity vision, goals, and objectives to secure the nation’s cyberspace, while continuing to promote the use of ICT to enable Kenya’s economic growth.

A cyber security risk assessment is quite important to identify the gaps in institution`s critical risk areas and to determine actions to fill in the identified gaps. It will also ensure that you invest time, funds and human resource in the correct areas and avoid wasting of resources. A risk assessment 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. 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.

Success of a cyber-security strategy depends on the stakeholder involvement and inclusion therefor it's important to identify the stakeholders who are mostly the government, public and private sector.

In order for stakeholders to understand better the cyber threat land scape evolution there is a need to have a powerful and trusted information sharing mechanism between different stakeholders. The private sector could share the threat matrix experienced and the mitigation technologies, mechanism and policies which they have employed to manage cyber-attacks. In turn the government can share their national outlook on the cyber-attacks and what as a government they are doing to combat the vice.

Formation of clear incident reporting structures provides an avenue for organization and institution to report issues and incident related to cyber security this allows creation for contingencies plans for recovery and allows to easily tailor security strategies to reduce or mitigate the impact of future cyber-attacks.

2.5 Theoretical Literature Review

A theory is a reasoned statement or group of statements, which are supported by evidence meant to explain some phenomena. A theory is a systematic explanation of the relationship among phenomena. Theories provide a generalized explanation to an occurrence (Ngumi, 2013).

2.5.1 Theory of Intersectionality

Crenshaw (1989) identifies the issue of 'single- axis' analysis that separates problems of social injustice into distinct challenges facing specific groups, for example based on race, gender, sexual orientation or socioeconomic status. Such analyses easily lead to conclusions that miss the bigger picture, creating divisive competition between issues and gaps that allow important problems and key issues to be overlooked. Cybersecurity and social justice are formally different fields but the core insight of intersectionality holds true for both: we must move beyond discussions over whether a core issue is about Problem X or Problem Y and instead focus on the relationships among Problem X and Problem Y and Problem Z and other related problems. For cybersecurity, intersectionality can help us better understand the ways in which cyber issues are not just technical but are simultaneously legal and governmental and cultural and economic and so on (TenCrunch, 2015).

2.5.2 Game Theory

Several researchers have designed security mechanisms using game theory—several directions have been explored such as using a stochastic game to model network security scenarios (Lye 2005), modeling DDoS attacks (Wu 2010), security of physical and MAC layers (Sagduyu 2009), intrusion detection systems (Alpcan 2006). 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 and this is quite an expansive an enormous space. The game theory comes in handy when model and analyze search large space which involve numerous what-if scenarios. Its able model the inherently selfish and competitive behaviors of the attacker and system administrator and analyze the possible strategies. In addition, game theory has the capability of examining hundreds of thousands of possible scenarios before taking the best action; hence, it can sophisticate the decision process of the network administrator to a large extent. (Shiva and Sankardas, 2010)

2.5.3 Theory of Securitization

The theory of securitization is a new theory for analysis that seeks to analyze security issues in a more openly manner than traditional security studies, and: "based on a clear idea of the nature of security, securitization studies aims to gain an increasingly precise understanding of who securitizes, on what issues (threats), for whom (referent objects), why, with what results and, not least, under what conditions" (Buzan et al ,1998). The theory of securitization defines a referent object as the state or an individual, but it can also be defined as a structural system like "the nature of states" (ibid, 1995) , the theory uses different levels to analyze why certain things happen and are not strictly defined.

Analysis of cyber security is dealt with on different levels in society from an international, regional and national outlook, as well as on how cyber security spreads across levels and creates an interrelation between the levels.

2.6 Empirical Reviews

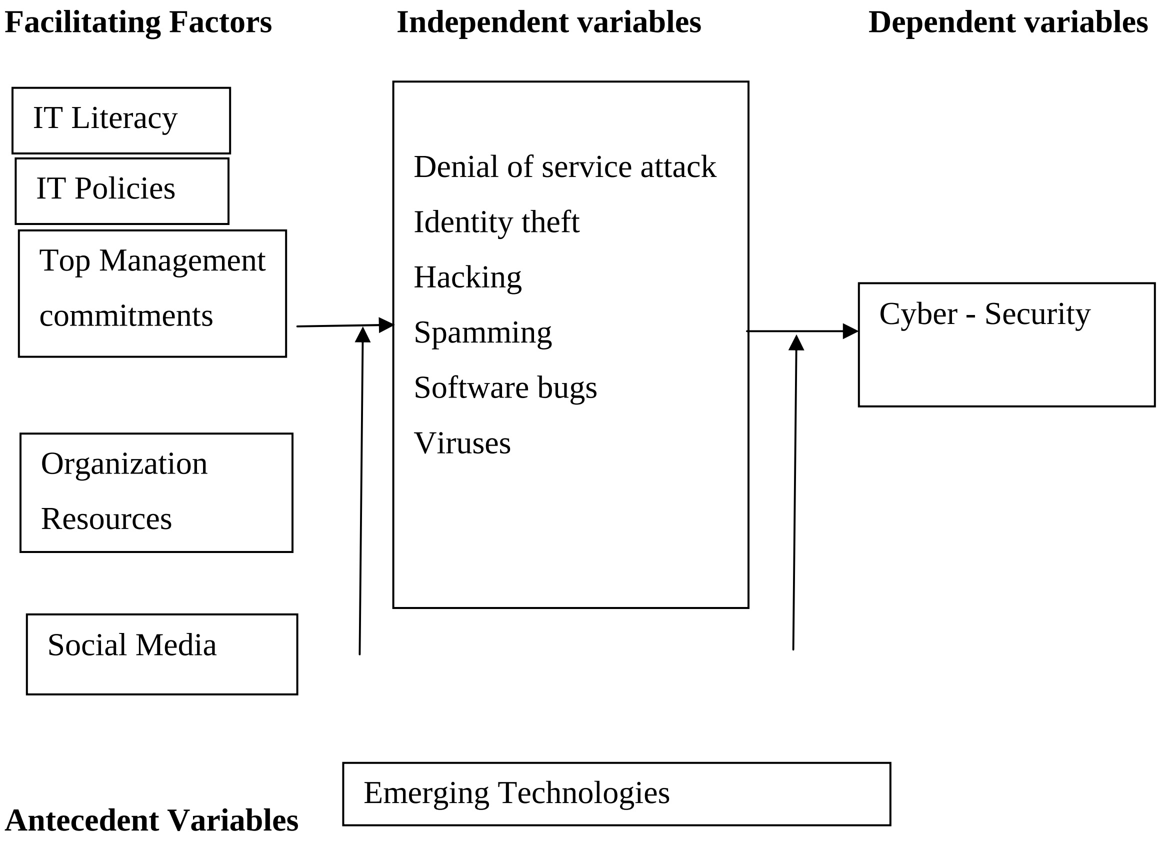
From reviewed relevant journals, thesis and literatures, it was quite clear from several writers like; french (2012), Nikhita and Gander (2012), Jassal and Sehgal (2013), Faheem (2013) that emerging technologies over the last 3 years have become more innovative they have all agreed that innovation especially in electronic transactions has been driven by the need for competition between banking institutions to meet customer demands for convenient and secure ways to transact business. They are in agreement that with increase in innovation in areas of electronic transaction technologies so does the increase in sophistication of the cyber threats targeted to these technologies. They insist that there is no a clear framework to completely eradicate cyber threats but to learn how to manage and to recover fast from any attack instigated. However other scholars like Nyambura (2015), Gichengo (2010), and Target (2010) did agree with the above review but 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.

The two groups of scholars did agree with the forms of ICT and Cyber threats being experienced in the financial sector. This study seeks to divert from the past and to incorporate several frameworks models that cut across different banking institutions and that could be easily be custom made to suite the institutions organizational, network and infrastructure and management structure. It also seeks to show how emerging technologies are prone to ICT and cyber security threats bearing in mind the banking industry has had tremendous ICT innovation growth in the last two years. From the previous Literature it's quite clear that there was some research done for the ICT threats in banking industry but there was limited focus in emerging technologies this study seeks to extensively cover the emerging technologies innovational growth experienced within the last two years. There is also the aspect of few research studies specific to Kenya on the areas of Cyber security specifically affecting the current emerging technologies, this was determined by survey of relevant literature.

2.7 Conceptual Framework

The conceptual framework in figure 2.1 shows the relationship between the independent variables and dependent variable distilled from the literature review.

Figure 2.1: Conceptual Framework



2.8 Summary

Cyber threats in the wake of emerging transaction that constitute internet banking, mobile banking , mobile transaction and cloud expansion is seen as the most deadly threat to the economy yet to be seen. Kenya is fast embracing technology and dynamically changing to Electronic transaction reliant country and without proper national cyber security strategy in place to identify the threats we are up against it will be a losing battle. According to (Kenya Cyber security Report, 2014) they is a sharp increase in the number of cyber-attacks to our public, private and mostly financial institutions leading to loss of approximately 2 billion with in the same year.

Therefore there is need to establish the threats facing the cyber space mainly targeting the Electronic transaction systems, factors which are facilitating these threats and to finally establish a model and a strategy that can be employed to mitigate further attacks and to look for more innovative ways protect our sensitive data.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter covers the methodology that will be used to collect and analyze the data in the study. The chapter also deals with the type of research design, the population, the sampling design, data collection methods and data analysis methods.

3.2 Research Design

This study adopted a descriptive research design. Descriptive research design is a type of consultative research that gives a description of something (Malhotra, 1996 descriptive research gathers quantifiable information that can be used for statistical inference on your target audience through data analysis (Penwarden, 2003). Khan, (1993) recommends descriptive survey design for its ability to produce statistical information about aspects of education that interest policy makers and researchers and its ability to describe the situation as it is.

Cooper & Schindler (2003) acknowledge this method as a design based on univariate questions or hypothesis that seeks to determine the state of the existing relationships between different variables, and characteristics of those variables by attempting to answer who, What, Where and how questions. Descriptive design is appropriate in providing the information on the challenges of cyber threats of emerging electronic transaction technologies in Kenyan banking sector.

3.3 Population of the Study

The population of the study is 44 Commercial banks based in Nairobi. A sample was drawn from this population.

3.4 Sampling Design and Sample Size

Sampling is a means of selecting some or part of a group to represent the entire group or the population of interest. Sampling reduces the length of time to complete a research. It cuts costs, is manageable, it increases accuracy and is almost a mirror of the sample population (Babbie, 2004). For this study, the Yamani Taro (1967) formula is proposed to be used. It states that the desired sample size is a function of the target population and the maximum acceptable margin of error (also known as the sampling error) and it expressed mathematically thus:

$$n = \frac{N}{1 + N * (e)^2}$$

n - The sample size, N - The population size, e - The acceptable sampling error * 95% confidence level and p = 0.5 are assumed.

$$n = \frac{44}{1+44(0.05)_2}$$

n= 39

The research used a 5% margin of error, therefore, 39 banks were targeted by the use of questionnaires.

3.5 Data Collection

The study used both primary and secondary data. Primary data was collected by use of a structured questionnaire and secondary data was drawn from review of organizations' profiles and journals, the internet, books, magazines, past research findings among others. Data was collected using a questionnaire developed by the researcher drawn from the three research questions. This questionnaire was self-administered and shared with respondents in two different ways. One by hand delivery while the second through emails. The interview targeted one Information security managers, at least two Information security officers, at least two project managers, at least two Network security engineers, at least two Information system business analyst.

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.

3.7 Data Analysis

The process of data analysis involved data clean up and explanation. The data was then coded and checked for any errors and omissions (Kothari, 2004). This process includes several stages. Data preparation entailed obtaining information and insights from the data which has been obtained. This was necessary as it has assisted in avoiding erroneous judgments and conclusions. In area of erroneous information editing was used to check and adjust data to ensure that inconsistency, illegibility and omission were properly handled and corrected. Frequency tables and percentages was used to present the findings. This data that was represented on frequency tables and as percentages was coded from and assigned on the representations. In case of clarity issues, the researcher contacted the respondents in cases where researcher needed to clarify some issues identified with the specific questionnaires. The data was analyzed using both descriptive for the objective one and three while on objective two inferential statistics such as regression analysis to identify the relationship between variables.

CHAPTER FOUR: DATA ANALYSIS ,RESULTS AND DISCUSSIONS

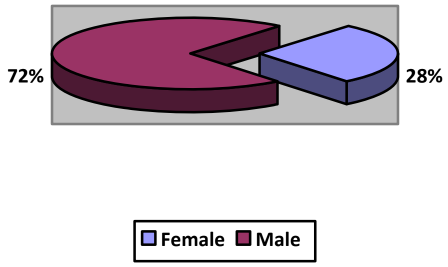
4.1 Introduction

This chapter outlines the outcome of the interviews conducted at the bank with the objective of answering the research questions that formed the basis of this research. Each research question will be analyzed with the intention of clearly presenting the findings of this research. Data was collected from 39 Kenyan banks based in Nairobi. This study was targeting a sample of 39 with 78 respondents attaining a 97% response rate of the total response rate. The interviewees are persons who have worked in various sections with in the bank including – the projects department, Alternate business channels such as mobile banking, internet banking, networking and IT security departments and finally data and core departments. The questionnaires were then coded individually and input into SPSS for analysis. Data was tabulated and presented in the form of frequencies and percentages, in charts and tables. The chapter is structured on the basis of background information, that is, general report of the respondents, the way they responded to each of the variables contained in the questionnaire regarding, factors contributing to occurrence of cybercrime in emerging e-transaction systems in Kenya banking sector.

