ADOPTION AND USE OF CYBERSECURITY IN THE FINANCIAL SECTOR IN DEVELOPING COUNTRIES

Case Study:

The Ugandan Financial Sector

(Banks, Micro Finance Institutions and Telecom Companies)

A postgraduate dissertation presented to the Faculty of Postgraduate studies / Science Department in partial fulfilment of the requirements for the award of the degree of

Masters of Science in ICT Management, Policy and Architectural Design

Uganda Martyrs University

Elizabeth Busingye

2014-M142-20019

OCTOBER 2016

DEDICATION

I dedicate this dissertation to my mother (Mrs. Joy Katebara Byaruhanga), father (Mr. Edward Byaruhanga), brother (Emmanuel Byaruhanga), sisters (Jeanne, Joanne, Jacqueline, Esther and Ethel), my best friend Charity Ndagire and friends (Group Three) for all the support and motivation they have given me to complete my masters. I want to thank them for the continuous support and the never give up attitude.

ACKNOWLEDGEMENTS

I am indebted to my supervisor Mr. Rahman Sanya for his support, guidance, comments, and encouragement throughout this research. I also appreciate all the assistance given to me by all the lecturers at the Faculty of Science, who laid the theoretical foundation during my studies in all the courses. Special thanks to Ms. Sheeba Nyakaisiki for the guidance and encouragement through the process of writing this research report.

I am also grateful for the support and assistance extended to me by the management and staff of Letshego Uganda Limited. Specifically, I thank the CEO, Mr. Geoffrey Kitakule for granting me some time to pursue my studies, use the boardroom with my group three members for discussions and be able to attend lectures and fulfil all my class obligations. The support of my work colleagues, Mugabi Allan, Ibrahim Kawooya and Lutaaya Tonny, is highly recognized.

Appreciation also goes to my classmates, group members and now friends for life, Alex Muhumuza, Racheal Mbabazi, Ninsiima Noah, Emmanuel Mugabi, and Jasmine Juliana for their firm beliefs that it was possible to complete the course and as a result they kept me going. I thank all my friends who cheered me on from the beginning especially Charity Ndagire my best friend for never giving up on me and always being there for me even when I thought this day would not reach

Finally I thank my family, my mother, father, sisters and brother for all the support they gave me. You are all truly a blessing and I wouldn't have reached this far had it not been for your determination and continuous push to have me achieve all my dreams.

Table of Contents

ACRONYMS

CISO – Chief Information Security Officer

NIST- National Institute of Standards and Technology

COSO - Committee of Sponsoring Organizations of the Treadway Commission

COBIT -Control Objectives for Information and Related Technologies

USB – Universal Serial Bus

ICT – Information Communications Technology

ATM – Automated Teller Machine

PASS 555 -

PCI - Peripheral Component Interconnect Express

ISO - International Organization for Standardization

ESG Cybersecurity Maturity Model – Enterprise Strategy Group

IAM – Identity and Access Management

List of Tables

List of Figures

ABSTRACT

Cybersecurity has increasingly become an area of concern for Financial Institutions. Banks and Micro finance institutions, have critical infrastructure, and are under attack by malicious intruders and players on a daily basis through various forms like deployment of malicious software, insider threat, and hack attempts all for financial gain with in the financial sector. Numerous pieces of legislation and policies on Cybersecurity have been proposed, ranging from piecemeal approaches to comprehensive policy packages. Issues addressed include facilitating cyber threat information sharing; requiring baseline Cybersecurity practices for critical financial infrastructure; creating a regulated standard for data breach notification; investing in Cybersecurity research and development, education, and workforce training; and updating cyber-crime statutes. Cybersecurity policy making should seek solutions that leverage the expertise of the Financial Sector and should be result-oriented and technology-neutral thus promoting the adoption and use of Cybersecurity within the Financial Sector.

CHAPTER ONE:

GENERAL INTRODUCTION

1.0 Introduction

Cybersecurity is a very broad term that can be broken down to a number of concepts, depending on the type of the system that has to be secured. In the Information and Communications Technology (ICT) realm, five quality attributes compose a system's security and these are Confidentiality, Integrity, Availability, Access control, Non-repudiation (*Lehtinen, Rick et al 2006*). As such the researcher looked at the best possible ways to secure ICTs for instance in the financial sector through the enhancement of Cybersecurity. This was achieved by looking at what ICTs are used within the financial sector, why the assets needed to be secured. This was achieved by looking at the impact of their compromise on the business.

Cybersecurity is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide (International Telecommunication Union, 2015, Hitesh Goel, 2015). It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures (Dr. Joe Chan, 2015). In that with one's ability to promote and adopt Cybersecurity comes the reliability of information assurance which is a practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. Information assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data. It uses physical, technical and administrative controls to accomplish these tasks. While focused predominantly on information in digital form, the full range of Information Assurance encompasses not only digital but also analogue or physical form. These protections apply to data in transit, both physical and electronic forms as well as data at rest in various types of physical and electronic storage facilities. Information assurance as a field has grown from the practice of information security and this can be seen from industry to industry including the financial sector.

The banking and financial services sector is one of the most advanced in terms of adoption, use and diffusion of technologies (Ali Alawneh, 2011). Essentially as information business, they do

not produce physical products and have been trading electronically for decades. They are ideally suited to E-business which, in fact, is progressing very quickly. ICT impacts on all aspects of the activity and is undoubtedly one of the main driving forces in the sector.

In the past decades, technological advances have already allowed increasing internal efficiency; more recently they have also increasingly influenced delivery methods. Presently, investments are progressively shifting from the management of operational needs (such as year 2000, Euro conversion) to the improvement of core internal processes, customer management and marketing. The increasing sensitivity towards more efficiency in core processes is forced by the decreasing profit margins and the turbulence of capital markets.

Billions of financial data transactions occur online every day of the year twenty-four hours a day seven days a week and as a result financial institutions are prone to very many cyber-attacks thus resulting into financial information of clients being compromised. There is an increase in the number of cybercrimes and attacks towards financial institutions and this is mainly through various attacks to the systems of the financial institutions both internally and externally (Paul Jeffery Marshall, 2010). This can be through the wide spread of malicious bank Trojan viruses, malware and software that allow remote access to the systems within the banks hence corrupting data and impending the quality of the services and the ICTs within the organisation.

1.1 Background of Study

According to the law dictionary (TheFreeDictionary.com, 2016), Cyber-crime and fraud is defined as the unauthorized use of credit and financial information for criminal activities. Such criminal behaviour has shown improvement in attack vector sophistication in bypassing tradition information security controls with a similar trend in increased usage of insider assistance. The introduction of various ICT customer channels like mobile and the web have increased financial institutions' risk exposure to cyber-crime with financial gain as the motivational factor (Banks likely to remain top cybercrime targets, 2012). Cyber – crime and fraud in financial institutions has become an increasing epidemic within the world and as a result it has been designed to go a step further into intrusion of personal and private information. In that there is a growing increase in cybercrime attacks not only in the western world but also within Africa (Pierluigi Paganini, 2015). With the increase and adoption of electronic banking and ICTs in the financial

institutions, there has been an increase in attacks towards these institutions, this has resulted into personal client data leaking and loss of income for the financial institutions as well as their customers.

In The East African article on, "worries over new avenues of cybercrime" in 2014, Kenya's Cabinet Secretary for Information Fred Matiang'i reported that Kenya as a country lost nearly "Ksh2 billion ($22.56 million) to cyber-crime, with close to 1,000 Kenyans falling victim to Internet fraud on a daily basis. Uganda's 2012-2013 annual Police Crime and Traffic Report as well showed that the country recorded a 149 per cent increase in economic crimes, with mobile money and automated teller machine (ATM) fraud blamed for the loss of about Ush1.5 billion ($575,373 million). Tanzania lost about Tsh1.3 billion ($782,419) last year, according to statistics from the Bank of Tanzania".

1.2 Statement of the Problem

There is an increasing adoption and use of ICTs within the financial sector in Uganda to the extent that they have become a critical component of daily business operations of banks and other financial service providers.

Financial sector players world over, especially banks are some of the institutions well known for being most risk averse and hence, adopting and using the most advanced security controls and measures

It is however, not known to what extent financial sector players in Uganda are adopting and using Cybersecurity to address challenges like cybercrime and threats that occur within the financial sector on a daily basis.

In order to achieve information assurance for their stability, there is need to mainstream the area of information security as a core function, elevating the role as well as developing a culture of Cybersecurity from Governance all the way down to ICT use and implementations which is currently missing or lacking in the financial sector.

1.3 Objectives of the Study

1.3.1 General Objective

The main research objective is to assess the extent of Cybersecurity governance in the financial sector in Uganda looking at the adoption and use of cybersecurity within the financial sector.

1.3.2 Specific Objectives

1. To identify common forms of cybercrime affecting the financial sector.
2. To determine the ways in which financial sector players are managing Cybersecurity risks.
3. To assess the extent of Cybersecurity (non-) governance in the financial sector.
4. To recommend improvements, for managing Cybersecurity risks in the financial sector.

1.4 Research Question or Hypothesis

1. To what extent do ICTs support the financial sector?
2. How have banks and microfinance institutions moved towards securing use of ICTs and mitigating risks?
3. At which level is Cybersecurity management placed with the Governance structure of financial institutions?
4. What gaps exist in the Cybersecurity management of financial institutions in regards to ICTs?
5. What measures can be set in place to improve the Cybersecurity management within in financial institutions?
6. Which Cybersecurity frameworks are used in the Financial Institutions in developing countries?

1.5 Scope of the Study

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets (von Solms and van Niekerk, 2013). Increase in criminal activities through computer network has led to the focus of attention towards protecting sensitive business and personal information, as well as safeguard national security (Philip Zimmerman, 2016). Subsequently, the scope of the study is to propose viable avenues of improving and mainstreaming of Cybersecurity

management within the Ugandan financial sector. This research will study multiple case studies focusing on selected financial institutions within Kampala – Uganda.

1.6 Significance of Study

This study is significant in two ways. First, although Cybersecurity is carried out within the financial sector in Uganda, there is some laggardness to fully adopting it within the various levels of the organisations thus resulting into services being compromised. There is also lack of sufficient research on factors affecting adoption and use of Cybersecurity in Uganda especially in the financial sector, in that most research done so far looks at specific units within Cybersecurity for instance adoption of online banking, adoption of mobile banking. Investigating the adoption and use of Cybersecurity within the financial sector overall may enable banks to increase their market share by creating solutions and strategies that attract consumers to use and adopt various types of technological services without having to worry about information security if all the proper steps in the proposed research framework are followed and fully utilized. Therefore, there is a need for a study of this kind.

Secondly, the study shall contribute to the extremely scanty literature on Cybersecurity mainly focusing on the current state of cyber-crimes and fraud in the financial sector within Uganda, especially since most of the empirical and research studies have largely been conducted in developed countries, while few studies have been conducted on this issue in developing countries, and hardly any has been conducted in Uganda.

1.7 Justification of the Study

The purpose for this study is to propose viable solutions and enlighten the financial sector that as much as there is a great deal of security and various monitoring tools that ensure Cybersecurity within the financial sector, there are still very many breaches and attacks coming in on a daily basis that need the financial sector to improve on the level of adoption and use of Cybersecurity so as to improve on the information assurance.

1.8 Limitations of the Study

The main concern of this study is the difficulty in acquiring the required information from the sampled Ugandan Financial Sector (Banks and Micro Finance Institutions) because of the policies and regulations set by the Institutions on information sharing. Determining how to maximize participation was an important consideration in this study. Participation was maximized by emphasizing confidentiality and anonymity of the informants.

1.9 Definition of Key Terms

The concepts that are central to this study are defined as follows:

Adoption:

The phase of exploration, research, deliberation and decision-making to introduce a new system into the organization. (Andriessen, 1989)

Use:

The term USE in ICT is the application of ICTs within the daily activities by members of an organization

Cybersecurity:

Cybersecurity can simply be defined as security measures being applied to information technology to provide a desired level of protection.

Information Assurance:

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (Source: SP 800-59; CNSSI-4009).

Cyber- Crime:

Cybercrime is criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet (Techterms.com, 2016).

Cyber-fraud:

This refers to any type of deliberate deception for unfair or unlawful gain that occurs online or offline. The most common form is online credit card theft (Netlingo.com, 2016).