4.1.1 Gender of Population

In figure 2 below shows that there was a total of 78 respondents. 72% of the total sample indicated that they were male while 28% indicated that they were females.

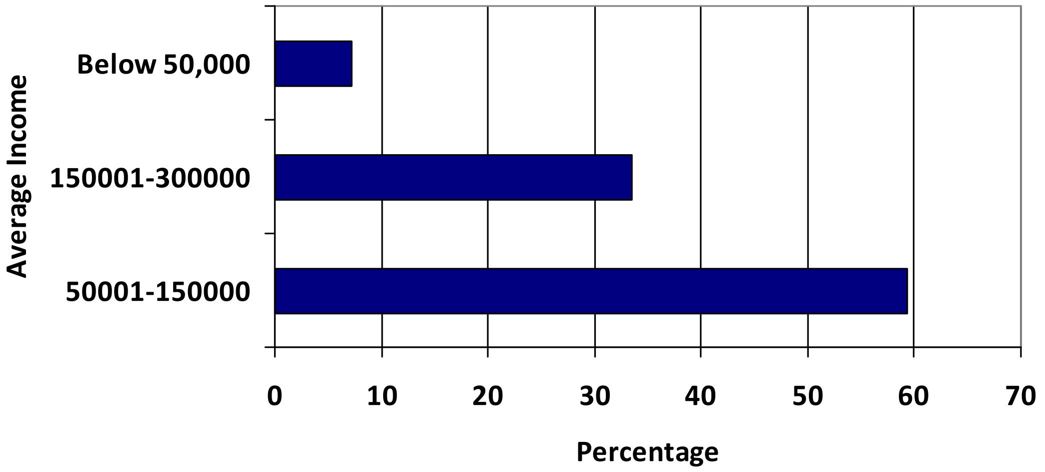
Figure2: Gender of the Population



4.1.2 Average Income per Month

This information was useful in asserting that the majority of the sampled respondents were employees of banks and their susceptibility to cybercrime in relation to their income 59.3% of those sampled said that they earn between 50001- 150000, 33.5% said that they earn between150001-300000 and 7.2% said that they earn below 50,000 per month.

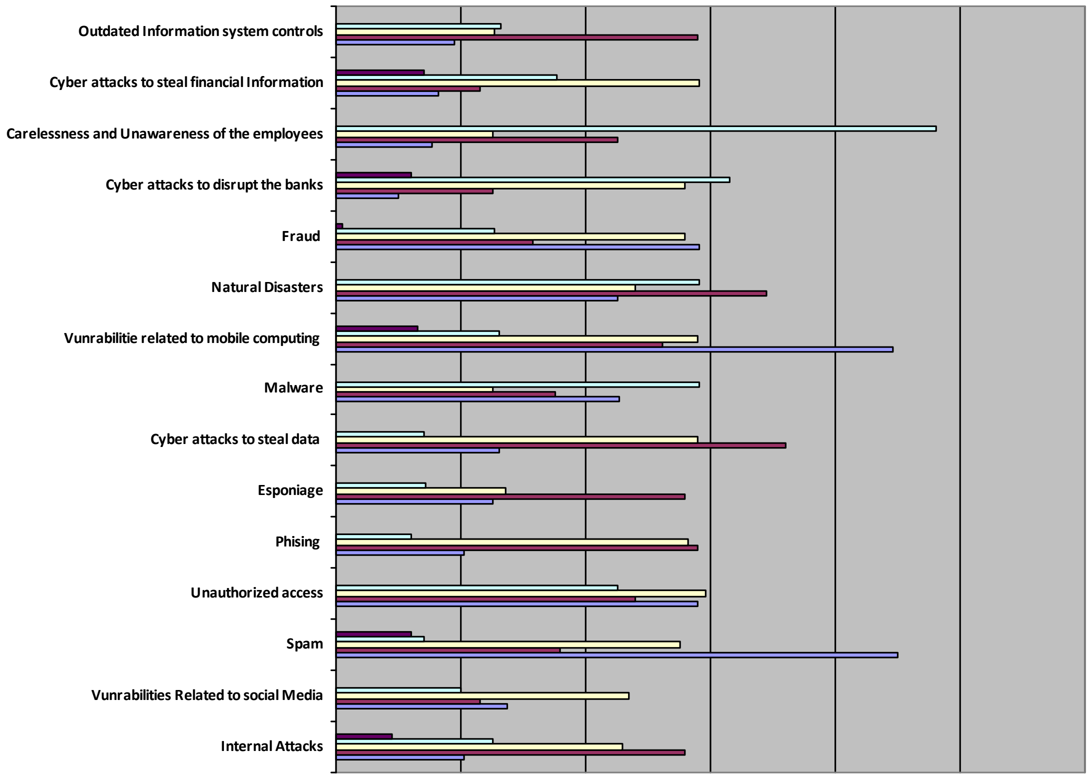
Figure 3: Average Income



4.1.3 Threats and vulnerabilities that have Increased Banks' Risk Exposure

Looking at security challenges that the banking sector faces today as shown in Figure 4, fraud (at 85%), careless or unaware employees (at 88%), internal attacks (at 73%), vulnerabilities relating to mobile computing (at 89%), cyber-attacks to steal financial information (at 89%) and outdated information security controls/architectures (at 90%) rated the highest among the respondents who are IT professionals dealing with security matters in the banking sector. Threats such as spam (at 29%), phishing (at 30%), espionage (at 31%) and natural disasters (at 28%) did not rate highly. This is an indication that IT professionals are now more worried on the silent threats rather than the noisy threats.

Figure 4: Security Challenges

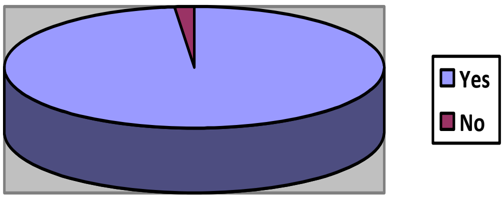


⬛ Strongly Disagree 🟨 Disagree 🟦 Neutral 🟪 Agree 🟥 Strongly Agree

4.1.4 Secure E-Transaction Services.

The study sought to find out whether the banks have a secure e-transaction services in place. The results as reflected in Figure 5, showed that 98.2% of the sampled banks offer secure e- banking services while only 1.8% of the banks indicated they might not have a fully secure e-banking services.

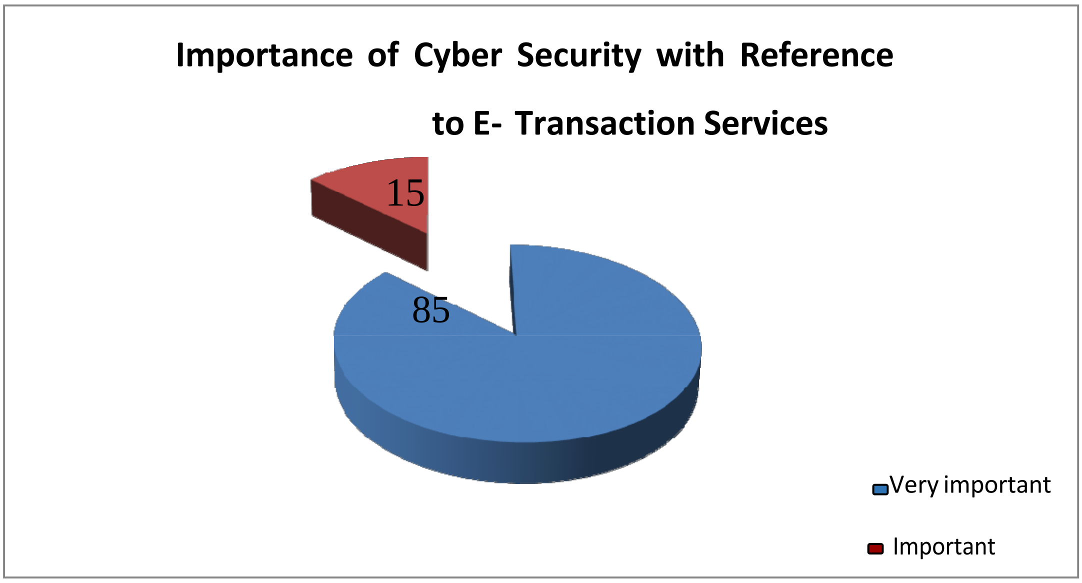
Figure 5: Secure E-Transaction Services



4.1.5 Importance of Cyber Security.

The study sought to find out how important cyber security matters were with reference e-transaction services on the sampled banks. 85% of the respondents opinioned that cyber security was very important while 15% of the respondents pinioned that cyber security was important.

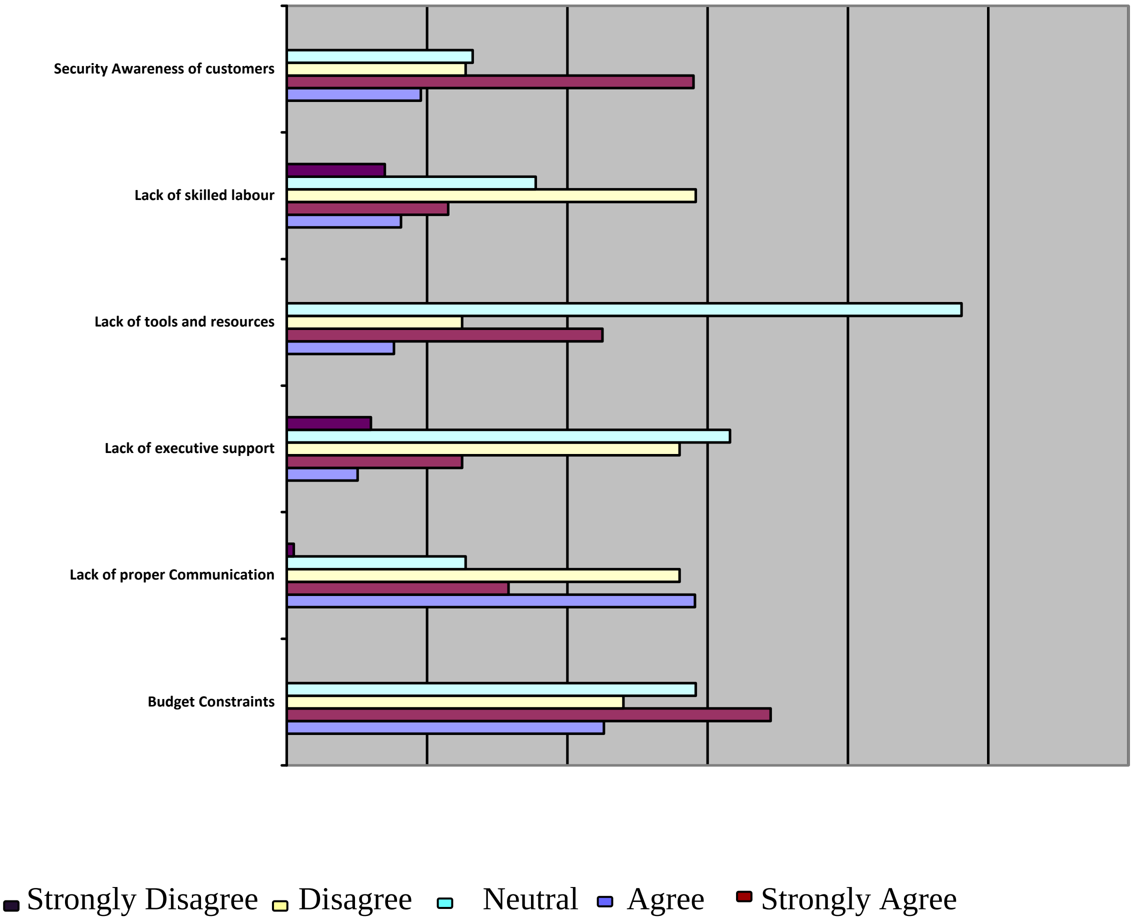
Figure 6: Cyber Security Importance



4.1.6 Obstacles to Information Security Effectiveness

In terms of the obstacles prevent information security effectiveness Figure 4.3 indicate that respondents agreed that lack of proper communication is a major obstacle at 93%. In addition, lack of skilled labor and security awareness by customers (at 80%) was also cited as a major obstacle in information security effectiveness. Lack of executive support was also highly rated beyond average as an obstacle in information effectiveness (at 51%).

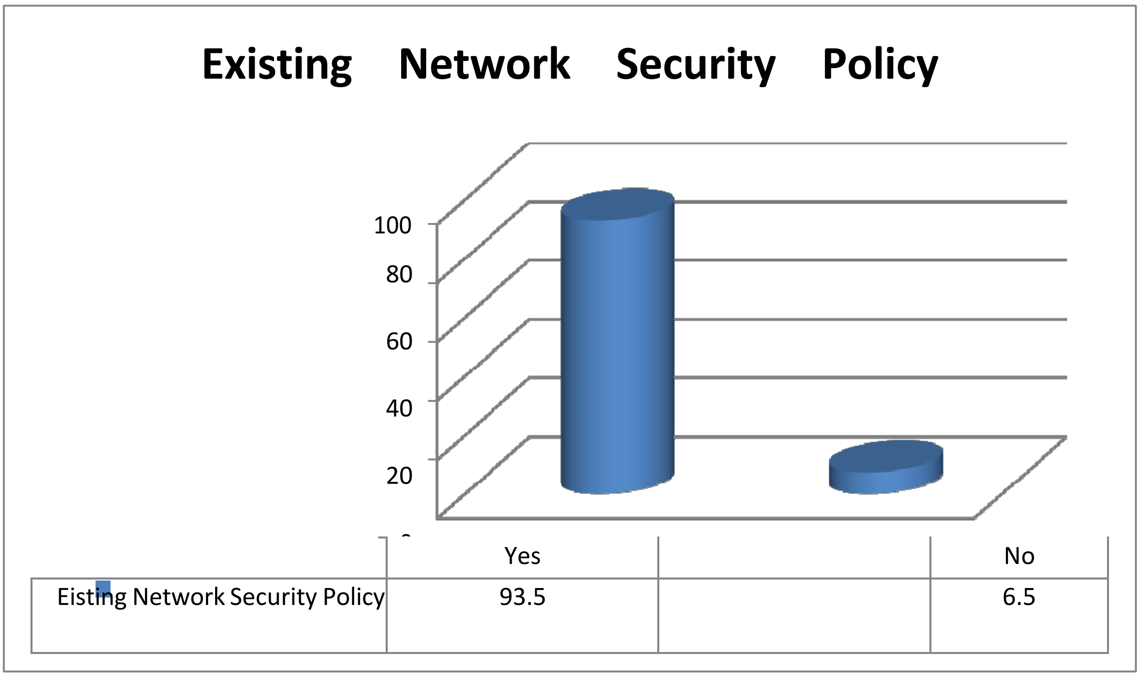
Figure 7: ***Obstacles to Information security effectiveness***



4.1.7 Existence of Network Security Policy

The study sought to find out whether the commercial banks had a network security policy. As shown in figure 8. Ninety two point Seven Percent (93.5%) of the respondents indicated that they have a network security policy while 6.5% of the respondents indicated they did not have a network security police.

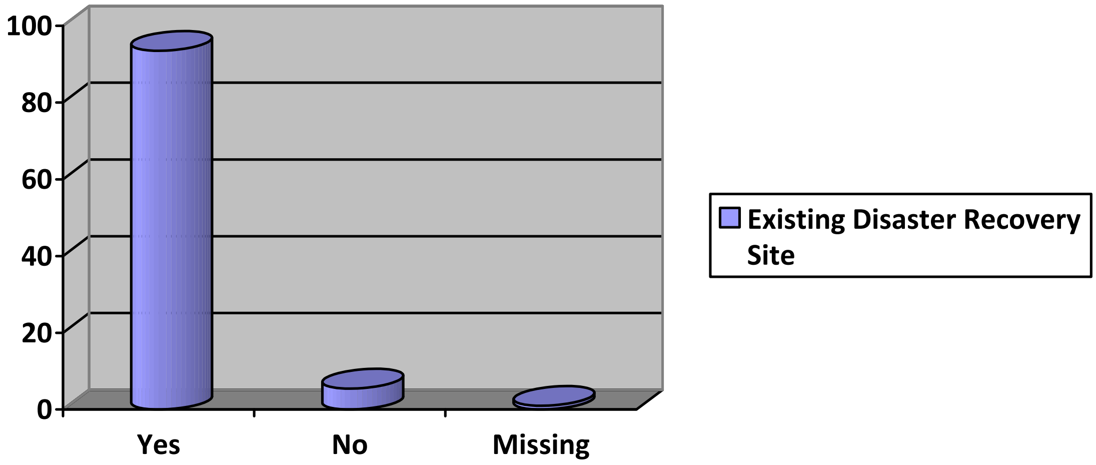
Figure 8: Network Security policies.



4.1.8 Existence of a Disaster Recovery Site

The study sought to find out whether the commercial banks had a disaster recovery site. As shown in figure 9, 93.5% of the respondents agreed to have an existing and working disaster recovery site while 6.5% of the respondents disagreed to having disaster recovery site.

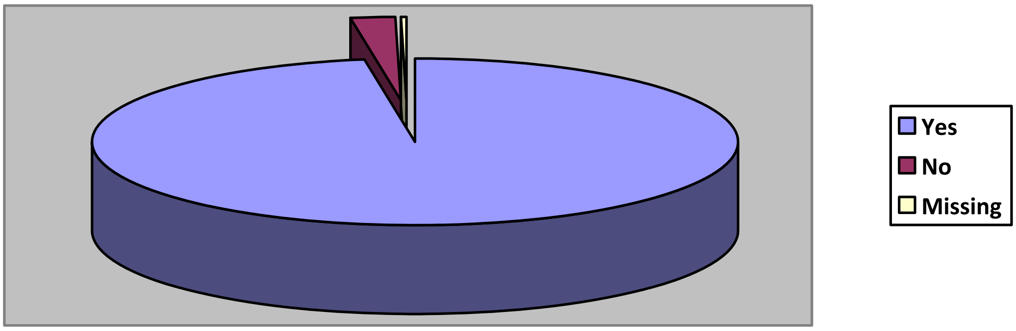
Figure 9: Existence of a Disaster Recovery Site



4.1.9 Existence of a Firewall

Ninety Seven point five percent (97.5%) of the respondents articulated that their organizations used firewalls and 2.5% of the respondents articulated that their organizations did not use firewalls. The results of these responses are shown on figure 10

Figure 10: Existence of a firewall

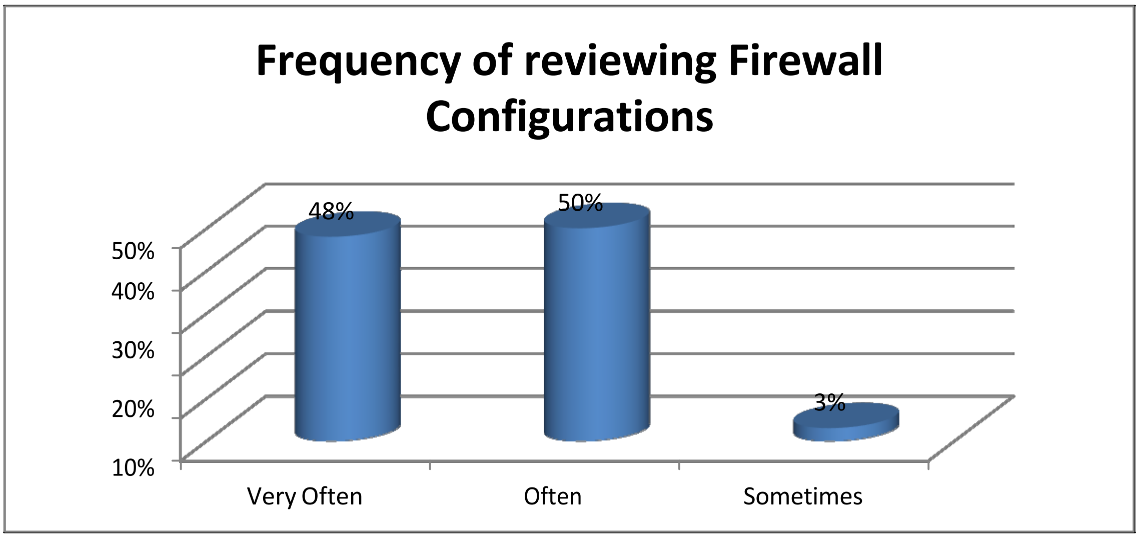


4.2.0 Frequency of Reviewing Firewall Configurations

The study sought to find out the frequency of reviewing firewall configurations by the commercial banks. Figure 11 diagrammatically represents the respondent's responses that 50% of the respondents indicated that they review the configurations of their

firewalls often; 48% indicated they review their firewalls very often while 3% indicated they review their firewall configurations sometimes.

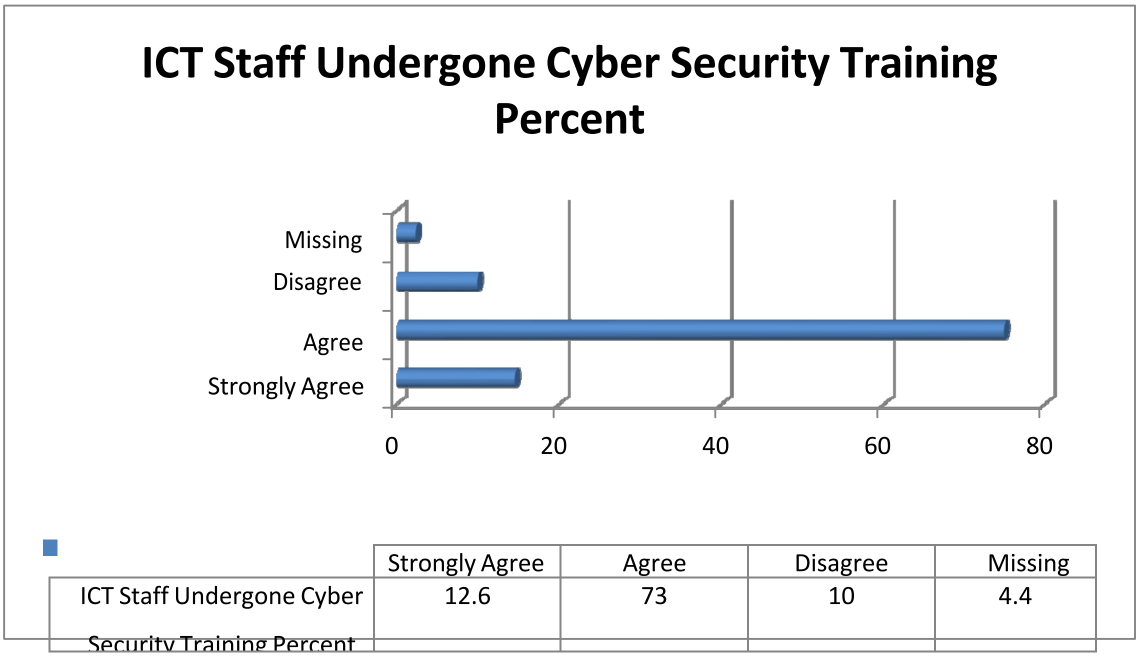
Figure 11: Firewall Configurations review



4.2.1 ICT Staff in have Undergone Cyber Security Training

The study sought to find out if ICT staff have undertaken cyber-security training. Seventy Five percent (73%) of the respondents stated that they agreed that the ICT staff had been trained; 12.6% stated that they strongly agreed that their ICT Staff had undergone Cyber Security training while 14.4% stated that they disagreed that their ICT Staff had undergone Cyber Security training. These responses are in

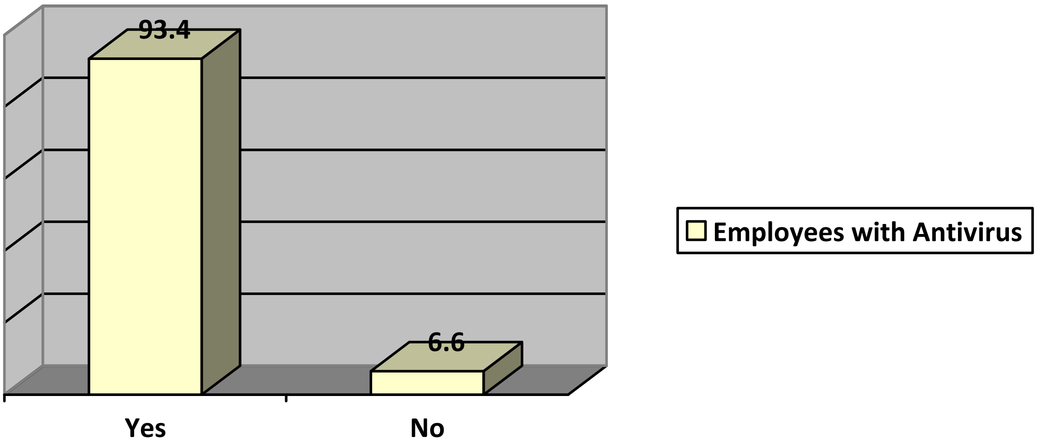
Figure 12: Cyber Security Training Undergone



4.2.2. Bank Employs the Use of Antivirus

The study sought to find out if the commercial banks in Kenya employ the use of an antivirus. Ninety five point one percent (93.4%) of the respondents indicated that they use an antivirus while 6.6% of the respondents indicated that they do not employ the use of an antivirus. Figure 13 below tabulates the respondent's views.