Confidentiality:

This refers to the information that data should only be viewable by authorized parties.

Integrity:

This is the principle that only authorized users are allowed to change data, and that these changes will be reflected uniformly across all aspects of the data.

Availability:

This refers to the principle that data and computer resources will always be available to authorized users.

Access Control:

This is the selective restriction of access to a place or other resource. The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization.

Non-repudiation:

A service that provides proof of the integrity and origin of data. An authentication that can be asserted to be genuine with high assurance.

Authenticity:

Authenticity is assurance that a message, transaction, or other exchange of information is from the source it claims to be from. Authenticity involves proof of identity.

CONCLUSION

The adoption and use of Cybersecurity in the financial sector is a critical element in that there are various measures that have been set up to secure the systems used within the financial sector however there is challenge of fully adopting and using the cybersecurity frameworks, policies and measures put in place. In chapter two the researcher look at the various ways the financial sector has been affected as a result of the minimal adoption and use of cybersecurity within the financial sector, this is broken down into the Global, African and East African context.

CHAPTER TWO:

LITERATURE REVIEW

2.0 INTRODUCTION

Computers are getting more sophisticated in that; they have given banks a potential they could only dream about and given bank customers' high expectations, the changes that new technologies have brought to banking industry are enormous in their impact on officers, employees, and customers of banks. Advances in technology are allowing for delivery of banking products and services more conveniently and effectively than ever before, thus creating new bases of competition. Rapid access to critical information and the ability to act quickly and effectively will distinguish the successful banks of the future. The bank gains a vital competitive advantage by having a direct marketing and accountable customer service environment and new, streamlined business processes. Consistent management and decision support systems provide the bank that competitive edge to forge ahead in the banking marketplace.

With the increase in technology also comes some liabilities in terms of cybercrime and fraud and as a result, we are looking at the current risks seeing as most of the existing academic and policy related literature on Cybersecurity in regards to cybercrime starts out by underlining the rise of the Information Age and thus the centrality of information and communication technologies in nearly all sectors of society from government, to business and even to the individual level. Of course information has always been important but now in post-industrial society information is more paramount, pervasive, accessible and vulnerable than ever before.

Looking at some of the biggest vulnerabilities in the financial sector the researcher considered some of the greatest cybercrimes and fraud attacks noticeably within the world, African continent, East African region and Uganda in details in this chapter focusing on the types of cybercrimes within the financial sector and vulnerabilities that have come up with advancement in technology. This chapter covered cybercrime issues like malware vulnerabilities, insider threat, external threat, physical threat, and denial of services, among others.

During the course of reviewing this literature the researcher looked at the various cybercrime types that are affecting the financial sector and relate them to the examples of what is happening both in developing countries and non-developing countries hence providing a look at the major areas that are crucial in the adoption of cybersecurity within the financial sector.

The main cybercrime types with in the financial sector can be categorized and looked at under the following umbrellas;

1. Exploring the global view of Cybersecurity and cyberfraud by analysing the different types of cybercrime that have been faced in the financial sector.
2. Exploring the growing issue of insider threat within the financial sector.
3. Undertaking a synopsis of cybercrime related literature on financial institutions within the African Continent and East African region.

2.1: TYPES OF CYBERSECURITY RISKS WITHIN THE FINANCIAL SECTOR: -

2.1.1 MALWARE

Malware is the short form for malicious software which is a computer program designed to infiltrate and damage computers without the users' knowledge. Malware can be spread through networks by just infiltrating one computer on a network, thus resulting into the wide spread of the malicious software from just one laptop or desktop to all the computers on that specific network hence resulting into damaging of the company's information and illegal access of the information from the company. Malware can be spread through inserting an infected stick (flash disk) into a Universal Serial Bus port of a laptop or desktop and as a result the malware corrupts the company's information by linking itself into the network and attacking any device on the network. Examples of Malware are Ransom ware, Stuxnet, and Carbanak.

One of the biggest malware heists was the Carbanak heist where 30 nations had their financial Institutions hacked and a form of malware known as Carbanak was spread through the network infecting everything that was on the bank network system (Owen Davis and Avaneesh Pandey, 2015). This malware was able to view and track everything that was happening within the banks from the monetary transfers to the movements that were made by the various bank staffs in the

30 institutions. This gave them leeway to be able to impersonate the staff and as a result dispense money at free will and steal millions of dollars from the Financial Institutions (Perlroth, 2015).

2.1.2 HACKING

Hacking is a type of crime where by a person's computer or digital access is broken into and his personal information is illegally accessed. Hacking can also be defined as exposing of personal information such as email addresses, phone number, and account details of a client or person without their knowledge. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. They extort money from corporate giants threatening them to publish the stolen information which is critical in nature.

Hackers can be categorized into various types and these are;

1. Black Hats; these are individuals with extra-ordinary computing skills, resorting to malicious destructive activities and are also known as crackers.
2. White Hats; these are individuals professing hacker skills and using them for defensive purposes and are also known as security analysts.
3. Gray Hats; they are hackers who work both offensively and defensively at various times.
4. Suicide Hackers are hackers who aim to bring down critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment.
5. Script Kiddies; they are unskilled hackers who compromise systems by running scripts, tools, and software developed by real hackers.
6. Cyber Terrorists are individuals with a wide range of skills, motivated by religious or political beliefs to create fear by large-scale disruption of computer networks.
7. State sponsored hackers are individuals employed by the government to penetrate and gain top-secrete information as well as damage information systems of other governments.
8. Hacktivists are people who promote a political agenda by hacking, especially by defacing or disabling websites. One example of hacktivists is the hacking group Anonymous, in

that they are known for hacking for a cause so as to show the corruption with in various governments in various countries.

2.1.3 COMPUTER FRAUD

Computer Fraud is the Intentional deception for personal gain via the use of computer systems.

2.1.4 IDENTITY THEFT

This is the process of stealing someone's personal information and impersonating them either for financial gain or other malicious reasons.

2.1.5 ELECTRONIC FUND TRANSFER

This entails gaining un-authorised access to bank computer networks and making illegal fund transfers. Electronic funds transfer systems have begun to proliferate, and so has the risk that such transactions may be intercepted and diverted. Valid credit card numbers can be intercepted electronically, as well as physically; the digital information stored on a card can be counterfeited.

Of course, we don't need Willie Sutton to remind us that banks are where they keep the money. In 1994, a Russian hacker Vladimir Levin, operating from St Petersburg, accessed the computers of Citibank's central wire transfer department, and transferred funds from large corporate accounts to other accounts which had been opened by his accomplices in The United States, the Netherlands, Finland, Germany, and Israel. Officials from one of the corporate victims, located in Argentina, notified the bank, and the suspect accounts, located in San Francisco, were frozen. The accomplice was arrested. Another accomplice was caught attempting to withdraw funds from an account in Rotterdam. Although Russian law precluded Levin's extradition, he was arrested during a visit to the United States and subsequently imprisoned. (Denning 1999, 55).

The above forms of computer-related crime are not necessarily mutually exclusive, and need not occur in isolation. Just as an armed robber might steal an automobile to facilitate a quick getaway, so too can one steal telecommunications services and use them for purposes of vandalism, fraud, or in furtherance of a criminal conspiracy.1 Computer-related crime may be compound in nature, combining two or more of the generic forms outlined above.

2.1.6 ELECTRONIC MONEY LAUNDERING

This is the process of using technology, computers to launder illegal money. For some time now, electronic funds transfers have assisted in concealing and in moving the proceeds of crime. Emerging technologies will greatly assist in concealing the origin of ill-gotten gains. Legitimately derived income may also be more easily concealed from taxation authorities. Large financial institutions will no longer be the only ones with the ability to achieve electronic funds transfers transiting numerous jurisdictions at the speed of light. The development of informal banking institutions and parallel banking systems may permit central bank supervision to be bypassed, but can also facilitate the evasion of cash transaction reporting requirements in those nations which have them. Traditional underground banks, which have flourished in Asian countries for centuries, will enjoy even greater capacity through the use of telecommunications.

With the emergence and proliferation of various technologies of electronic commerce, one can easily envisage how traditional countermeasures against money laundering and tax evasion may soon be of limited value. I may soon be able to sell you a quantity of heroin, in return for an untraceable transfer of stored value to my "smart-card", which I then download anonymously to my account in a financial institution situated in an overseas jurisdiction which protects the privacy of banking clients. I can discreetly draw upon these funds as and when I may require, downloading them back to my stored value card (Wahlert 1996).

2.1.7 ATM FRAUD

This is the process whereby ATM details are intercepted by criminals for example the account number details, pin numbers thus resulting into the criminals illegally accessing the information and withdrawing someone’s money without their knowledge.

2.1.8 DENIAL OF SERVICE ATTACKS

Denial of service attacks is also known as Distributed denial of service attacks, and these involve the use of computers in multiple locations to attack servers with a view of shutting them down, thus rendering the systems within the organisation useless.

2.1.9 SPAM

Spam is the process of sending un-authorised emails. These emails usually are made up of online advertisements.

2.1.10 INSIDER THREAT

Thwarting Insider Threat for Financial Institutions whitepaper looks at the past 10 years, and the primary concern for financial institutions being the securing of the perimeter of their network from attack by anonymous hackers. They look at the biggest threat being the internal threat in Today's financial institutions that being the human interface. Today, financial institution employees have multiple sets of identities contained within different directories and applications (Identity and Access Management Solution, 2005). Access policies for these identities are managed within silos of authentication and access systems that don't communicate with each other. These systems also have related silos of audit and reporting which means that employee activities are not easily tracked and monitored, providing an environment ripe for misuse or access of critical information assets. (Carnegie Mellon University, 2015).

Insiders according to Hamin (2000), are in an advantageous position to misuse organizational Information systems, due to their familiarity with the system structures and potential weak spots in security administration. "The insider threat identifies a serious threat to Cybersecurity and computer security. It describes a breach of trust by people within an organization or system, as contrasted to external entities for whom firewalls and other mechanisms can deny access" (Bishop, Engle, Peisert, Whalen, & Gates, 2000). A security incident perpetrated by an insider can impact an organization in various ways. Potential results of insider threat incidents could be negative impact on the public image of an organization, negative impact on the revenue of an organization or litigation due to disclosure of confidential information (Colwill, 2009), (Ophoff, J., Jensen, A., Sanderson-Smith, J., Porter, M., & Johnston, K 2014).

2.2 THEORETICAL FRAMEWORK

2.2.1 THE ADOPTION AND USE OF CYBERSECURITY IN FINANCIAL INSTITUTION.

2.2.2 Social Psychology

The raw power of ICTs continues to improve, making sophisticated applications economically feasible. As technical barriers disappear, a pivotal factor in harnessing this expanding power becomes the ability to create applications that people are willing to use. Therefore resulting into the need for us as researchers to better understand why there is poor or limited adoption to Cyber security within the financial sector.

This results into the ability to carry out certain evaluations and analysis to see how the community (Financial community) responds to changes in the adoption of cyber security and look at how best the implementations are done.

There have been some models that have been discussed and suggested which would act as theoretical foundations for research on the determinants of user behaviour in ICT (Swanson, 1982).

2.2.3 Theory of reasoned Action (TRA)

The theory of Reasoned Action is a widely studied model from Social Psychology, which is concerned with the determinants of consciously intended behaviours (Ajzen and Fishbein, 1980; Fishbein and Ajzen, 1975). It is composed of attitudinal, social influence, and intention variables to predict behaviour. Figure 1-1 is a schematic representation of the relationships among constructs in TRA. It is hypothesized by TRA that the individual's behavioural intention (BI) to perform a behaviour is jointly determined by the individual's attitude toward performing the Behaviour (ATB) and subjective norm (SN), which is the overall perception of what relevant others think the individual should do or not do. The importance of ATB and SN to predict BI will vary by behavioural

domain. For behaviours which attitudinal or personal-based influence is stronger (e.g. purchasing something for personal consumption or use in relation to ICTs and Cyber security implementation), ATB will be the dominant predictor of the BI, and SN will be of little or no predictive efficacy. While for behaviours in which normative implications are strong (e.g. purchasing the ICTs that will be used by the financial organisations). SN should be the dominant predictor of BI and ATB will be of lesser importance (Ajzen and Fishbein, 1980).

The theory of Reasoned Action also hypothesizes that BI is the only direct antecedent of actual behaviour (AB). BI is expected to predict AB accurately if the three boundary conditions specified by Fishbein and Ajzen (1975) can be held: (a) the degree to which the measure of intention and the behavioural criterion correspond with respect to their levels of specificity of action, target, context and time frame; (b) the stability of intentions between time of measurement and performance of the behaviour; and (c) the degree to which carrying out the intention is under the volitional control of the individual (i.e., the individual can decide at will to perform or not to perform the behaviour).

TRA is a general model that doesn't specify the beliefs that are operative for a particular behaviour. Researchers using TRA must first identify the beliefs that are salient for subjects regarding the behaviour under investigation.

Fishbein and Ajzen (1975) and Ajzen and Fishbein (1980), suggest eliciting five to nine salient beliefs using free response interviews with various staff of financial institutions. Fishbein and Ajzen recommend using "modal" salient beliefs for the population, obtained by taking the beliefs most frequently elicited from a representative sample of the group.

The TRA has been successfully applied to large numbers of situations to predict the performance of behaviour and intentions. For example, TRA predicted turnover (Prestholdt et al., 1987); education (Fredricks and Dossett, 1983); and breast cancer examination (Timko, 1987). In a meta-analysis of research on Theory of Reasoned Action, Sheppard et al. (1988) concluded that the predictive Utility of the TRA was strong across conditions.

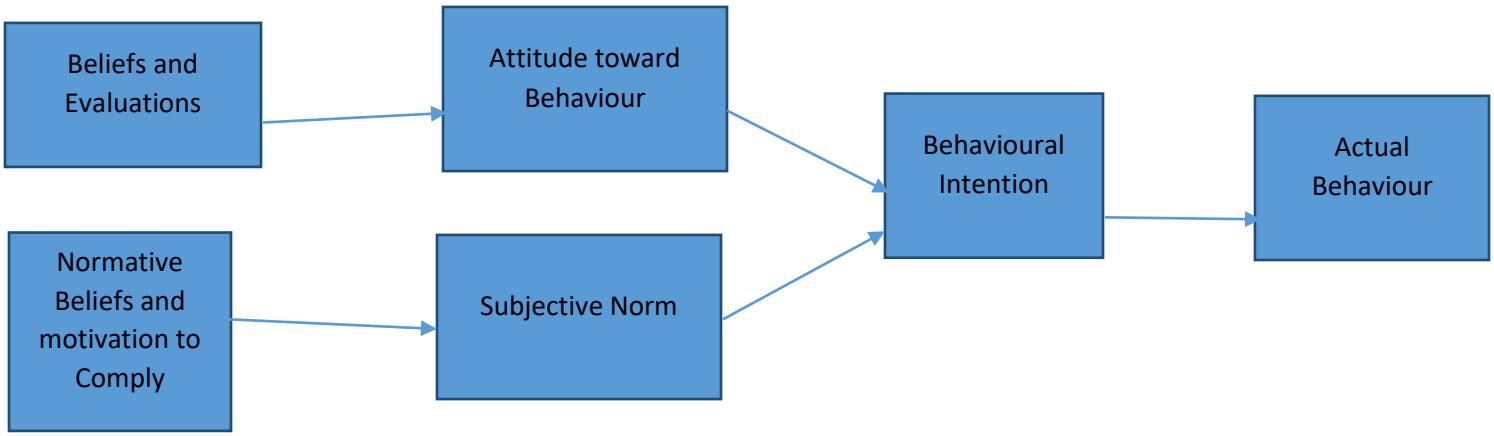


Figure 1.1 Theory of Reasoned Action. Source: Fishbein and Ajzen, 1975

2.2.4 Theory of Planned Behavior (TPB)

Despite the predictability of the TRA is strong across studies, it becomes problematic if the behaviour under study is not under full volitional control.

Sheppard et al. (1988) pointed out two problems of the theory. First, one must differentiate the difference between behaviours from intention. This could be problematic because a variety of factors in addition to one's intentions determine how the behaviour is performed. Second, there is no provision in the model for considering whether the probability of failing to perform is due to one's behaviour or due to one's intentions. To deal with these problems, Ajzen (1985) extended the Theory of Reasoned Action by including another construct called perceived behavioural control, which predicts behavior intentions and behavior. The extended model is called the Theory of Planned Behavior (TPB).

As figure 1.2 shows, TRA and TPB have many similarities. In both models, BI is a key factor in the prediction of actual behavior. Both theories assume that human beings are basically rational and make systematic use of information available to them when making decisions. By considering control- related factors, TRA assumes that the behavior being studied is under total volitional control of the performer (Madden et al., 1992). However, TPB expands the boundary conditions of TRA to more goal- directed actions.

Attitude toward Behavior (ATB) is defined as "a person's general feeling of favourableness or unfavourableness for that behavior" (Ajzen and Fishbein, 1980).

Subjective Norm (SN) is defined as a person's "perception that most people who are important to him/her think he/she should or should not perform the behavior in question" (Ajzen and Fishbein, 1980). Attitude toward behavior is a function of the product of one's salient beliefs that performing the behavior will lead to certain outcomes, and an evaluation of the outcomes, i.e., rating of the desirability of the outcome.

The main difference between these two theories is that the TPB has added Perceived Behavioral Control (PBC) as the determinant of Behavioral Intention, as well as control beliefs that affect the perceived behavioral control. Though it may be difficult to assess actual control before behavior, TPB asserts that it is possible to measure PBC "people's perception of the ease of difficulty in performing the behavior of interest" (Ajzen, 1991). PBC is a function of control beliefs and perceived facilitation. Control belief is the perception of the presence or absence of requisite resources and opportunities needed to carry out the behavior. Perceived facilitation is one's assessment of the importance of those resources to the achievement of the outcome (Ajzen and Madden, 1986).

PBC is included as an exogenous variable that has both a direct effect on actual behavior and an indirect effect on actual behavior through intentions. The indirect effect is based on the assumption that PBC has motivational implications for behavioral intentions. When people believe that they have little control over performing the behavior because of lack of requisite resources and opportunities, then their intentions to perform the behavior maybe low even if they have favourable attitudes and /or subjective norms concerning performance of the behavior. Bandura (1977) has provided empirical evidence that people's behavior is strongly influenced by the confidence they have in their ability to perform the behavior. The structural link from PBC to BI reflects the motivational influence of control on actual behavior through intentions.

The direct path from PBC to AB is assumed to reflect the actual control an individual has over performing the behavior. Ajzen (1985) offers the following rationale for this direct path. First, if intention is held constant, the effort needed to perform the behavior is likely to increase with PBC. For example, if two people have equally strong intentions to learn to drive a car, and both try to do so, the confident person who believes that it would take them a shorter timeframe to master this task would be the one to drive the car faster than the one who has doubts. In addition PBC often serves as a substitute for actual control, and insofar as perceived control is realistic estimate of actual control, PBC should help to predict AB.

As with TRA, the relative importance of BI predictors varies with the behavioral domain. In some applications, it may be found that only ATB has a significant impact on BI; in others, ATB and PBC will be significant; in still others, ATB, SN and PBC will contribute to the prediction of BI (Ajzen, 1985). Similarly, the ability of PBC and BI to predict AB also will vary across behaviours and situations. Both BI and PBC can make significant contributions to the prediction of goal-directed actions. In any given application, however, one predictor may be more important than the other, and only one of the two may be significant.

The theory pf Planned Behavior has been successfully applied to various situations in predicting the performance of behavior and intention, such as predicting user intentions to use new software (Mathieson, 1991), to perform unethical behaviour (Man,1998).

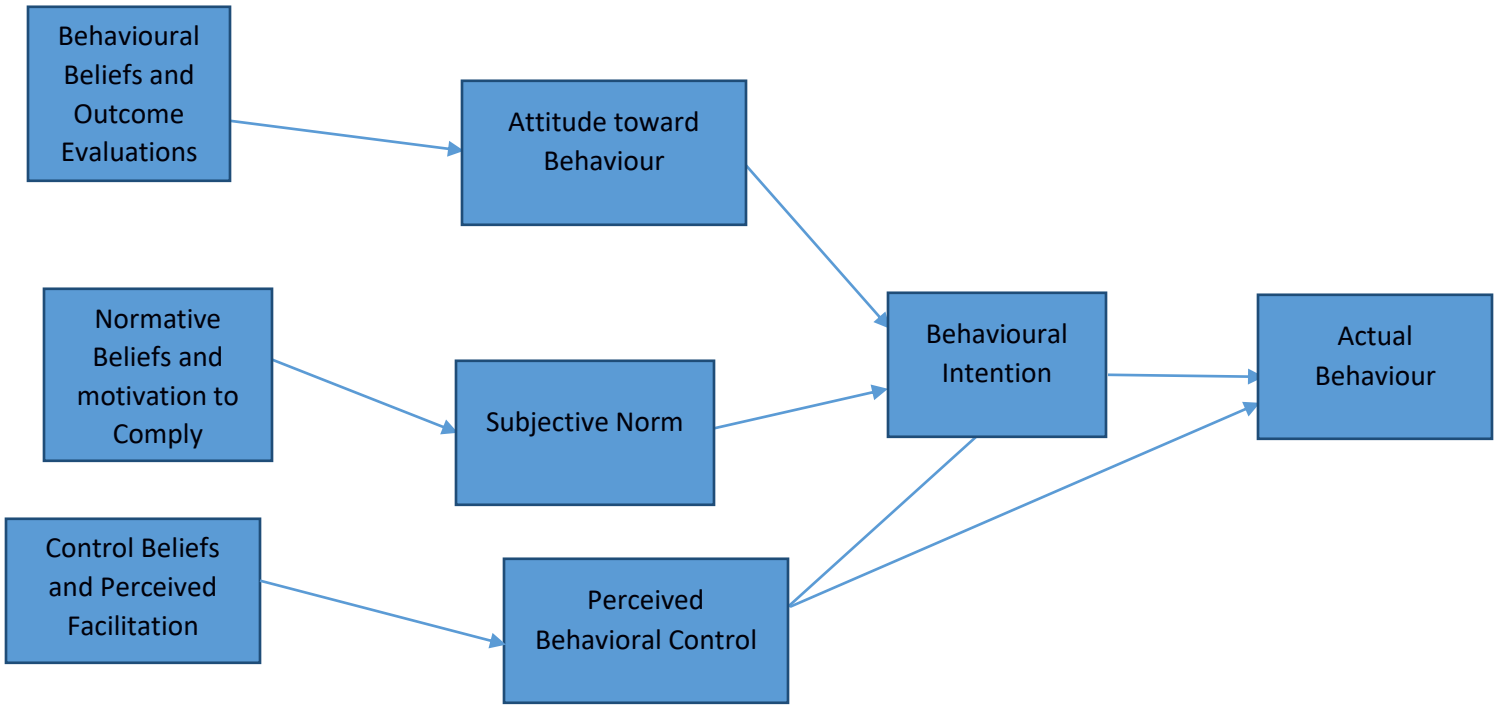


Figure 1.2 Theory of Planned Behavior. Source: Adopted from Pavlou, 2001

2.2.5 Decomposed of Theory of Planned Behavior

Taylor and Todd (1995) indicated that a better understanding of the relationships between the belief structures and antecedents of intention requires the decomposition of attitudinal beliefs. Shimp and Kavas (1984) argued that the cognitive components of belief could not be organised into a single conceptual or cognitive unit. Taylor and Todd (1995) also specified that, based on the diffusion of innovation theory, the attitudinal Use belief has three salient characteristics of an innovation that influence adoption, are relative advantage, complexity and compatibility (Rogers, 1983). Taylor and Todd (1995) showed that the decomposed model of the TPB has better explanatory power than the pure TPB and TRA models. So, the argument of our empirical study is that Cyber security is a technological innovation and thus the decomposed TPB model gives a more satisfactory explanation of adoption intention.

Related advantage refers to the degree to which an innovation provides benefits which supersede those of its precursor and may incorporate factors such as economic benefits, image, enhancement, convenience and satisfaction (Rogers, 1983).

Relative advantages should be positively related to an innovation's rate of adoption (Rogers, 1983; Tan and Teo, 2000).