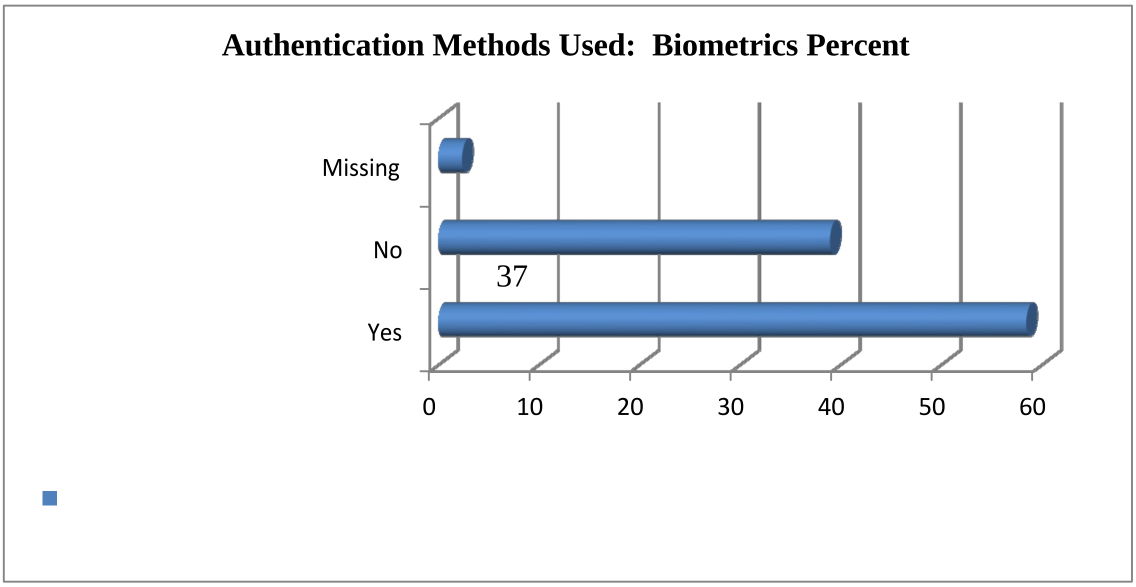
Figure 13: Employees with Antivirus



4.2.3 Authentication Methods Used: Biometrics

The study sought to find out the authentication methods used in the Kenyan commercial banks. As per the diagrammatic representation in figure 14, 55.5% of the respondents indicated that they use biometrics as a method of accessing a network while 39% of the respondents indicated that they do not use biometrics as a method of accessing a network while.

Figure 14: Authentication Using Biometrics

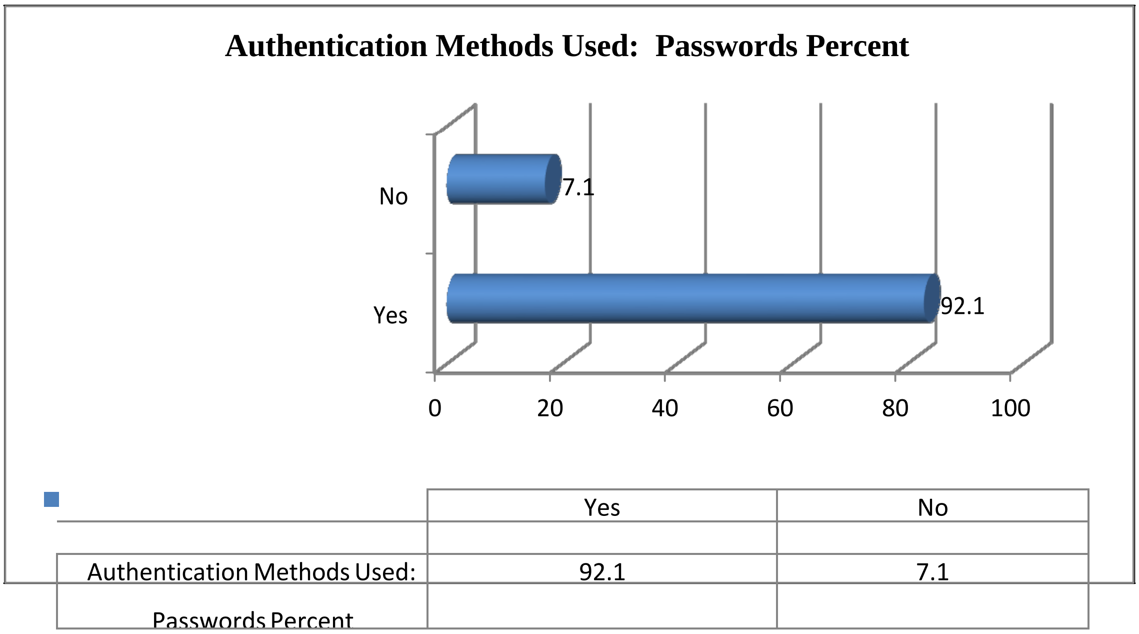


	Yes	No	Missing
Authentication Methods Used:	55.5	39	5.5

4.2.4 Authentication Methods Used: Passwords

The study sought to find out the authentication methods used in the Kenyan commercial banks. As per the illustration on Figure 15, 92.1% of the respondents indicated that they use a password as a method of accessing a network while 7.9% of the respondents indicated they did not use passwords as an authentication method in their banks.

Figure 15: Authentication Methods Used: Passwords

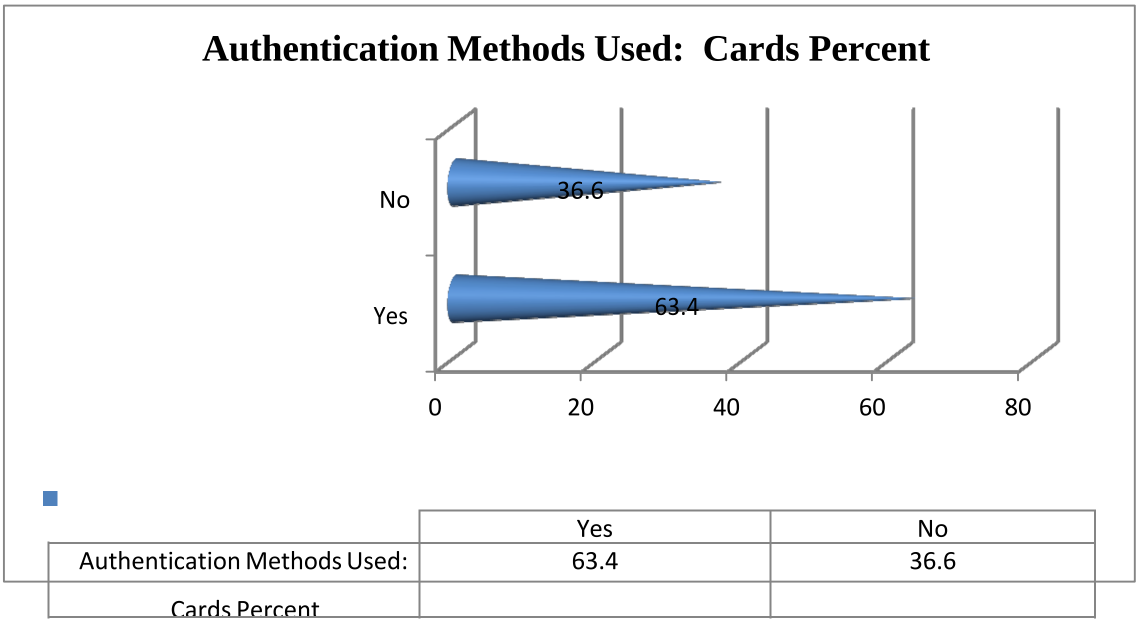


■	Yes	No
Authentication Methods Used: Passwords Percent	92.1	7.1

4.2.5 Authentication Methods Used: Cards

The study sought to find out the authentication whether the commercial banks were using cards as a method of preventing cybercrime. As per the illustration on Figure 15 , 63.4% of the respondents mentioned that they use cards as a method of accessing a network while 36.6% of the respondents mentioned that they did not use passwords as an authentication method in their banks.

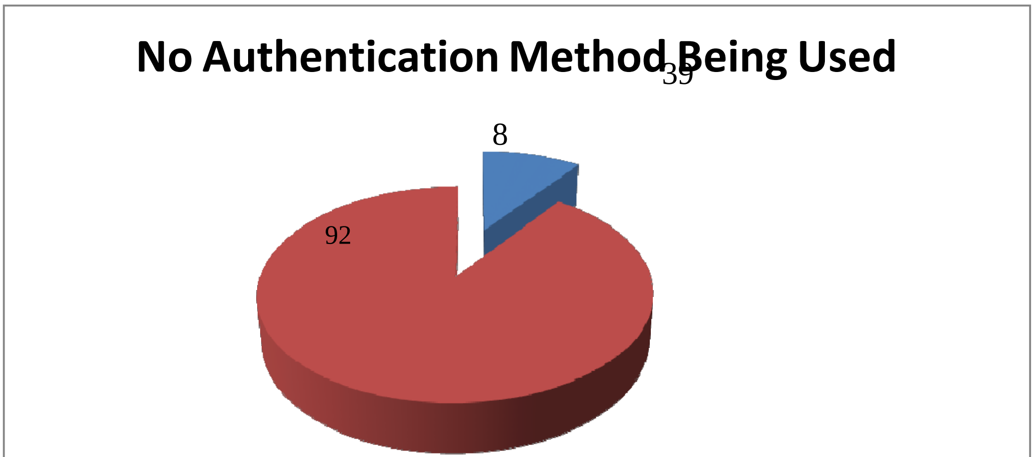
Figure 15: Cards Used for Authentication methods



4.2.6 No Authentication Methods Used

The study sought to find out if the commercial banks had methods of authenticating a customer or user into the network. Ninety two Percent (92%) of the respondents pronounced that they use authentication methods and only 8% of the respondents pronounced that they did not use authentication methods.

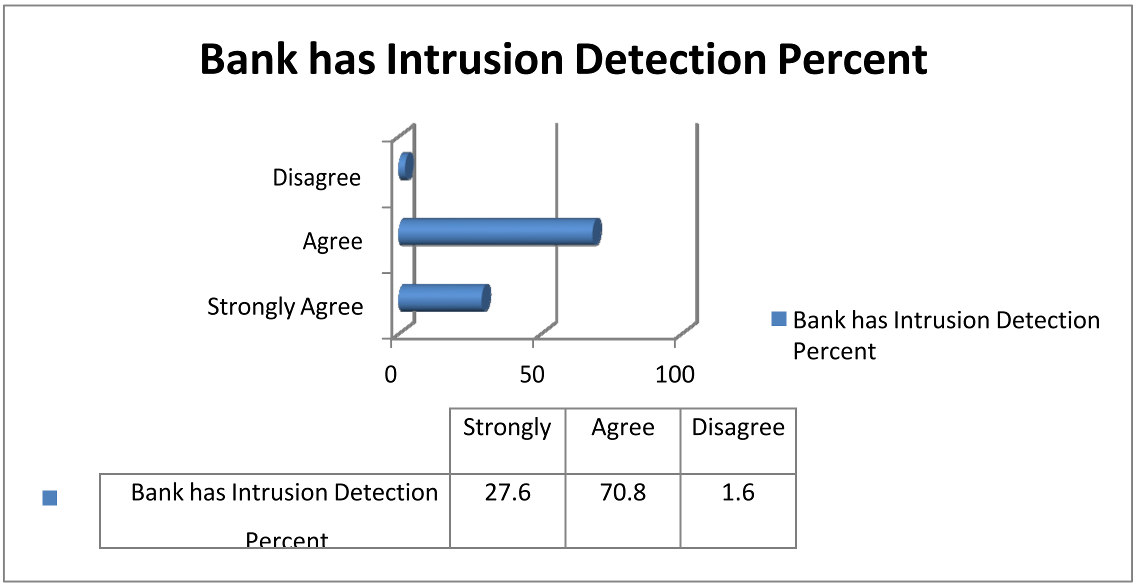
Figure 16: No Authentication method



4.2.7 Bank has an Intrusion Detection System for Logical Intrusions

The study sought to find out whether the banks have an intrusion detection system for logical intrusion as a constituent of threat model and prevention. Figure 17 diagrammatically shows the respondents responses. Twenty seven point three percent (27.6%) of the respondents expressed that they strongly agreed that their banks employed the use of intrusion detection systems, 70.8% of the respondents expressed that they agreed that their banks employed the use of intrusion detection systems agreed and 1.6% of the respondents expressed that they disagreed that their banks employed the use of intrusion detection systems.