2.2.6 Technology Acceptance Model (TAM)

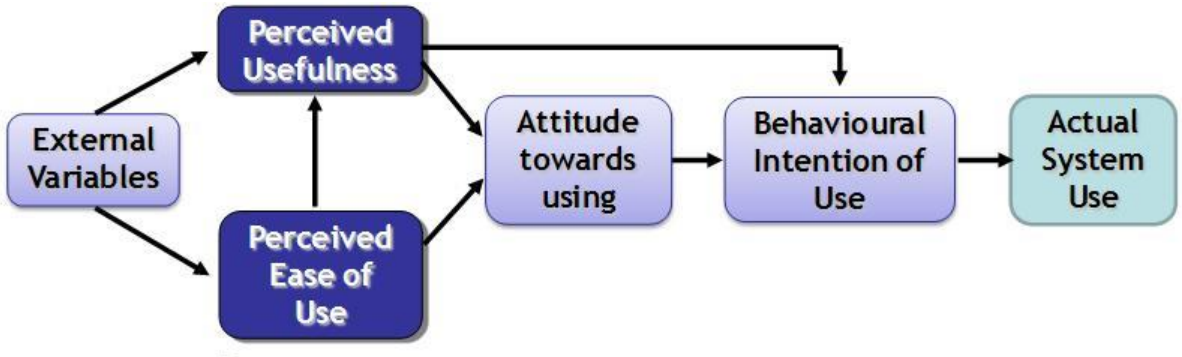
Technology Acceptance Model (TAM), introduced by Davis (1989), is an adaptation of the Theory of Reasoned Action (TRA) specifically tailored for modelling user acceptance of information systems. The goal of TAM is to provide an explanation of the determinants of computer acceptance that is general, capable of explaining user behavior across a broad range of end-user computing technologies and user populations, while at the same time being both parsimonious and theoretically justified. Ideally one would like a model that is helpful not only for prediction but also for explanation, so that researchers and practitioners can identify why a particular system may be unacceptable, and pursue appropriate corrective steps. A key purpose of TAM, therefore, is to provide a basis for tracing the impact of external factors on internal beliefs, attitudes, and intentions. TAM was formulated in an attempt to achieve these goals by identifying a small number of fundamental variables suggested by previous research dealing with

the cognitive and affective determinants of computer acceptance, and using TRA as a theoretical backdrop for modelling the theoretical relationships among these variables.

As Figure 1-3 shows, TAM posits that two particular beliefs, perceived usefulness (PU) and perceived ease of use (PEOU), are the primary relevance for computer acceptance behavior. PU is defined as the degree to which a prospective user believes that using a particular system would enhance his or her job performance. This follows from the definition of the word "useful": "capable of being used advantageously". Within an organizational context, people are generally reinforced for good performance by raises, promotions, bonuses, and other rewards (Pfeffer, 1982; Vroom, 1964). A system high in perceived usefulness, in turn, is one for which a user believes in the existence of a positive use-performance relationship.

PEOU refers to the degree to which a prospective user believes that using a particular system would be free of effort. This follows from the definition of "ease": "freedom from difficulty or great effort". Effort is a finite resource that a person may allocate to the various activities for which he or she is responsible. All else being equal, an application perceived to be easier to use than another is more likely to be accepted by users. In January 2000, the Institute for Scientific Information's Social Science Citation Index® listed 424 journal citations of the two journal articles that introduced TAM (i.e., Davis 1989, Davis et al. 1989). In the past decade, TAM has become well established as a robust, powerful, and parsimonious model for predicting user acceptance.

Figure 1-3 Technology Acceptance Model. Source: Davis, 1989



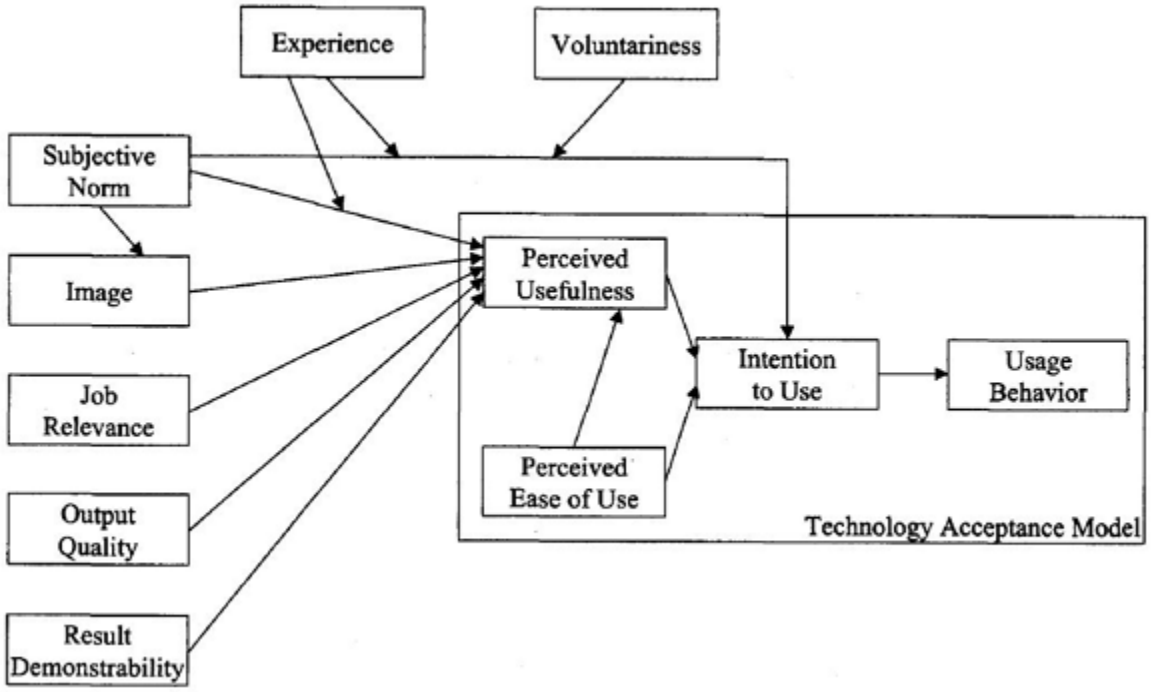
2.2.7 Extension of Technology Acceptance Model (ETAM)

A study of the adoption of telemedicine technology by physician using TAM has found relatively low explanation power of TAM attitude and intention (Hu et al., 1999). The researchers suggested that integration of TAM with other IT acceptance models or incorporating additional factors could help to improve the specificity and explanatory utility in a specific area.

Is researchers have begun to use TAM to examine the possible antecedents of perceived usefulness and perceived Ease of Use toward microcomputer usage (Igbaria, Guimaraes, and Davis, 1995; Igbaria, livari, and Maragahh, 1995). However, one criticism of the current TAM studies is that there are very few investigations target at the study of the factors (i.e., the external variables) that affect the PU and PEOU (Gefen and Keil, 1998). In order to address this issue, Venkatesh and Davis (1996) used three experiments to investigate the determinants of perceived Ease of Use. The results showed that general Computer self – efficacy significantly affects perceived Ease of Use at all time, while Objective Usability of the system affects users' perception after they have direct experience with the system.

Furthermore, Venkatesh and Davis (2000) developed and tested a TAM2 model by including a number of determinants to perceived Usefulness into the new model (see figure 1-4). It is a theoretical extension of the Technology Acceptance Model that explains perceived Usefulness and Usage Intentions in terms of social influence processes (Job Relevance, Output Quality, Result Demonstrability and Perceived Ease of Use).

Figure 1- 4 Technology Acceptance Model (TAM2)



Source: Venkatesh and Davis (2000)

2.2.8 Diffusion of Innovation

Innovation of Diffusion Theory (IDT) is a model that explains the process by which innovations in technology are adopted by users. Rogers defines an innovation as “an idea, practice, or object that is perceived as new by an individual or other unit of adoption” (Rogers, 1995). Diffusion is defined as “the process by which an innovation is communicated through certain channels over time among the members of a social system.” So, it follows that Innovation Diffusion theory focuses on explaining how new ideas and concepts gain widespread adoption.

Innovation Diffusion Theory considers a set of attributes associated with technological innovations that affect their rate of widespread adoption. Rogers defines these attributes as:

Relative advantage – “The degree to which an innovation is perceived to be better than the idea it supersedes.”

Compatibility – “The degree to which an innovation is perceived as consistent with the existing values, past experiences, and needs of potential adopters.”

Complexity – “The degree to which an innovation is perceived as relatively difficult to understand and use.”

Trialability – “The degree to which an innovation maybe experimented with on a limited basis.”

Observability – “The degree to which the results of an innovation are visible to others.”

Among these attributes, only relative advantage, compatibility and complexity are consistently related to innovation adoption (Chen et al., 2000)

Rogers reviewed nearly 1500 studies where variants of IDT are used to investigate the adoption of technological innovations in an array of settings including agriculture, healthcare, city planning, financial sectors, and economic development. A smaller set of studies focus on, how these attributes influence behavioral intention and use. Rogers developed his IDT constructs by identifying the product attributes that most greatly influenced adoption.

2.3 FRAMEWORKS ASSOCIATED WITH THE ADOPTION AND USE OF CYBERSECURITY IN FINANCIAL INSTITUTION IN DEVELOPING COUNTRIES.

Perks and Beveridge (2003) consider frameworks as "a reasoned, cohesive, adaptable, vendor-independent, domain neutral and scalable conceptual foundation for detailed architecture representation".

On the other hand, as defined in the NIST (2014) A Framework is defined as "a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors".

There are several frameworks for ICT Governance which relates to Cybersecurity. The most widely used frameworks for cybersecurity are: ISO27000 series, COSO, COBIT, NIST, and PCIDSS (Rajendra et al., 2016).

These frameworks have different profiles and methodologies used in each benchmarks in implementing cybersecurity for organisations. Having the aspects of cybersecurity adoption and use in the financial sector in developing countries the researcher discusses the commonly used cybersecurity frameworks or standards in the world.

2.3.1 COSO Framework

The COSO Framework is a framework that was designed by the Committee of Sponsoring Organisations of the Treadway Commission. COSO was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting (the Treadway Commission). The Treadway Commission was originally jointly sponsored and funded by five main professional accounting associations and institutes headquartered in the United States: the American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), Financial Executives International (FEI), Institute of Internal Auditors (IIA) and the Institute of Management Accountants (IMA). The Treadway Commission recommended that the organizations sponsoring the Commission work together to develop integrated guidance on internal control. These five organizations formed what is now called the Committee of Sponsoring Organizations of the Treadway Commission.

The COSO framework defines internal control as a process, effected by an entity's board of directors, management and other personnel, designed to provide "reasonable assurance" regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations.
- Safeguarding of Assets (MHA)

2.3.1.1 Five framework components

The COSO internal control framework consists of five interrelated components derived from the way management runs a business. According to COSO, these components provide an effective framework for describing and analyzing the internal control system implemented in an organization as required by financial regulations.

The five components are the following:

Control environment: The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, management's operating style, delegation of authority systems, as well as the processes for managing and developing people in the organization.

Risk assessment: Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives and thus risk assessment is the identification and analysis of relevant risks to the achievement of assigned objectives. Risk assessment is a prerequisite for determining how the risks should be managed.

Control activities: Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address the risks that may hinder the achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of

activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

Information and communication: Information systems play a key role in internal control systems as they produce reports, including operational, financial and compliance-related information that make it possible to run and control the business. In a broader sense, effective communication must ensure information flows down, across and up the organization. For example, formalized procedures exist for people to report suspected fraud. Effective communication should also be ensured with external parties, such as customers, suppliers, regulators and shareholders about related policy positions.

Monitoring: Internal control systems need to be monitored—a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities or separate evaluations. Internal control deficiencies detected through these monitoring activities should be reported upstream and corrective actions should be taken to ensure continuous improvement of the system.

Table 2.1: COSO framework

Internal Control Component	Principles
Control environment	1. Demonstrate commitment to integrity and ethical values 2. Ensure that board exercises oversight responsibility 3. Establish structures, reporting lines, authorities and responsibilities 4. Demonstrate commitment to a competent workforce 5. Hold people accountable
Risk assessment	6. Specify appropriate objectives 7. Identify and analyze risks 8. Evaluate fraud risks 9. Identify and analyze changes that could significantly affect internal controls
Control activities	10. Select and develop control activities that mitigate risks 11. Select and develop technology controls 12. Deploy control activities through policies and procedures
Information and communication	13. Use relevant, quality information to support the internal control function 14. Communicate internal control information internally

	15. Communicate internal control information externally
Monitoring	16. Perform ongoing or periodic evaluations of internal controls (or a combination of the two) 17. Communicate internal control deficiencies

There are certain limitation as the Framework recognizes that as internal control provide assurance of achieving the organizations objective, but limitations do exist as internal controls do not overcome bad judgments, external events etc. which can cause failure to achieve its operational goals. Organizations can face the failure from multiple factors:

- Breakdown due to human failures.
- Cases in which management override internal control.
- External event beyond the organizations control.
- Mistakes due to human intervention.

2.2.3 National Institute of Standards and Technology Framework

The Framework provides a common language for understanding, managing, and expressing Cybersecurity risk both internally and externally. It can be used to help identify and prioritize actions for reducing Cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage Cybersecurity risk across entire organizations or it can be focused on the delivery of critical services within an organization. Different types of entities including sector coordinating structures, associations, and organizations can use the Framework for different purposes, including the creation of common Profiles(Matousek & Sanford 2013).

The Nist framework concentrates on mitigating risks with in the infrastructure of the organisation all the way from the governance aspect to the hardware aspect of the organisation. The figure below summarises the NIST core framework;

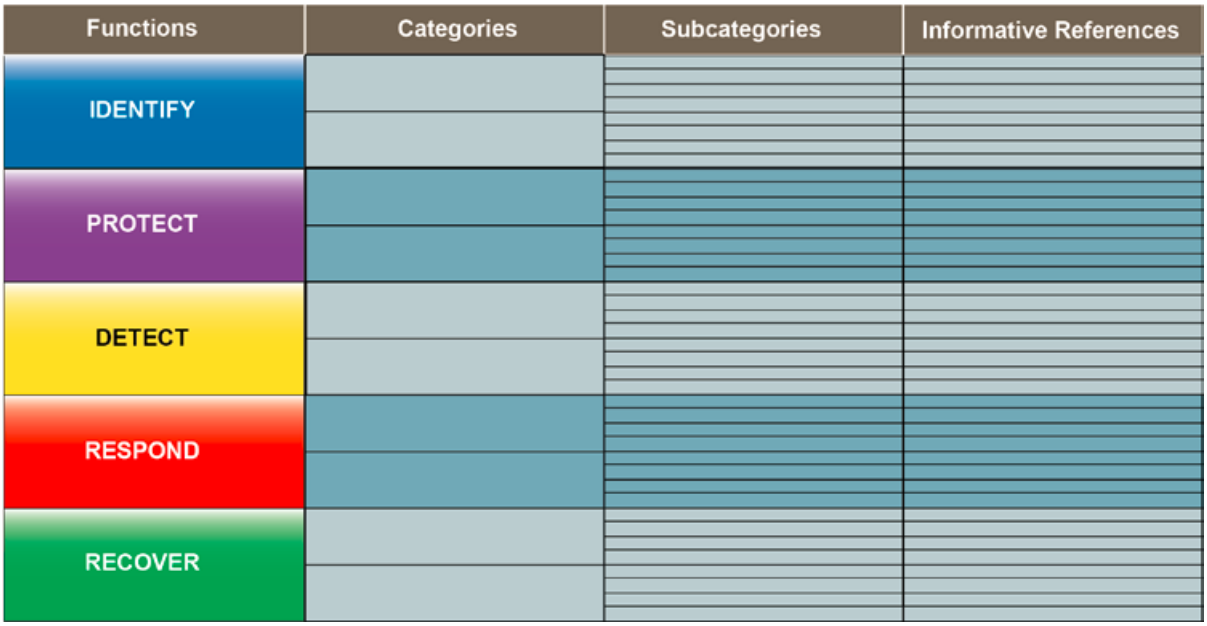


Figure 2-7: The NIST Core Framework

2.2.4 COBIT Framework (IT Governance Framework)

COBIT (Control objective for information and related technology) is a framework for developing, implementing, monitoring and improving Information technology governance and management practices (Rajendra et al., 2016). The COBIT framework was published by ISACA (Information Systems Audit and Control Association) in 1996. The framework supports organization governance by aligning IT goals with business goals. It helps enterprises to drive optimal value from IT by maintaining balance between resources use, benefits and optimizing risk levels. Adoption of COBIT allows organizations to achieve the following goals:

- Alignment of IT with the business goals.
- Increase in the importance of IT to business.
- Risk reduction.
- Continual improvement of IT.
- Development of goals and scorecards for measurement of IT in a structured way.

COBIT describes a method for controlling the risks arising from the use of IT to support business-related processes (BSI-standard 100-1, 2008). From the various standards available, only COBIT fully addresses the entire spectrum of IT governance duties (Jimmy, 2012).

COBIT version 5 is the current version of COBIT and the complete package consists of: The Executive summary, Governance and Control Framework, Control Objectives, Management Guidelines, Implementation Guide and IT Assurance Guide (ISACA, 2016)

2.3.4 PASS 555 Framework

PAS 555 supplies a holistic framework for effective Cybersecurity which not only considers the technical aspects, but also the related physical, cultural and behavioural aspects of an organization's approach to addressing cyber threats, including effective leadership and governance.

Through this approach, **PAS 555** enables organizations to:

- Focus investment in the most appropriate way, minimising potential losses and improving operational effectiveness and efficiency;
- Develop organisational resilience by improving loss prevention and incident management;
- Identify and mitigate Cybersecurity risk throughout the organisation.

PAS 555 applies to the whole organization and its supply chain, avoiding the dangers that can arise when the security measures fail to cover the whole of the business. It is an adaptable approach which can apply to any organization, whatever its size or type, whether commercial, not-for-profit or public sector.

PAS 555's flexibility allows an organization to utilize its own defined processes or the adoption of other standards and management systems to achieve its intended Cybersecurity ends.

PAS 555 can be used alone, but is also compatible with many major security standards, such as ISO20000-1, ISO27001, ISO22301 and ISO31000.

2.2.6 Payment Card Industry- Data Security Standard (PCIDSS)

PCIDSS is a cybersecurity / information security standard for companies and organizations that handle branded credit and debit cards. These include the likes of; Visa, Mastercard, American Express, among others. The PCIDSS standards where developed by the Payment Card Industry Security Council. The standards were developed to increase controls around the cardholder data so as to mitigate the risk of credit / debit card fraud(PCI DSS Compliance, 2016).

The first ever PCIDSS standard was released in 2004, this was as a result of five different programs namely; Visa's Cardholder Information Security Program, MasterCard's Site Data Protection, American Express' Data Security Operating Policy, Discover's Information Security and Compliance, and the JCB's Data Security Program were started by card companies.

There intentions were roughly similar: in that they wanted to create an additional level of protection for card issuers by ensuring that merchants meet minimum levels of security when they stored, processed and transmitted cardholder data.

The Payment Card Industry Security Standards Council (PCI SSC) was then formed and these companies aligned their individual policies to create the PCI DSS framework.

The PCIDSS looks at twelve requirements for compliance, setup in six groups known as control objectives. Each version of the PCIDSS contains all these requirements and has them divided into sub requirements differently. However the twelve high requirements have not changed since the setup of the standard (PCI DSS Quick Reference Guide Understanding the Payment Card Industry Data Security Standard version 2.0, 2010).

Table 2.2: PCIDSS Framework Requirements

Control objectives	**PCI DSS requirements**
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software on all systems commonly affected by malware
	6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security

2.2.7 ISO 27000 Series Framework

International Organization for Standardization (ISO), founded on February 23, 1947, promulgates worldwide proprietary industrial and commercial standards, has headquarters in Geneva, Switzerland (Heru et al., 2011).ISO is "the world's largest developer and publisher of international standards in a wide area of subjects including information security management systems and practices" (Munirul et al., 2011). ISO as international standardization body is issuing standards in many areas including IT and its security management systems. These standards could either be applied by the member countries (which are around 163 out of 203 countries as Heru et al., (2011) explained) as they are or can be customized to national current development situation and requirements. Implementations of these standards help organizations to effectively manage their information systems security.

ISO27001:2005 Standard The international standard of ISO/IEC 27001 is one of the ISO standards which specify the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving documented ISMS within an organization (ISO/IEC 27001-2 & Yigezu, 2011). ISO/IEC 2700-2 (2005) standard is derived from the BS 7799:2, 2002, which is meant for Information Security Management System – Requirements and it covers all type of organization (Yigezu, 2011).

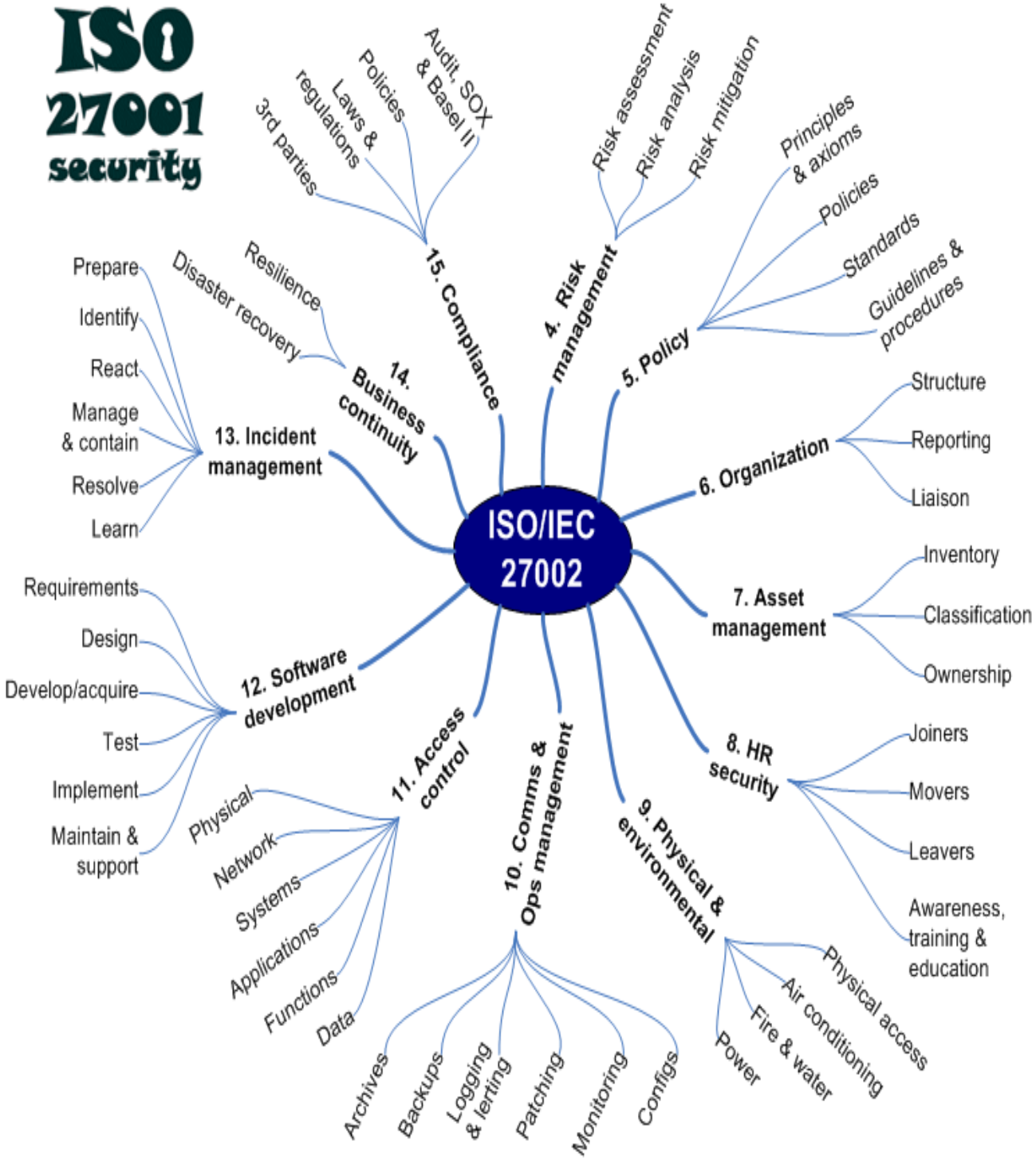
Due to the complexity of information technology and the demand for certifications, numerous manuals, standards and national norms for information security have emerged over the past several years. The ISO/IEC 27001 "Information Technology – Security Techniques – Information Security Management Systems Requirements Specification" is the first 16 international standard for management of information security that also allows certification (BSI-standard 100-1, 2008). As stated in ISO/IEC 27001-2 (2005) and summarized by Yigezu (2011) this standard contains security recommendations for 12 Security domains which include:

1. Security policy - management direction;
2. Organization of information security - governance of information security;
3. Asset management - inventory and classification of information assets;
4. Human resources security - security aspects of employee joining and leaving organization;
5. Physical and environmental security - protection of computer security;

6. Communications and operations management - management of technical security;
7. Access control - restriction of access control to systems, resources and network facilities;
8. Information systems acquisition, development and maintenance - building security into applications;
9. Information security incident management - anticipating and responding to security breaches;
10. Business continuity management - protecting, maintain and recovering business critical systems, processes and assets;
11. Compliance - ensuring compliance with organizational standards, policies, rules and regulations, procedures and norms; and
12. Risk assessment - analysis, planning, controlling and monitoring of implemented solutions and measures.