Figure 17: Intrusion detection

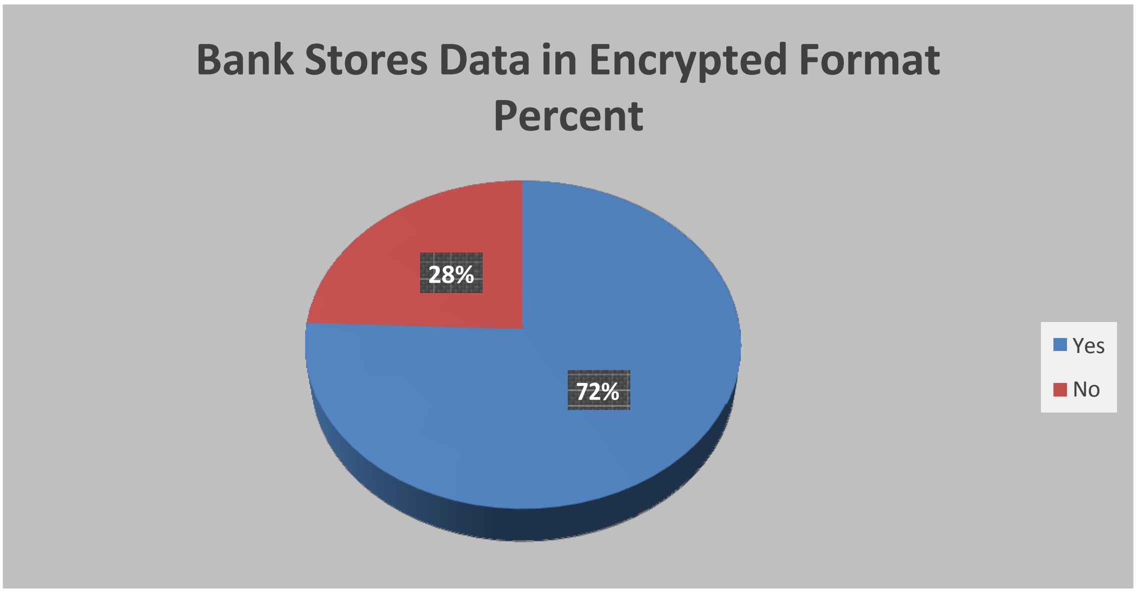


	Strongly	Agree	Disagree
🟦 Bank has Intrusion Detection Percent	27.6	70.8	1.6

4.2.8 Bank Stores Data in Encrypted Format

The study sought to find out whether the banks store data in encrypted format as a constituent of threat model and prevention. As represented in Figure 18, 72.6% of the respondents pinioned that their banks store data in encrypted format while 27.4% of the respondents pinioned that their banks store do not data in encrypted format.

Figure 17: Bank Data store Encryption

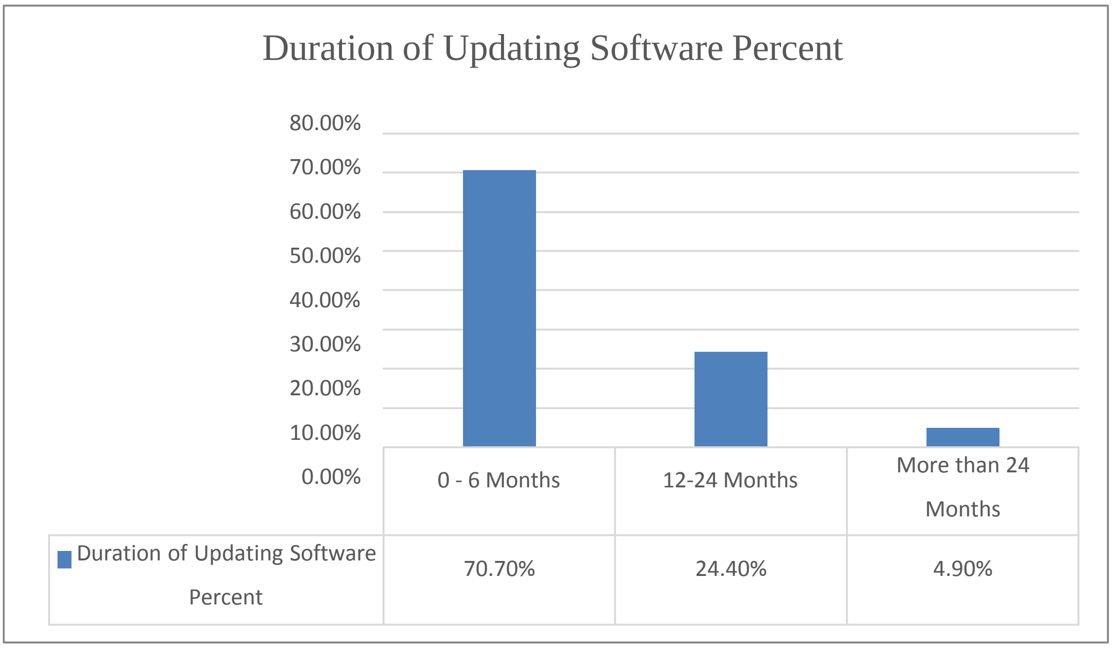


A cross tabulation showed that there was a positive relationship intrusion detection system in banks that store data in encrypted format. It showed that majority of the respondents either strongly agreed or agreed 46% that banks with an intrusion detection system for logical intrusion store data in encrypted format.

4.2.9 How Often the Banks Updates/Patches their Software

The study sought to find out how often the banks update/patches its software as a constituent of threat model and prevention. The results in Figure 19 showed that 70.7% or the respondents expressed that they update/patch their software between 0-6 months, 24.4% or the respondents expressed that they update/patch their software between 12-24 months and 4.9% of the respondents expressed that they update/patch their software within a period of more than 24 months.

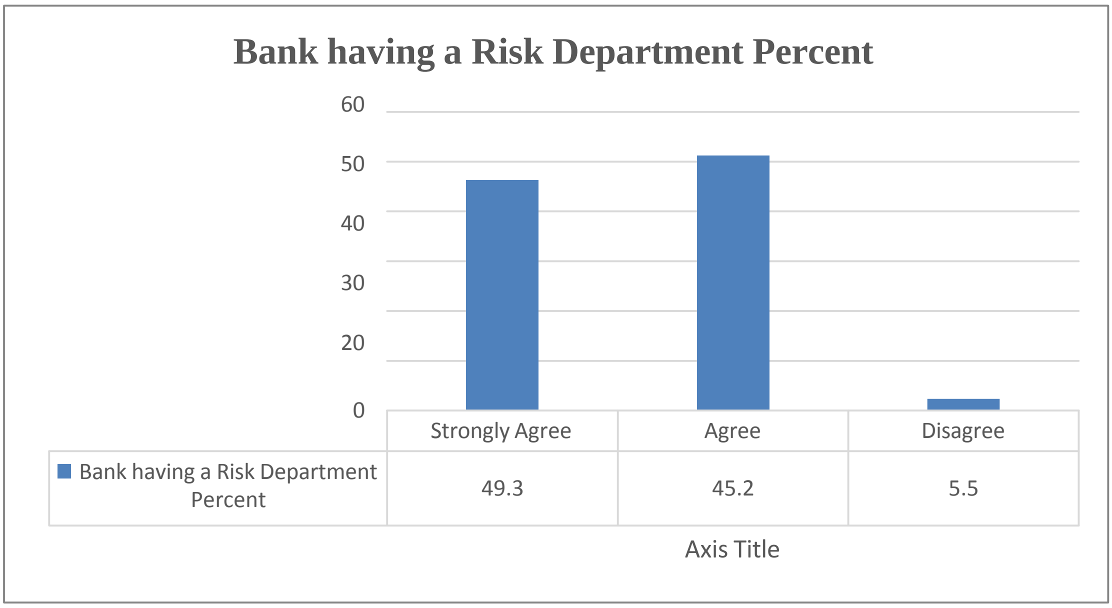
Figure 18: Patches and Software in Banks



4.3.0 Bank having a Risk Department Dealing with Risk Associated with Technology

The study sought to find out whether the banks had a risk department dealing with risk associated with the technology as a constituent of threat model and prevention. The results in Figure 19 enumerated that 49.3% of the respondents indicated that they strongly agreed that their firms had risk departments dealing with risk associated with technology; 45.2% of the respondents indicated that they agreed that their firms had risk departments dealing with risk associated with technology agreed while 5.5% of the respondents indicated that they disagreed that their firms had risk departments dealing with risk associated with technology.

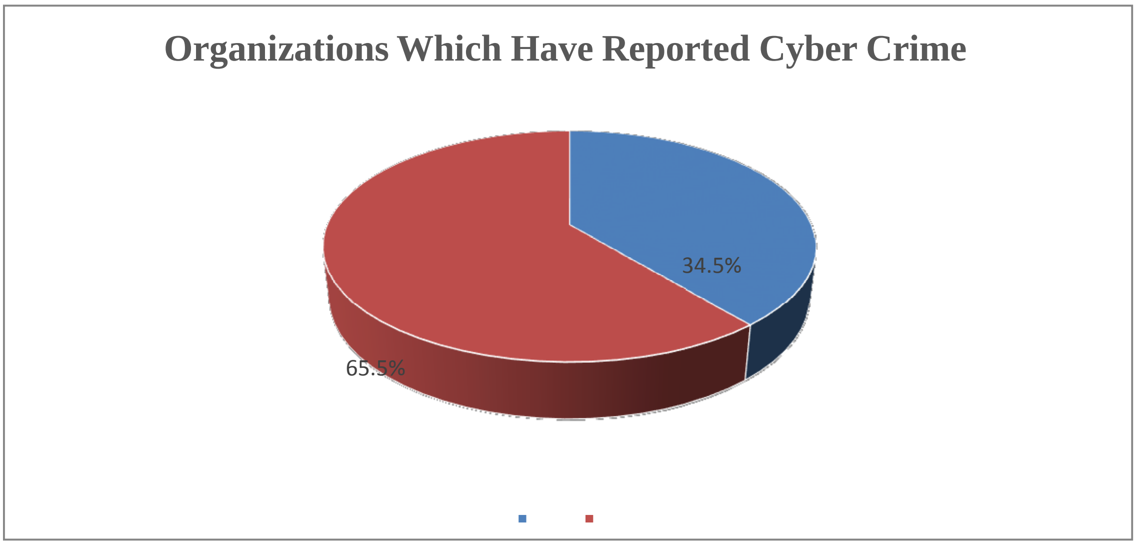
Figure 19: Banks having risk department.



4.3.1 Reporting Any Cases of Cybercrime

The study sought to find out whether commercial banks reported any cases of cybercrime. Sixty one point one percent (65.5%) of the respondents cited that they had not reported any cases of cybercrime while 34.5% of the respondents cited that they had reported any cases of cybercrime. The diagrammatic representation of these citing is shown in Figure 20.

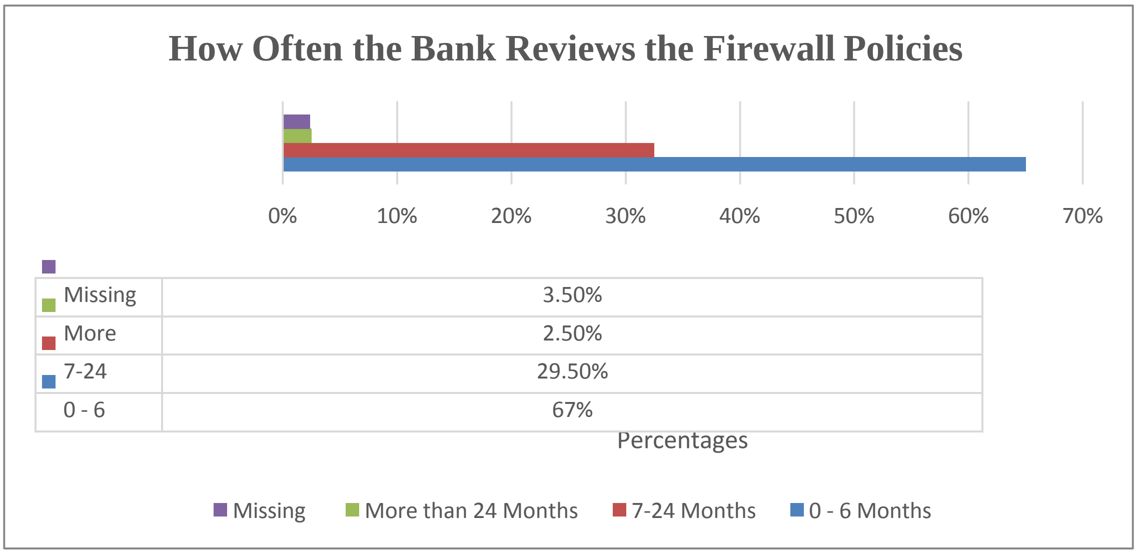
Figure 20: Cases reported for cybercrime



4.3.2 How Often the Banks Review the Firewall Policies

The study sought to find out how often the banks reviewed the firewall policies as a way of regulating cybercrime. Figure 21 is a pictographic representation of the responses from the respondents. Sixty seven percent (67%) of the respondents indicated they reviewed their firewall policies in less than 6 months, 29.5% of the respondents indicated they reviewed their firewall policies in a duration of between 7-24 months while 3.5% of the respondents indicated they reviewed their firewall policies in more than 24 months.

Figure21: How Often the Bank Reviews the Firewall Policies



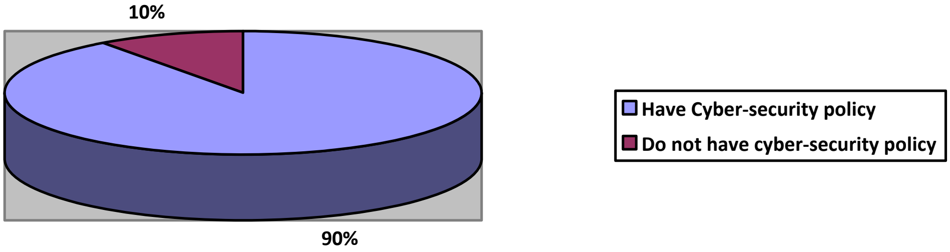
Missing	3.50%
More	2.50%
7-24	29.50%
0 - 6	67%

From the respondents responses. There was a significant negative relationship between how often the bank reviews the firewall policies and the average income per month r (36) = -.440. p=006

4.3.3 Bank has a Cyber –Security Policy

The study sought to find out how often the banks had a cyber-security policy as a way of regulating cybercrime. Graph 4.4.3 is a visual representation of the responses given by the respondents. Of all the respondents, 93% of them specified they had a cyber-security policy while 7% of them specified they did not have a cyber-security policy.

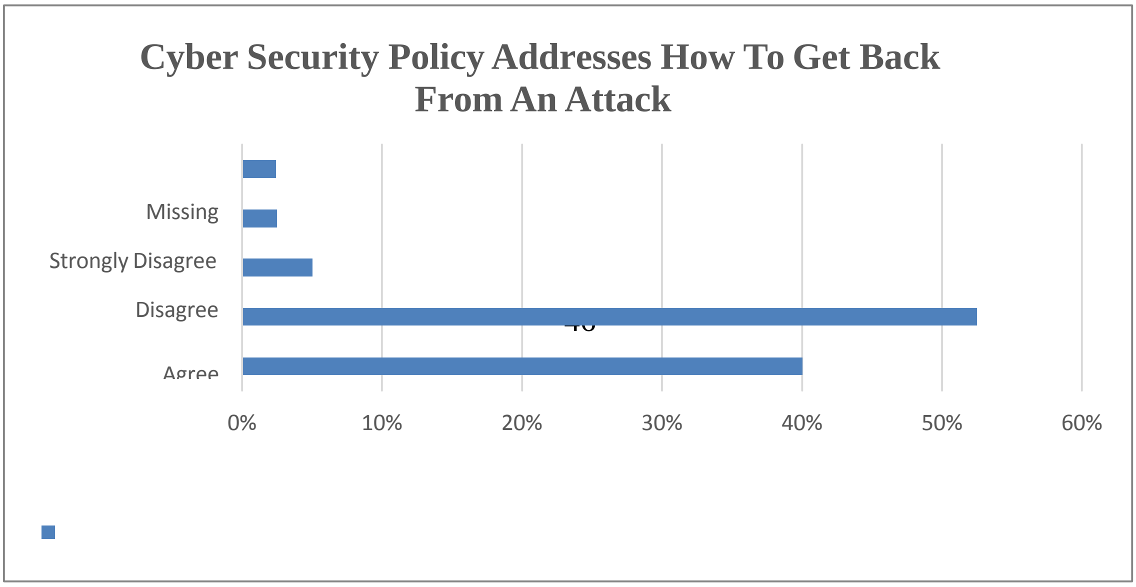
Figure 23: Bank has Cyber- Security policy



4.3.4 Cyber Security Policy Addresses how to get back from an Attack

The study sought to find out whether the banks that had a cyber-security policy, which described how to get back from an attack. Fifty Two point five percent (52.5%) of the respondents indicated that they agreed that their Cyber Security policies described on how to get back from an attack 40% of the respondents indicated that they strongly agreed that their Cyber Security policies described on how to get back from an attack, 5% of the respondents disagreed that their Cyber Security policies described on how to get back from an attack and 2.5% of the respondents indicated that they strongly disagreed that their Cyber Security policies described on how to get back from an attack strongly disagreed.2.4% of the respondents did not respond to this question.

Figure 24 Cyber Security Policy Addresses how to get back from an Attack

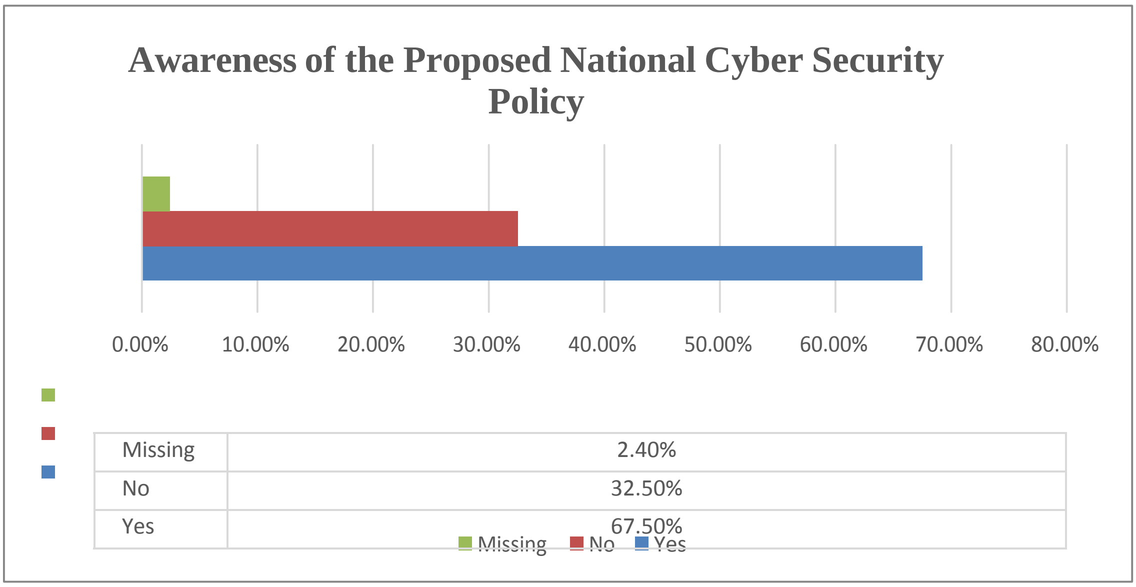


	Strongly Agree	Agree	Disagree	Strongly	Missing
Response Percent	40%	52.50%	5%	2.50%	2.40%

4.3.5 Awareness of the Proposed National Cyber Security Policy#

The study sought to find out whether the banks were aware of the proposed National Cyber Security Policy which is a way of regulating cybercrime. Figure 25 is a pictorial representation of the responses obtained from the respondents. Sixty Seven point five percent (67.5%) of the respondents expressed they were aware of the proposed national cyber security policy while 31.7% of the respondents expressed they were not aware of the proposed national cyber security policy.

Figure 25 Awareness of the Proposed National Cyber Security Policy

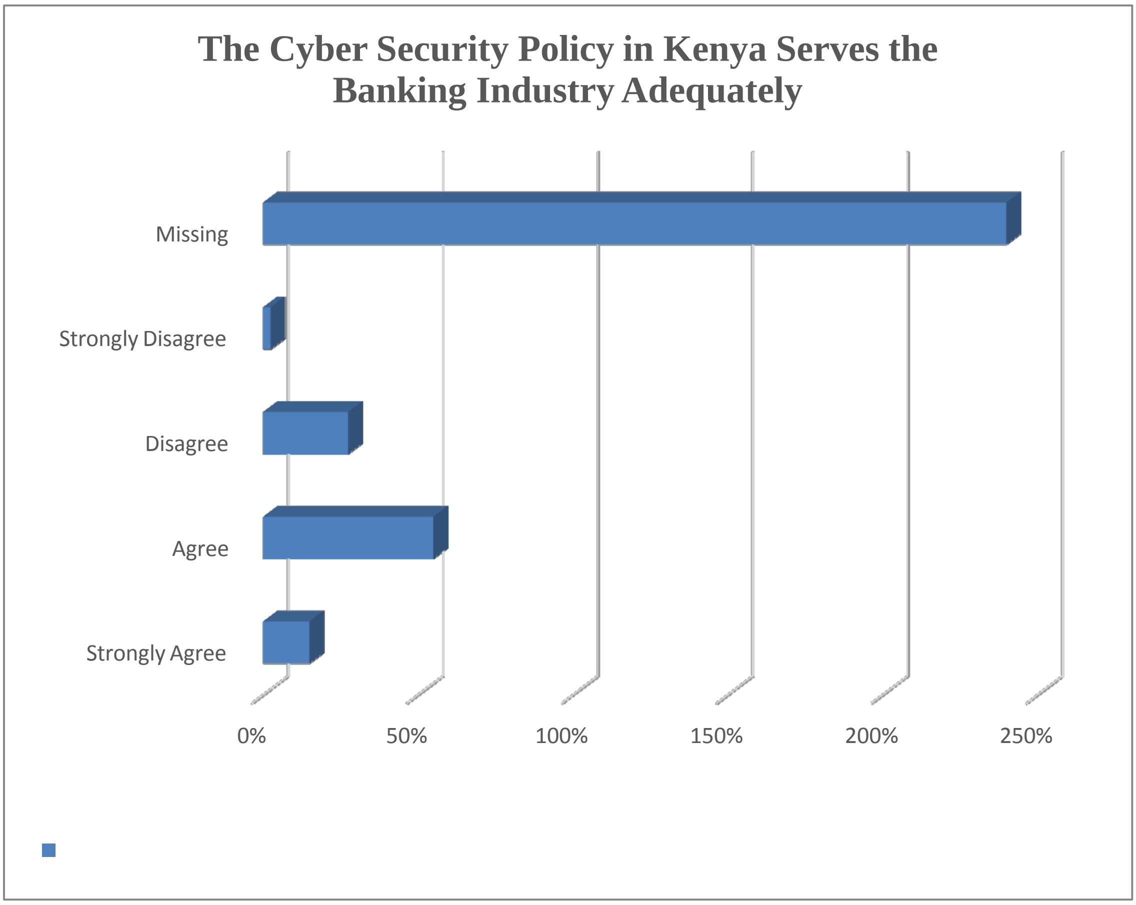


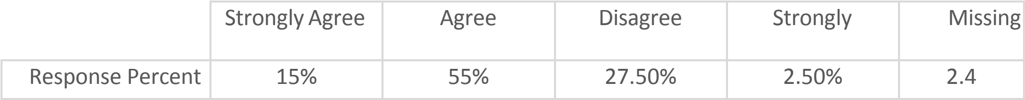
Missing	2.40%
No	32.50%
Yes	67.50%

4.3.6 The Cyber Security Policy in Kenya Serves the Banking Industry Adequately

The study sought to find out from the banks whether the Cyber Security Policy in Kenya Serves the Banking Industry adequately in tandem with nationally recognized standards. Figure 26 exhibited that 55% of the respondents pronounced that they agreed the Cyber Security Policy in Kenya serves the banking industry adequately, 14.6% of the respondents pronounced that strongly agreed the Cyber Security Policy in Kenya serves the banking industry adequately, 26.8% of the respondents pronounced that they agreed the Cyber Security Policy in Kenya serves the banking industry adequately 2.4% of the respondents pronounced that they strongly disagreed that the Cyber Security Policy in Kenya serves the banking industry adequately.

Figure 26 the Cyber Security Policy in Kenya Serves the Banking Industry Adequately



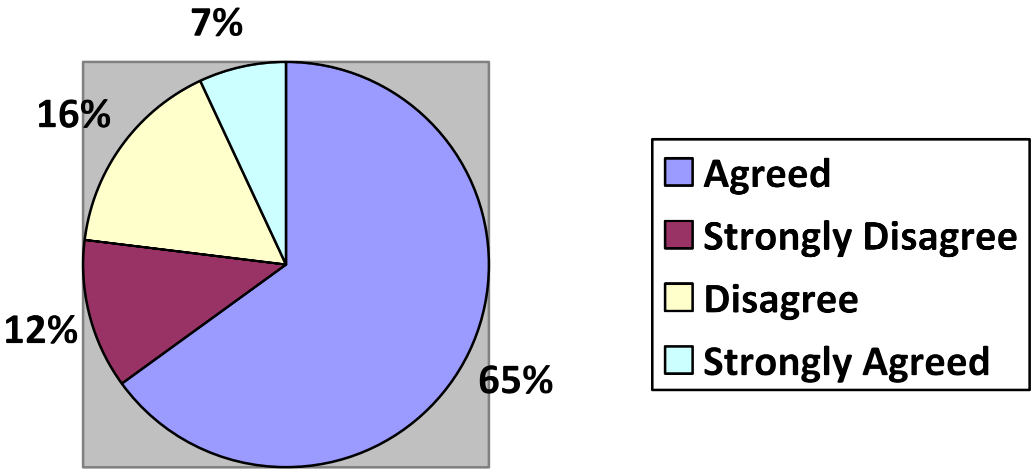


	Strongly Agree	Agree	Disagree	Strongly	Missing
Response Percent	15%	55%	27.50%	2.50%	2.4

4.3.7 Bank had educated its Customers to Protect Themselves from Cyber Stalking

The study sought to find out whether the bank has educated its customers to protect themselves from cyber stalking. Fifty Six Percent (65%) of the respondents indicated that they agreed that they had educated customers to protect themselves from cyber stalking while 12% of the respondents indicated that they strongly disagreed that they had educated customers to protect themselves from cyber stalking; 16% of the respondents indicated that they disagreed that they had educated customers to protect themselves from cyber stalking and another 7% of the respondents indicated that they strongly agreed that they had educated customers to protect themselves from cyber stalking.