ISO/IEC 27001:2005 is always implemented together with ISO/IEC 27002:2005 (Yigezu, 2011).

Figure 2.8 Main contents of ISO/IEC 27002: 2005 adopted from (Yigezu, 2011)



2.2.8 Theory and Framework Comparisons

In conclusion after analysing through some of the theories and the various sections that are covered in regards to Cybersecurity the most viable theories to consider are the Technology Acceptance model, Expansion Technology Acceptance Model, and the Diffusion of Innovation Theory. This is because they majorly look at the adoption and use of technology looking at the main three pillars within an organisation that being the strategic, tactical and operational and thus being able to guide users on accepting the business, processes and technology that is used within the financial sector. These theories will work Hand-in hand with a framework designed by the researcher comprising of various elements of the different Cybersecurity frameworks, encompassing the NIST framework, COSO framework, ISO 27001 and 27002 frameworks, COBIT framework and PCI framework which look at the overall state of Cybersecurity providing solutions on how best to improve on the adoption and usage of Cybersecurity measures within the Financial Sector.

CONCLUSION

In conclusion the researcher realises that Cybersecurity threats are an ever growing problem within the financial sector as seen in the literature review above which clearly depicts constant rise in cyber warfare and threats within the world at a geographical level highlighting the major types of cybercrime ranging from External threats, and Internal threats as seen in the literature review above. This can be noted by looking at the trend in developed countries as well as penetrating the developing countries more and more, implying that with an increase in technology advancement, infrastructure and Internet usage the rise of threats also increases.

As the researcher looks at the Methodology needed to ensure proper adoption and use of Cybersecurity to provide information assurance within the financial sector, she looks at the current trends and frameworks that are being used in the financial sector and how best they can be, fully utilized to come up with a probable solution to mitigate the risk factors that are seen in the adoption and use of Cybersecurity with the financial sector so as to promote information assurance.

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

3.0 Introduction

This chapter presents what research design and method was employed to answer the research questions formulated. Review of the research methods: qualitative, quantitative and mixed research methods are made and choice of the research methods and the reasons for that is stated. As a result the researcher mainly concentrates on qualitative research and this is explained further in the research. Questions answered in this part are: What research paradigm is used? How samples for the study are selected and why? What data collection techniques are employed? How data is analysed?

3.1 Research Design

A conceptual Cybersecurity Framework development process has followed the following main research design components and steps which guide the research process. The research design acts as the guidance of the research, in that the student researcher preferred to use the combination of Action Research as well as Design Research. (Kothari &Robert, 2007)

This can be seen in the context where by,

3.1.1 **Main Research Design Components**

The student researcher preferred the following research design methods so as to come to a probable response in terms of respondents input towards the research questions so as to come up with a plausible solution to the impending gaps within the adoption and use of Cybersecurity in the financial sector in developing countries especially in the Ugandan financial sector.

a. ***Literature Review:***

This research starts with a literature review focusing on the objectives of the study, so as to be able to analyse the gaps within the adoption and use of Cybersecurity by studying the current cybercrimes with the financial sector.

b. ***Assessing the current extent of Cybersecurity governance in the financial sector:***

Qualitative methodology was applied to access the current Cybersecurity governance in the financial sector. The backing behind the selection of the mixed methods design is to get a better understanding of the problem identified in the research and come up with viable solutions to mitigate the problem. In addition to the above there was minimal quantitative analysis carried out as a way to justify the emphasis made through the qualitative analysis.

The mixed method would allow for both text and statistical data collection and analysis, and would permit more flexibility when designing questions for survey interviews (Questionnaires and face- to-face interviews), i.e. both open and close-ended questions.

c. ***Using a Cybersecurity capability maturity model:***

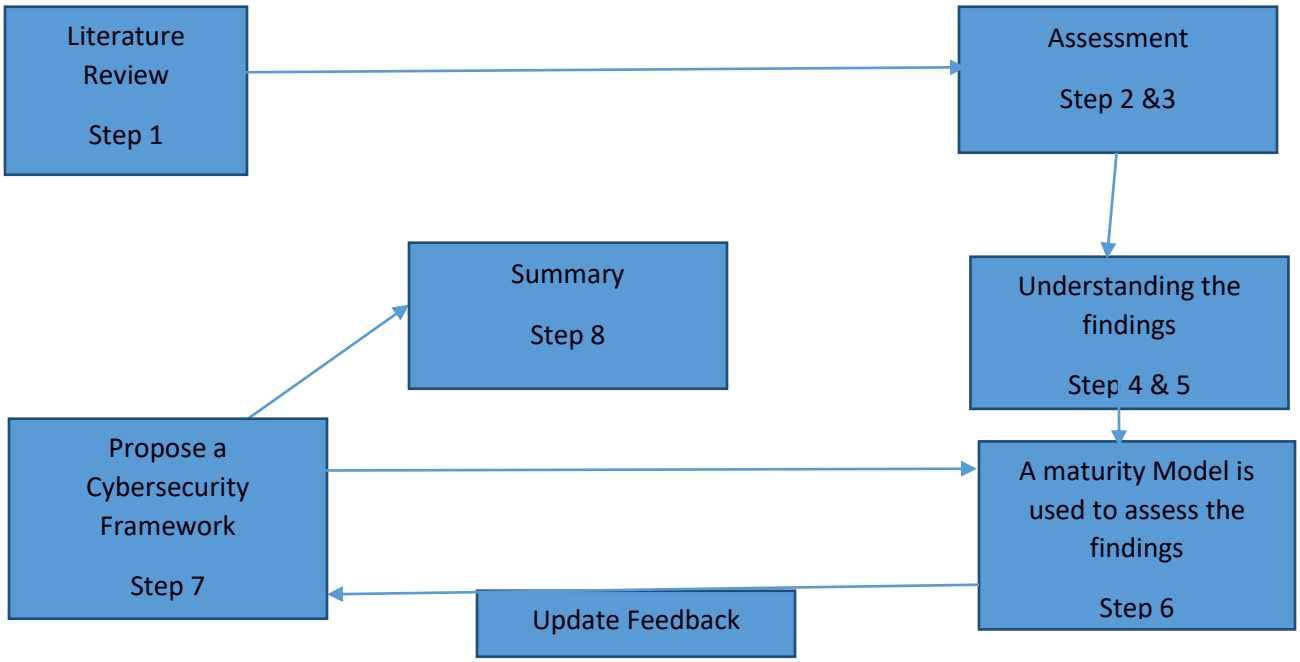
The Cybersecurity capability maturity model helps the student researcher to assess some of the arising questions in the research. For instance by using the questionnaires and interviews as a way to measure the level of Cybersecurity adoption and use in the financial sector in developing countries.

d. ***Propose a conceptual Cybersecurity framework:***

The conceptual Cybersecurity framework was modelled based on literature review findings and the assessment result of the current Cybersecurity framework.

The overall thesis structure is governed by the following main research design components and steps as shown below:

Figure 3-1. Depicts the research design and steps



3.1.2 Steps that have been taken during this study

1. Conducting the literature review to capture the gaps in Cybersecurity adoption by studying the various cybercrimes in the financial sector; In addition to the above the literature review captured the various Cybersecurity frameworks used in the financial sector.
2. Assessing the current state of Cybersecurity adoption and use in the financial sector.
3. The data that was collected from the sample space was analyzed.
4. The findings resulting from the data analysis were discussed with respect to the research questions.
5. The findings are interpreted within the context of the frameworks and capability maturity model.
6. The capability maturity model was used to assess the level the financial sector is at in terms of Cybersecurity adoption and use.
7. Incorporation of a sound feedback was done from the analysis into a proposed conceptual Cybersecurity maturity model.

8. The thesis is concluded with a summary of the findings and the final proposed Cybersecurity maturity model.

3.2 RESEARCH METHODOLOGY

This is primarily exploratory research making it. It is used to gain an understanding of underlying reasons, opinions, and motivations. It provides insights into the problem or helps to develop ideas or hypotheses for potential quantitative research. Qualitative Research is also used to uncover trends in thought and opinions, and dive deeper into the problem. Qualitative data collection methods vary using unstructured or semi-structured techniques. Some common methods include focus groups (group discussions), individual interviews, and participation/observations. The sample size is typically small, and respondents are selected to fulfil a given quota.

3.2 Area of Study

The area of study mainly looked at the adoption and use of cybersecurity in the financial sector in developing countries. In that it studies how best the developing countries can adopt and use the benefits and crucial areas within cybersecurity to ensure information assurance.

3.3 Study population

The study population for the research is comprised of the banking sector, micro finance sector and the telecom sector (mobile money). Under the banking sector the student research looked at five banks; in the microfinance sector the researcher studies two microfinance institutes and in the telecom sector the researcher looks at two telecom companies in Uganda.

3.4 Sampling Procedures

3.4.1 Sample Size

Sampling scope refers to a list or set of direction that identifies the target population. Thus, the target population of this study is those 5 (five) selected Banks, 2(two) Micro Finance Institutions and 2(two) Telecom companies.

3.4.2 Sampling Techniques

It is incumbent on the researcher to clearly define the target population. There are no strict rules to follow, and the researcher must rely on logic and judgment. The population is defined in keeping with the objectives of the study. This is because the sample size is small and as a result the researcher is looking at attaining the best out the limited sample size.

Sometimes, the entire population will be sufficiently small, and the researcher can include the entire population in the study. This type of research is called a census study because data is gathered on every member of the population.

Usually, the population is too large for the researcher to attempt to survey all of its members. A small, but carefully chosen sample can be used to represent the population. The sample reflects the characteristics of the population from which it is drawn.

Sampling methods are classified as either *probability* or *nonprobability*. In probability samples, each member of the population has a known non-zero probability of being selected. Probability methods include random sampling, systematic sampling, and stratified sampling. In nonprobability sampling, members are selected from the population in some nonrandom manner. These include convenience sampling, judgment sampling, quota sampling, and snowball sampling. The advantage of probability sampling is that sampling error can be calculated. Sampling error is the degree to which a sample might differ from the population. When inferring to the population, results are reported plus or minus the sampling error. In nonprobability sampling, the degree to which the sample differs from the population remains unknown.

Random sampling is the purest form of probability sampling. Each member of the population has an equal and known chance of being selected. When there are very large populations, it is

often difficult or impossible to identify every member of the population, so the pool of available subjects becomes biased.

Systematic sampling is often used instead of random sampling. It is also called an nth name selection technique. After the required sample size has been calculated, every nth record is selected from a list of population members. As long as the list does not contain any hidden order, this sampling method is as good as the random sampling method. Its only advantage over the random sampling technique is simplicity. Systematic sampling is frequently used to select a specified number of records from a computer file.

Stratified sampling is commonly used probability method that is superior to random sampling because it reduces sampling error. A stratum is a subset of the population that share at least one common characteristic. Examples of stratums might be males and females, or managers and non-managers. The researcher first identifies the relevant stratums and their actual representation in the population. Random sampling is then used to select a *sufficient* number of subjects from each stratum. "*Sufficient*" refers to a sample size large enough for us to be reasonably confident that the stratum represents the population. Stratified sampling is often used when one or more of the stratums in the population have a low incidence relative to the other stratums.

Convenience sampling is used in exploratory research where the researcher is interested in getting an inexpensive approximation of the truth. As the name implies, the sample is selected because they are convenient. This nonprobability method is often used during preliminary research efforts to get a gross estimate of the results, without incurring the cost or time required to select a random sample.

Judgment sampling is a common nonprobability method. The researcher selects the sample based on judgment. This is usually and extension of convenience sampling. For example, a researcher may decide to draw the entire sample from one "representative" city, even though the population includes all cities. When using this method, the researcher must be confident that the chosen sample is truly representative of the entire population.

Quota sampling is the nonprobability equivalent of stratified sampling. Like stratified sampling, the researcher first identifies the stratums and their proportions as they are represented in the

population. Then convenience or judgment sampling is used to select the required number of subjects from each stratum. This differs from stratified sampling, where the stratums are filled by random sampling.

Snowball sampling is a special nonprobability method used when the desired sample characteristic is rare. It may be extremely difficult or cost prohibitive to locate respondents in these situations. Snowball sampling relies on referrals from initial subjects to generate additional subjects. While this technique can dramatically lower search costs, it comes at the expense of introducing bias because the technique itself reduces the likelihood that the sample will represent a good cross section from the population.

3.5 Data Collections Methods and Instruments

Generally, three types of instruments, namely: questionnaire, Document analysis and interview were employed for the data collection. The primary data was collected through questionnaires (structured) and interview (unstructured and structured).

3.5.1 Questionnaire

A set of questionnaires were designed based on the Strategic, Tactical and Operational aspects within the organization in relation to the adoption and use of cybersecurity in the financial sector in developing countries . The question items are open and closed on practices and status in Cybersecurity Management process. The questioners were prepared and distributed to ICT department, Human Resource department, Audit department, Procurement department, Finance department and Top management of the respective sampled Banks, Microfinance institutions and Telecom companies. The questionnaire developed for the ICT department had 29 questions, HR department had 23 questions, the Procurement department had 12 questions, the Finance department had 19 questions, the Audit department had 18 questions and the Governance team (Senior Management, Top Management) had 33 questions in three categories. The first section dealt with the policy-related. The second section inquired about the strategy of the financial sector in the aspect of cybersecurity. And the third section deals with the HR aspect of Cybersecurity interms of the people, processes and technology.

3.5.2 Interview

Informal information about interviewees' experience and knowledge has been collected by the researcher prior to conducting an interview. They possess the experience and perspective in cybersecurity adoption and use that this research wishes to understand. Given the cybersecurity management experience and background of potential interviewees, purposive sampling method seems the most logical choice for data collection in this research (Anene & Annette, 2007). The main purpose of this interview session is to supplement and increase the validity and reliability of the information obtained through the questionnaire.

3.4.3 Document Analysis

Document analysis was made as believed necessary. Printed materials; books, journal articles, conference proceedings, and internet sources were used to know the subject area in depth, and assess other countries experiences in fighting against their Information systems and cybersecurity threats.

3.6 Quality Control Methods

3.6.1 Validity

According to Sekaran (2000), validity refers to the ability of the instruments to measure what the researcher intends to measure, not another concept altogether. This was measured by seeking expert opinion as to whether the items represent the concepts to be studied. Before setting out to find opinion of experts, in the area of study and questionnaire construction, the advice and opinion of my supervisor will be sought. Content validity in this study will be ensured through testing some questions on a small group prior to the field of research. Questions will be evaluated using the five likert scale of strongly agree, agree, undecided, disagree and strongly disagree. The content validity index (CVI) will be obtained by dividing the number of items declared relevant by the total number of items.

3.6.2 Reliability

A test- retest method of assessing reliability of data which involves administering the same instrument twice to the same group of subjects will be carried out. A correlation of the two sets of scores will be carried out and results evaluated. Where the stability coefficient will become 0.7 or above, the conclusion will be that the test has good test–retest reliability and if it is below

the set reliability coefficient then there will be need to use other measures. Using Alpha Cronbach reliability test, values will be obtained for interpretation (Mugenda & Mugenda, 2003).

3.7 Pilot Study

In order to assess the relevance of the instruments designed to collect data for the study, the pilot study was conducted in one of the sample Banks and one of the sample Micro finance Institutions. The aim was to find out and avoid ambiguity, omissions and misunderstanding of each item. Using the relevant comments from results of the pilot study and suggestions of the advisor corrections were made. Some of the changes that have been made are: The Questionnaires were adjusted to cover the three categories of emphasis which are the Policy, Strategy and Human resource, also by using a sample questionnaire the research student with the help of the supervisor realised that some questions in the questionnaire would have been ideal to assess the results of the questionnaire thus they were removed from the final questionnaires that were distributed out to the financial organisations.

3.8 Data management and Processing

The student researcher collected the data through questionnaires and face to face interviews, and analyse it to assess how each sample study has used and adopted cybersecurity within the financial sector, what gaps they have seen and what plausible solutions they have advised.

3.9 Data Analysis

Data was gathered using online questionnaires, and face to face interviews were carried out and continually edited, later coded and exported to SPSS computer programme for analysis. Descriptive statistics was used to describe the distribution of scores or measurements. Measurements like mode, mean and median will be used to identify the score that will occur most frequently, the average set of scores and the medium score respectively. Likewise, data gathered from key informants using an interview guide, and documentary review will be edited and sorted to give it some meaning. Information recorded verbatim will help the researcher to compare with the responses from the general survey questionnaires so as to arrive at an informed

conclusions about the subject of study. Relevant literature will also be used to compare, discuss and analyse the findings.

3.10 Ethical Considerations

The goal of ethics in research is to ensure that no one is harmed or suffers adverse consequences from research activities (Cooper&Schindler, 2001). The following were done to ensure that the respondents' rights are protected:

- Informed consent was sought and appropriate documentation was kept
- Questionnaires were coded guarantee anonymity as one of the respondents was not named at any time during the research or in the subsequent study.
- Respondents were selected for their willingness to participate without compulsion, and no risk of exposure of the respondents could be identified at any stage during the research.

3.11 Limitations of the study

1. The limitation of the study is due to the sensitivity of the information required from the sampled organisations, there might not be full openness in terms of getting the required information thus resulting into some of the data not being fully accurate.
2. Due to the limited time frame the researcher was unable to collect as much data as possible from the organisations sampled interms of face to face interview. In that some organisation where not easily accessible and some users where not willing to be interviewed.

Conclusion

In conclusion the student researcher mainly focused on qualitative research, and this was achieved through the use of online questionnaires, face to face interviews both structured and unstructured following the three main categories in regards to the adoption and use of cybersecurity in the financial sector and these are; strategic, policy, and human resources.

CHAPTER FOUR:

PRESENTATION, ANALYSIS AND DISCUSSION OF FINDINGS

4.0 INTRODUCTION

During the presentation and analysis of the information captured through the various streams of data collection, the researcher critically analyses the adoption and use of cyber security within the financial sector in developing countries with much emphasis on the Ugandan Financial sector. This is achieved through the various interviews and questionnaires that were administered to the various people.

The chapter looked at exploring and assessing the adoption and use of cyber security within the financial sector in developing countries. This was done by assessing the data that was acquired by the researcher through interviews and questionnaires. The emphasis of the interviews and questionnaires was to cover the objectives that had been raised by the researcher in chapter two of the research thesis.

The Questionnaires were divided among departments; Audit, Human Resource, Finance, Procurement, and ICT. As the researcher explorers the analysis, she will be able to list each department's responses.

4.1 Response Rates of respondents

Response rate (also known as completion rate or return rate) in survey research refers to the number of people who answered the survey divided by the number of people in the sample. It is usually expressed in the form of a percentage. A low response rate can give rise to sampling bias if the non-response is unequal among the participants regarding exposure and /or outcome (AAPOR, 2000). In this study, the targeted sample size was 46 but 31 staff responded to the questionnaires, 3 respondents participated in the face to face interviews making it a total of 34 respondents.

Table 4.1 Presents the response rates to the study In the case of Adoption and Use of Cyber security in the financial sector in developing countries.

Category of Respondents	Sample Size	Actual Response	Percentage
Managers/officers/support staff	40	31	77.5%
Specialists/Directors (CEOs, CISOs, CIOs, ICT managers and consultants)	6	3	50%
Total	46	**34**	73.91%

According to Table 4.1 above, out of the 40 questionnaires administered in total, 31 were returned fully completed giving a response rate of 77.5%. Out of 6 respondents targeted for interviews, 3 were fully interviewed giving a response rate of 50%. The overall response rate of the respondents was thus, 73.91%. With that high response rate, the findings of the study were representative of the actual population and could therefore be generalized as observed by Sekaran (2003).

4.2 Background Information of the Respondents

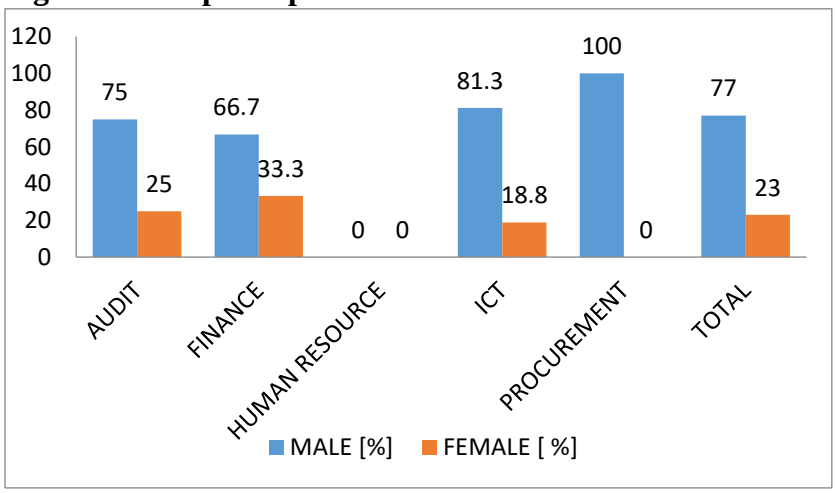
The respondents where a composition of employees from various departments within the banking sector and specialists with in the topic of cyber security adoption and use in the financial sector in developing countries. In that; The Questionnaires were divided among departments; Audit, Human Resource, Finance, Procurement, and ICT. As the researcher explorers the analysis, she will be able to list each department's responses.

The analysis and presentation breakdown for the questionnaires will therefore be categorized according to the departmental responses, while the interview questions will be broken down according to the management level and industry standards.

Bio data

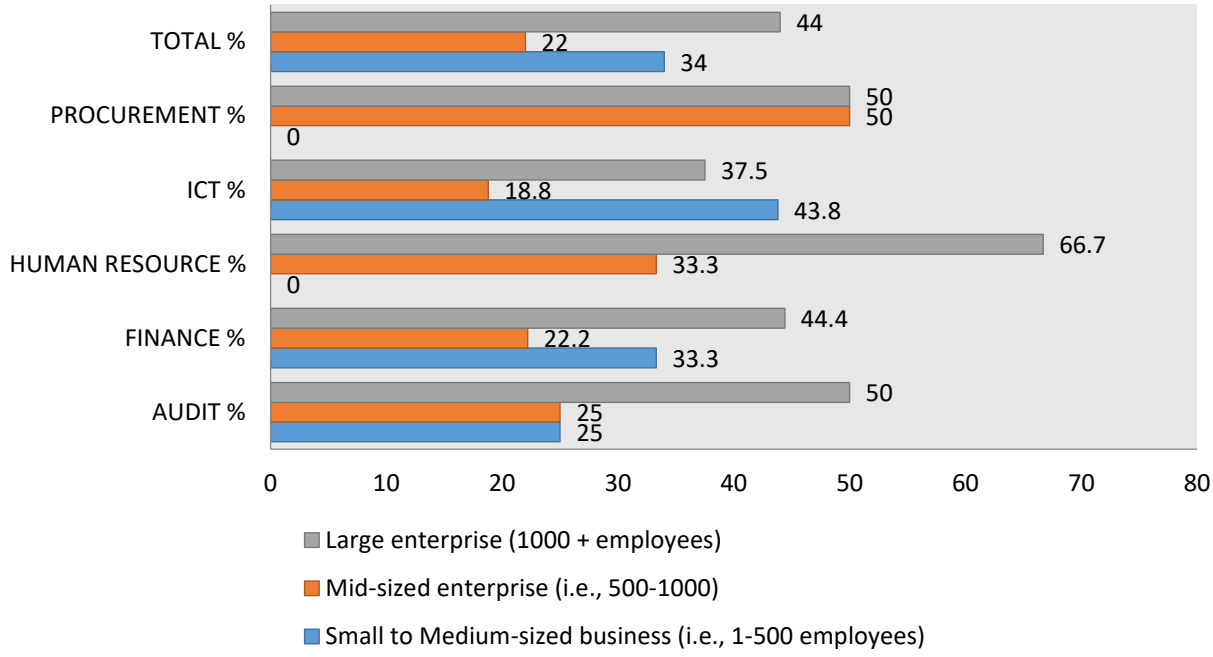
What is your sex?