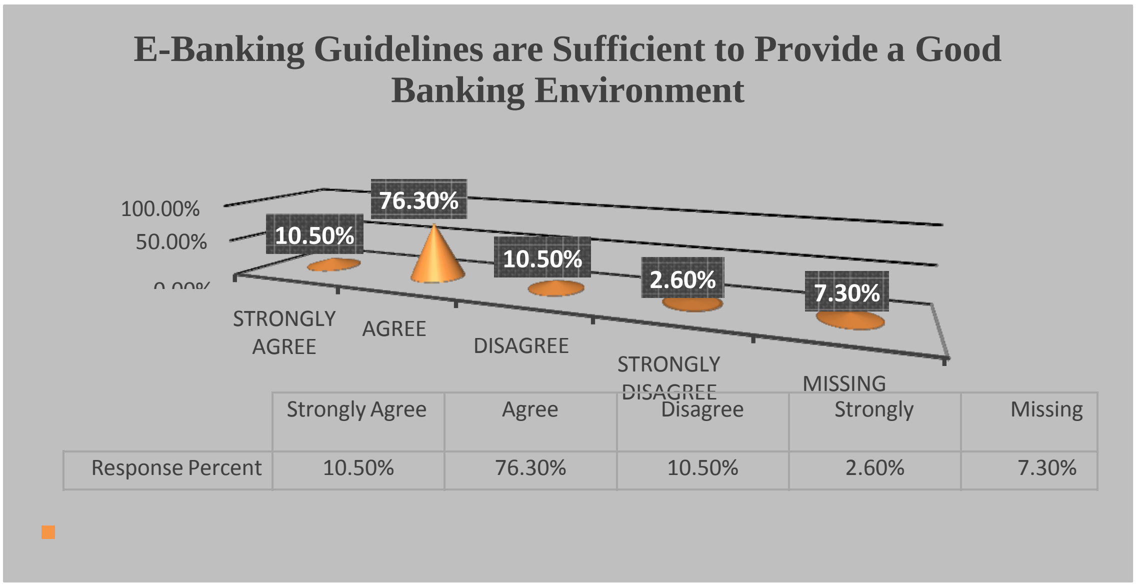
Figure 26 Educating of customers to protect themselves by the banking institutions



4.3.8 Electronic Banking Guidelines are Sufficient to Provide a Good Banking Environment

The study also sought to assess from the commercial banks whether the electronic banking guidelines were sufficient to provide a good banking environment. The responses collected from the respondents are represented in the Figure 27 below. Seventy Six point three percent (76.3%) of the respondents mentioned that they agreed that Electronic Banking Guidelines were sufficient to provide a good banking environment, 10.5% of the respondents mentioned that they strongly agreed that Electronic Banking Guidelines were sufficient to provide a good banking environment and 10.5% of the respondents mentioned that they disagreed that Electronic Banking Guidelines were sufficient to provide a good banking environment.

Figure 27: Electronic Banking Guidelines are Sufficient to Provide a Good Banking Environment

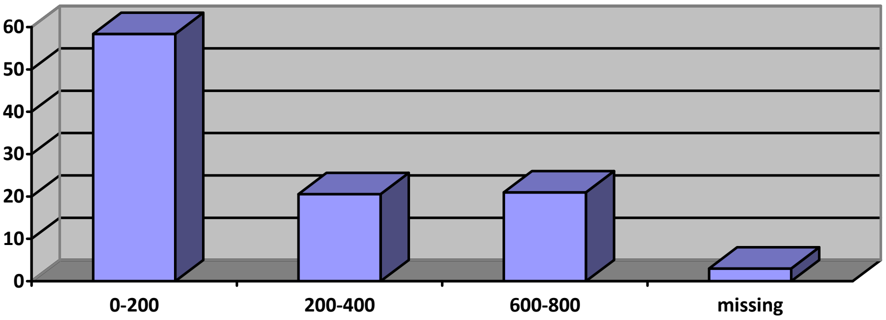


	Strongly Agree	Agree	Disagree	Strongly	Missing
Response Percent	10.50%	76.30%	10.50%	2.60%	7.30%

4.3.9 Number of Non ICT Staff Trained on Cyber Security

The study sought to find out the number of non ICT staff trained on cyber security. The respondent’s responses are in Figure 28. Fifty eight Point four Percent (58.4 %) of the respondents indicated that non ICT staff members in their organizations who were trained on cyber security were ranging between 0-200, 20.6% of the respondents indicated that non ICT staff members in their organizations who were trained on cyber security were ranging between 601-800 members, 21% of the respondents indicated that non ICT staff members in their organizations who were trained on cyber security were ranging between 201-400 non ICT staff members trained on cyber security.

Figure 28 Number of non-trained ICT staff

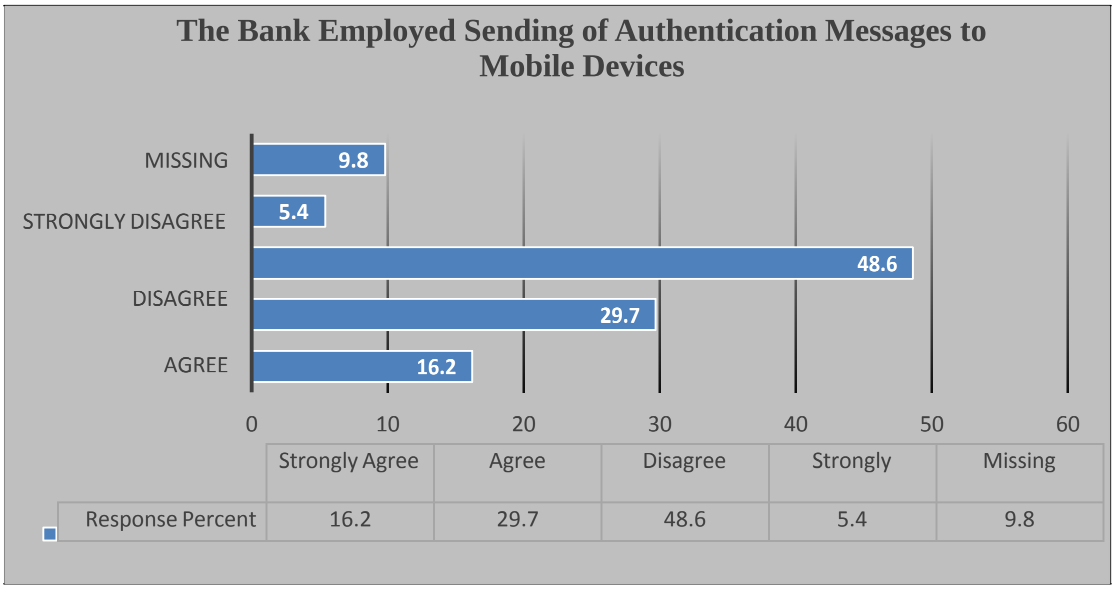


	0-200	201-400	601-800	Missing
No of ICT Staff trained for cyber security.	58.4%	20.6%	21%	1.2%

4.4.0 Banks Employ Sending of Authentication Messages to Mobile Devices.

The research sought to find out whether banks employed sending of authentication messages to mobile devices. Sixteen point two percent (16.2%) of the respondents said that they strongly agreed that their institutions send authentication messages to mobile devices; 29.7% of the respondents said that they agreed that their institutions send authentication messages to mobile devices 48.6% of the respondents said that they strongly disagreed that their institutions send authentication messages to mobile devices while 5.4% of the respondents said that they strongly disagreed that their institutions send authentication messages to mobile devices. The figure 28 below depicts these responses.

Figure 28: Banks Employ Sending of Authentication Messages to Mobile Devices.

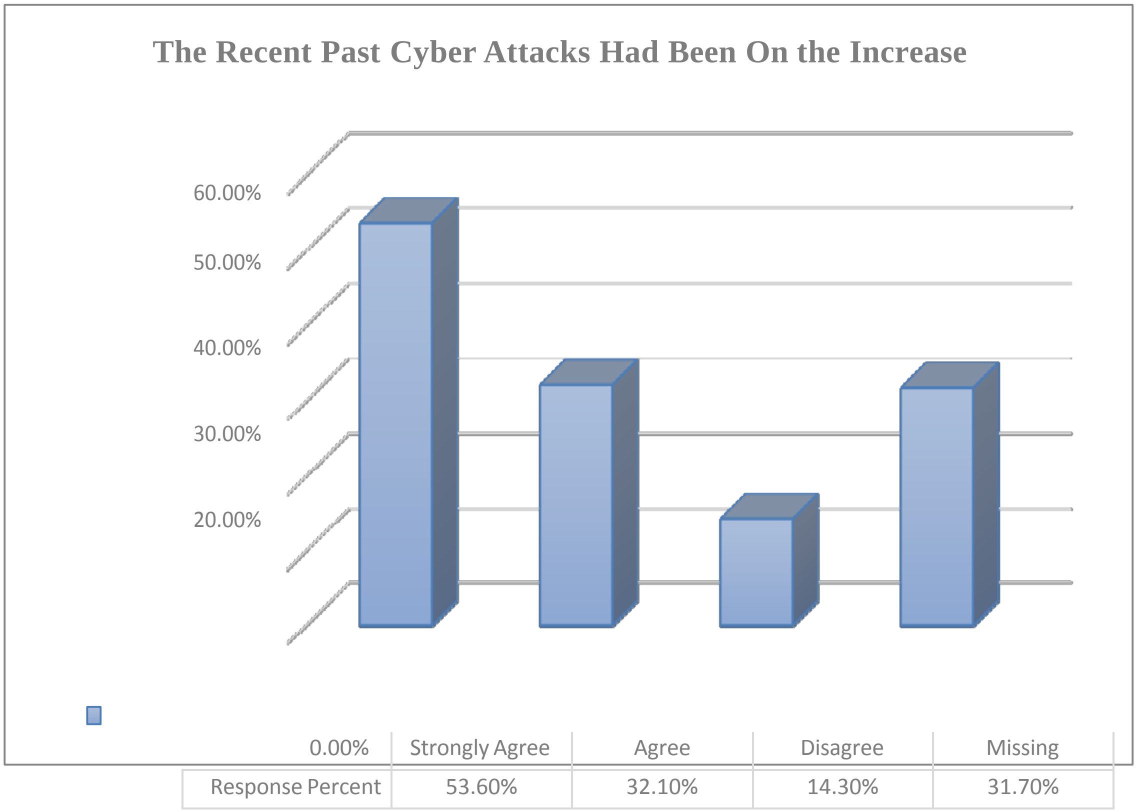


	Strongly Agree	Agree	Disagree	Strongly	Missing
■ Response Percent	16.2	29.7	48.6	5.4	9.8

4.4.1 The Recent Past Cyber Attacks Had Been on the Increase

The study sought to find out whether the recent past cyber-attacks had been on the increase. Fifty three point six percent (53.6%) of the respondents pinioned that they strongly agreed that in the recent past cyber-attacks had been on the increase, 32.1% of the respondents pinioned that they agreed that in the recent past cyber-attacks had been on the increase and 14.3% of the respondents pinioned that they disagreed that in the recent past cyber-attacks had been on the increase. Graph 4.5.19 shows in a tabular format the opinions of the respondents.

Figure 29: The recent past cyber Attacks had been on increase



4.4.2 Discussion of the findings

In summary, the study sought to find out factors contributing to occurrence of cybercrime on e-banking in commercial banks in Kenya. The results showed data was collected from 39 banking institutions. This study was targeting a sample of 90 respondents resulting in a 100% response rate.

Seventy three Percent (73%) of the respondents were aged between 25-35 years. There was representation of both gender majority being males who constituted of 68% of the total sample population. Fifty three percent (53%) of the respondents had a 1st degree, most of whom were IT experts while the lowest qualification was Professional certifications constituting 20% of the respondents. The sample comprised of ICT staff in various levels within a bank setup. This information was important for validity and authentication of the research. Of the above described respondents, Fifty Two point Six percent (52.6%) of the respondents indicated that they strongly agree that their organizations employed the use of Technology to serve their customers.

The study sought to find out the factors contributing to the occurrence of cybercrime on e-banking in commercial banks in Kenya. Ninety two point seven percent (93.5%) of the respondents specified that they have a network policy. Ninety two point five Percent (93.5%) of the respondents agreed to have a disaster recovery site. Ninety two point five percent (97.5%) of the commercial banks had a firewall. The respondents were also asked to indicate how often their firewall configurations were reviewed. The most frequent review was done in intervals described as very often and this response was given by 48% of the respondents while the one that was only reviewed sometimes was at 3%. The 95.1% of the respondents expressed that that Kenyan commercial banks employ the use of an antivirus.

Of importance as well was to know the level of awareness, sensitization and education on cybercrime an if the ICT staff and the other staff in the commercial banks had been take through the same? 12.6% stated that they strongly agreed that their ICT Staff had undergone Cyber Security training. With regards to the customers, Fifty Six Percent (65%) of the respondents indicated that they agreed that they had educated customers to protect themselves from cyber stalking. It is notable to say that Sixteen point two percent (5.4%) of the respondents said that they strongly agreed that their institutions send authentication messages to mobile devices. There was also a representation of the various authentication methods used within the banks where the respondents pinioned that the use of No authentication methods ranked highest, followed by the use of Biometrics.

CHAPTER FIVE: SUMMARY, CONCLUSSIONS AND RECOMMENDATIONS

5.1 Introduction

This study had three objectives. First was to establish ICT security threats facing electronic transactions in the cyber space. It also sought to establish factors that accelerate Cyber security threats on Electronic transaction. Finally was to establish a cyber-security model for adoption of ICT security on Electronic transaction by the banking sector in Kenya.

5.2 Summary of findings

The study targeted the projects department, Alternate business channels such as mobile banking, internet banking, networking and IT security departments and finally data and core departments. The study employed a case study approach and used questionnaires to collect the required information. The number of questionnaires returned was 76 and the return rate was 98%. Data was analyzed using the Statistical Package for Social Sciences (SPSS) version 17.0 to process the frequencies, percentages and descriptive statistics which were used to discuss the findings. The following were the findings of the study.

Most banking institutions irrespective of size experienced intrusions or attempted intrusions into their IT systems over the past three years. The attempted methods cover a wide range, with most banking institutions reporting incidents involving malicious software (malware) (29%), phishing (30%), pharming (31%), and botnets or zombies (15%). The larger the bank, the more likely it appeared to experience malware and phishing attempts. The most frequent types of wrongful activity resulting from a cyber intrusion reported by institutions were fraud (at 85%), careless or unaware employees (at 88%), internal attacks (at 73%), vulnerabilities relating to mobile computing (at 89%), cyber-attacks to steal financial information (at 89%). Although several banking institutions reported numerous attempted systems intrusions over the prior 12 months, very few banks experienced successful breaches resulting in significant monetary damages. But a greater number of large Banks than small and medium banks reported experiencing financial losses resulting from cyber breaches. These breaches are usually information breaches, 76% of banking institutions indicated that they have suffered breaches within the previous 12 months. These breaches included: inadvertent breaches by users, deliberate attacks, asset theft, equipment failure, backup failure, data theft, site disaster, copyright infringement, and privacy breaches.

Although Banking institutions have taken significant steps to increase cyber security efforts in recent years, banks and other financial services companies will continue to be challenged by the speed of technological dynamic change and the increasing sophisticated nature of threats. While institutions are aware that the threat landscape is constantly evolving, they may find it difficult to keep up with the latest developments amid competitive pressure to integrate new technologies into their product offerings e.g. Mpesa, Mkesho, internet banking. Information sharing is a factor to consider, although institutions are keen on internal intelligence gathering they have limitation on obtaining of external information. Although institutions seem more willing than in the past to share information regarding threats and attacks, many remain hesitant to reveal perceived or actual security weaknesses to competitor. This leads to lack of proper information on the ever dynamic and sophisticated threat landscape and thus lack of proper skills to combat the threats since as the saying goes “you can’t protect yourself from what you do not know”.

Another contributing factor is the banking industry’s reliance on third-party service providers for critical banking functions. As per the findings 97% of banking institutions irrespective of size rely on third-party vendors for cyber security. In addition, most small and medium banking institutions outsource functions such as payment processing and most of their web application and online banking systems to external companies. This interconnectedness suggests that a bank`s cyber risk level depends in large part on the processes, policies and controls put in place by third parties vendors. Banks may not be permitted by their vendors to undertake penetration testing. Even more likely, small and medium institutions may not have the resources and the capacity to do so.

Almost 90% of the banking institutions reported having an information security framework in place that includes what are considered to be the key pillars of Security: Written information security policy, security awareness education and employee training, risk management of cyber-risk, inclusive of identification of key risks and trends, information security audits and incident monitoring and reporting.

However, information security frameworks and models at medium and large institutions tend to be particularly well developed, with 89% and 98%, respectively, having implemented all five pillars. Apart from the security frame work there is also the Kenya Cyber Security strategy that was developed and launched in 2014. Seventy seven point eight percent (77.8%) of the respondents expressed they were aware of the existence of the policy. The respondents were asked about their priorities in implementing the main focuses, their responses were as follows; Forty nine point five Percent (49.5%) of the respondents indicated that they would incorporate the Information Security Policy followed by the Management Controls and Procedures. The respondents ranked Cyber Security Systems and Access Management systems at 70.5% in their list of priorities. This indeed indicated a high level of commitment. The research noted that its quite difficult to come up with a common framework for all banking institutions and further on although 90% of the banks have a cyber security frame work in place they are all quite different depending on several factors. In an attempt to streamline the transaction and also as a security issue, the computer industry as a whole has already begun the move to try and standardize various protocols for e-transactions. The study also revealed that 62% of the respondents agreed the ICT staff had been trained on cyber security. These findings were aligned to Tendulkar, (2013) sentimental that who asserts that Cyber-security measures could be easily side-stepped if the crime is perpetrated by an ‘insider’

Training for all staff is important and given the innovation of cybercrime, training is best executed periodically with staff being kept up-to date on new threats and trends .

5.3 Conclusion

Conclusion is reached that the threat landscape in the banking sector are becoming very sophisticated and ever evolving this is due to the ever dynamic product development environment that is fueled by the cutting edge competition between banking institutions to provide increasingly better services to their customers. Further on the threats that have a usually larger impacts are the internal breaches that are caused by internal bank users/ staff, this is due to the fact that they understand the policies, controls and the weaknesses of the existing policies and how to manipulate them for their benefit. Most threats are usually due to weak security structure be it logical security or physical security structures this is inclusive of security policies put in place. Another conclusion is that the ultimate goal of a breach is to access sensitive information with the aim of obtaining monetary advantage.

A conclusion is reached that there are several factors that accelerate the Cyber security threat with the highest and the one with the greatest impact is insider penetration this is perceived as the most deadly since the staff is aware of the systems and processes this is inclusive of their weaknesses thus can take advantage before being detected. Another conclusion is the internal weak security infrastructures and policies this is mostly inversely proportional to the size of the banks the bigger the banking institution the more resources are allocated to the ICT security department the better the systems invested. This doesn’t apply in smaller banking institutions who tend to focus more on other core banking operations. Another conclusion is the reliant on third party vendors by the banks for e-payment systems, cloud storage, internet provision, MPLS link provision. These creates points of entry especially if the third party provider doesn’t practice certain security procedures. Penetration test becomes difficult conducting especially in smaller banks due to the magnitude of the infrastructure.

Most banking institutions have an existing Cyber-security model/frame work, unfortunately there is a tendency to have laxity when it comes to implementing of some of these policies. There is need to strictly adhere to the set model within all spheres of the organization. Due to different nature of banking institutions it’s quite difficult to adopt an all across detailed banking Cyber-security model. Though there is need to have some basic minimum security model which already exist across banking institution but there is need to emphasize the model. Another conclusion reached is reporting of the cybercrimes that have occurred to the authorities it’s lowest. Commercial banks need to come out clean and report cases of cybercrime which happen within their institutions. This shall assist the country as a whole develop proper policies and measures to safeguard the National networks. This shall also help the government to come up with the proper laws which can be used to deal with cases of cybercrime.

5.4 Recommendations

From the results of this study there are several proposed improvements that can be undertaken to improved cyber security in the banking industry. Banking institutions need to invest in proper ICT security structures example the use of new generation firewall which has capability of Intrusion prevention, advanced malware protection and URL filtering. Therefore there is need to improve the current security policies and framework that exist and to ensure that all the departments adhere to the ICT security frame work that is put in place. There is also need to share cyber intrusion and penetration between the banking industry to provide a forum to enable the industry to manage the cyber-crime menace and to improve their current systems and policies. SLA are the surest way to get proper services thus SLA between the third party vendors and the banks needs to be formulated this covers ICT security in addition to the normal availability that the third parties vendors make. Penetration test should be done at least twice a year, this allows identification of areas that could be penetrated.

5.5 Limitation of the study.

The limitation of the study was the difficulty in the obtaining of information from the banking institutions mostly due to the fear of victimization. Thus led to the inadequate information from the banking institutions. Another limitation was time allocated for data collection was limited since getting these ICT practitioners to be able to sit down and fill the questionnaires due to the nature of their jobs. Finally most of the e-transaction functionalities are operated by third party vendors it's quite difficult to obtain data that is highly relied on the third party vendor.

5.6 Suggestions for Further Research

Due to the dynamic nature of the ICT and the cyber-challenge and the ever dynamic and innovation of ICT products in the banking industry to meet the customers need and to the on the competitive edge. There is need to further study and to determine the changes and the dynamic nature of cyber-crime that becomes sophisticated with every e-transaction innovation.

REFERENCES

Authority, I. (2013). Cyber-security Framework for the Government of Kenya. Retrieved 11 15, 2013, from ICT Authority: http://www.ict.go.ke/index.php/cybrsecurity-framework-for-the-government-of-kenya.

Abramowitz, M. (1956). Research and output trends in the United States since 1870. American Economic Review 46, 5-23.

Acharya, R.N., and Kagan, A. (2004). Commercial B2B Web site attributes within the perishable sector. Journal of Internet Commerce, 3(4):79-91.

Acharya, V. V., & Subramanian, K. V. (2009). Bankruptcy codes and innovation. Review of Financial Studies, 22, 4949-4988

Aderonke, A.A., & Charles, K.A. (2010). An Empirical investigation of the level of users, acceptance of e-banking in Nigeria. Journal of Internet Banking and Commerce 15 (1), http://www.arraydev.com/commerce/jibc/ [Accessed 8th August 2011]

Adesina, A. A., & Ayo, C.K. (2010). An empirical investigation of the level of users acceptance of ebanking in Nigeria. Journal of Internet Banking and Commerce, 15(1).

Agboola, A. (2006). Information and communication technology (ICT) in banking operations in Nigeria: An evaluation of recent experiences. From http://unpan1.un.org/intradoc/groups/public/documents/AAPAM/UNPAN026533.pdf. Retrieved on 18th August 2011

Aghion, P., Bloom, N., Blundell, R., Griffith, R., & Howitt, P. (2005). Competition and innovation: An inverted-U relationship. Quarterly Journal of Economics, 120, 701-728.

Aghion, P., VanReenen, J., & Zingales, L. (2009). Innovation and institutional ownership. Working Paper, Harvard University.

Akamavi, R.K. (2005). A research agenda for investigation of product innovation in thefinancial services sector," Journal of Services Marketing, 19(6), 359-378.

Aker, J. C. (2008). Does digital divide or provide? the impact of mobile phones on grain markets in Niger. BREAD Working Paper 177.

Aker, J. C. (2010). Information from markets near and far: mobile phones and agricultural markets in Niger. American Economic Journal: Applied Economics, 2(3): 46–59.

Aker, J. C., & Mbiti, I. M. (2010). Mobile phones and economic development in Africa Journal of Economic Perspectives, 24(3),207–232, Summer 2010

Akram, J. K., & Allam, M. H. (2010). The impact of information technology on improving banking performance matrix: Jordanian banks as case study. European, Mediterranean & Middle Eastern Conference on Information Systems 2010. April 12-13 2010, Abu Dhabi, UAE.

Aliyu, A. A., & Tasmin, R.B. (2012). The impact of information and communication technology on banks' performance and customer service delivery in the banking industry. International Journal of Latest Trends in Finance & Economic Science. Vol-2 No. 1 March 2012

Allen, F. & Gale, D. (1994). Financial Innovation and Risk Sharing. Cambridge, MA: Cambridge University Press.

Anbalagan, C. (2011).Impact and role of technology in modern financial innovation and invention. Sri Krishna International Research & Educational Consortium http://www.skirec.com. Accessed on 2nd September 2011

Andy, F. (2009). Discovering Statistics using SPSS. 3rd edition. Sage Publications

Armour, J., & Cumming, D.J. (2008). Bankruptcy law and entrepreneurship. American Law and Economics Review 10, 303-350.

Arnaboldi, F., & Claeys, P. (2008). Financial innovation in internet banking: A comparative analysis. Available at SSRN: http://ssrn.com/abstract=109409. Retrieved on 18th August 2011

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.

Ayo, C. K., Adebiyi, A. A., Fatudimu, I.T., & Ekong, O.U. (2008). Framework for e-commerce implementation: Nigeria a case study. Journal of Internet Banking and Commerce, August 2008, 13 (2).

Barnes, S.J. (2003). Enterprise mobility: Concepts and examples. International Journal of Mobile Communications, 1(4), 341-359.

Batiz-Lazo, B., & Woldesenbet, K. (2006). The dynamics of product and process innovation in UK banking. International Journal of Financial Services Management, 1 (4), 400-421.

BCG, Boston Consulting Group. (2009). BCG Innovation 2009 Report

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

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