Figure 4.1 sex per department



From the graph above majority of the respondents were male (77%) with only 23% of the females; this mighty have been attributed to the fact that men take on technical jobs like IT more than women. As per department most of the female respondents were observed in the finance department (33.3%) followed by the Audit department (25%). The question of what is your sex was not included on the questionnaire for Human resource department.

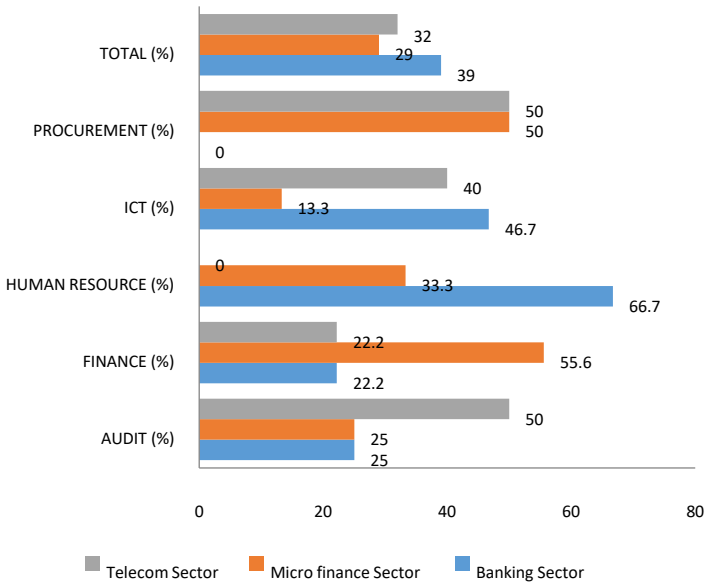
Figure 4.2 The demand for ICTs Company size



From the graph above 44% of the total number of responses indicated that their company was large enterprise (1000+ employees), 34% indicated mid-sized business (i.e., 500-1000) and only 22% indicated small to medium-sized business; this indicates the increasing demand for cyber security in the financial sector. In addition to the above highest percentages for large enterprise are observed on the graph in all departments.

Figure 4.3 Vertical markets for ICTs

What vertical market best describes your organization?



The data reveals that 39% of the total number of responses noted that the banking sector was a vertical market which best described their organization this was most probably because the banking sector involves numerous transactions with huge amounts of money (according to an interview with Naturinda Hosea). 32% of the responses noted telecom due to the rapid growth of money banking in the country and only 29% noted micro finance.

The table also shows the preferences of the different departments where 66.7% of the responses in the Human Resource noted that the banking sector was the best vertical market for their organization, 55.6% of the responses in finance noted micro finance sector, 50% of the respondents in Audit noted telecom sector which was not different from the procurement department.

How have banks and microfinance institutions moved towards securing use of ICTs and mitigating risks?

AUDIT DEPARTMENT

Table 4.2 control review and update of registry audit tool

	Regularly review controls		keeping the registry audit tool up to date	
	Frequency	**%**	**Frequency**	**%**
Yes	4	100	3	75
No	0	0	1	25
Total	4	100	4	100

The data reveals that 100% of the responses indicated that the audit department regularly reviews controls pertaining to cyber security. Of these three quarters further showed that the registry audit tool is always kept up-to-date on the latest developments and does include related cyber security issues with only 25% revealing that the registry audit tool is always kept up-to-date.

Regularly reviewing controls pertaining to cyber security and always keeping the registry audit tool up-to-date on the latest developments including cyber security related issues enables the audit department to trace for any irregularities within the use of ICTs.

FINANCE DEPARTMENT

Budget

Table 4.3 cyber budget

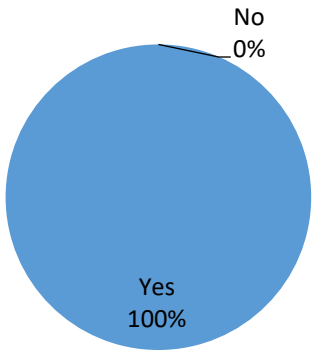
	Budget for cyber budget		Is the budget sufficient	
	Frequency	**%**	**Frequency**	**%**
Yes	4	50	5	62.5
No	4	50	3	37.5
Total	8	100	8	100

Similar responses (50% each) were got on issues relating to whether there was a budget to cater for cyber security breaches or not. On the other side 62.5% of the responses revealed that the budget allocated to the ICT department was sufficient to combat the ICT risks that may arise.

Having a budget which is sufficient enables banks and financial institutions to have the required expertise, equipment, software and infrastructures necessary for securing the use of ICTs and mitigating risks.

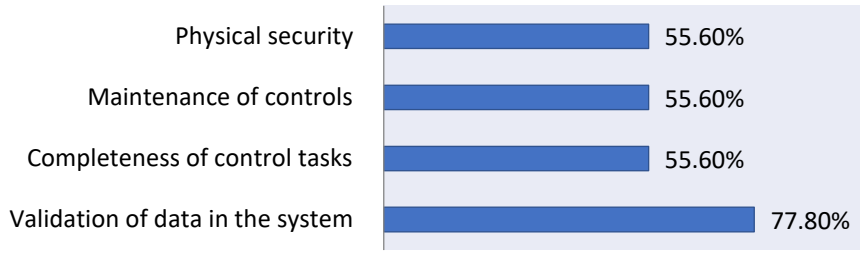
Figure 4.5 Financial policy

Do you have a financial policy?



The data reveals that 100% of the responses indicated that there was a financial policy. Of these 77.8% revealed that the financial policy uses the guideline of validation of data in the system. 55.6% of the responses indicated that that the policy uses the guidelines of physical security, maintenance of controls and completeness of control tasks as shown in the below

Figure 4.6 Guidelines for mitigating cyber security risks in the financial policy



Validation of data in the system endorses and justifies that the data in the ICT system. In addition physical security, maintenance of controls and completeness of control tasks eliminates any possibilities of insecurities and risks

HUMAN RESOURCE

Table 4.4 Applicant commitment and recruitment checks

	Applicants Agree& abide to policies, standards and guidelines		Applicants Sign declaration forms		Recruitment checks	
	Frequency	**%**	**Frequency**	**%**	**Frequency**	**%**
Yes	**3**	**100**	**3**	**100**	**3**	**100**
No	**0**	**0**	**0**	**0**	**0**	**0**
Total	**3**	**100**	**3**	**100**	**3**	**100**

The data reveals that 100% of the responses agreed that their organization ensure that individuals agree and abide by all the policies, standards and guidelines for protecting information and physical assets against security threats regardless of type of origin. 100% of the responses agreed that their organization confirm that, as part of the HR process all employees, accessing and/ or operating critical infrastructure sign declaration forms acknowledging their obligation to abide

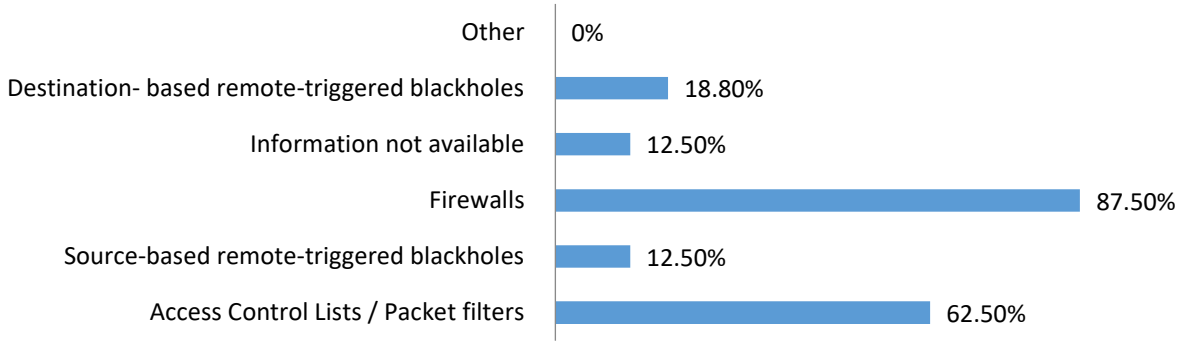
by related industry standards and also that the organizations carry out Recruitment checks such as level of training in the set field and experience of staff in the field of expertise.

In addition to the above, the human resource department of the organization also conducts checks to verify the identity of the candidate by conducting using government or third party issued documents such as passports or similar forms of identification, establish whether the applicant has the right to work in Uganda, check the candidate's employment record validating the completeness and accuracy of the curriculum vitae, obtain satisfactory character references about the applicant, establish whether the applicant is qualified for the job they applied for by confirming the claimed academic and professional qualifications, maintain an up to date personnel records file of all staff/ employees of the organization and ensure that security clearances undergo regular review.

This guarantees confidentiality, hiring of the required expertise and protection of the ICT system.

ICT DEPARTMENT

Figure 4.2 mitigation measures for cyber security attacks targeted



Most of the responses (87.5%) revealed that setting up firewalls would mitigate cyber security attacks targeted at their organization’s infrastructure / customers, 62.5% indicated setting up of access control list/packet filters and 18.8% indicated setting up destination-based remote-triggered black holes.

The use of firewalls blocks all unauthorized communications between the machines within the organization and the outside world thus ensuring that ICT is secure for use.

PROCUREMENT DEPARTMENT

Table 4.5 procurement checks

	Identifying &evaluation of security risks during out sourcing		**Accountability for managing risks**		**fully acquainted and compliant with the ICT policies**	
	Frequency	**%**	**Frequency**	**%**	**Frequency**	**%**
Yes	2	100	2	100	2	100
No	0	0	0	0	0	0
Total	2	100	2	100	2	100

The data reveals that 100% of the responses indicated that the procurement department identifies and evaluates the security risks related to the outsourcing or offshoring before approving contracts for critical infrastructure and services, recognize that they retain accountability for managing their information risks even where they outsource ICT systems and services to third parties and fully acquainted and compliant with the ICT policies and the organization impact assessment processes for ICT suppliers.

In addition the department abides by the ICT policy to identify, document and incorporate security requirements into outsourcing contracts with suppliers and contractors, follows the security management plan outlining the strategies for reducing security risks when acquiring suppliers and carry out checks to confirm that ICT suppliers are certified.

These activities performed by the procurement department ensure that the contracted suppliers work with the agreed upon terms and conditions, have the required documentation and are Competent

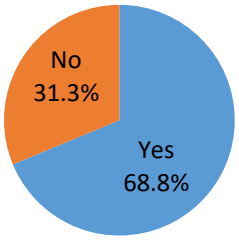
At which level is Cyber security management placed with the Governance structure of financial institutions?

Figure 4.7 do you have department responsible cyber security

A reasonable portion of the responses (40%) indicated that there was a dedicated department/unit responsible for cyber security, 33.3% indicated that it was part of another department while 26.7% revealed that didn't have a department responsible for cyber security.

Does your organization have a chief information security officer?

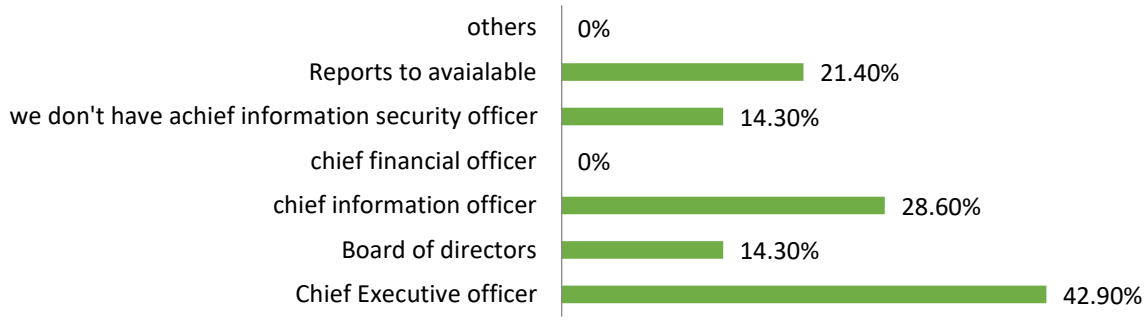
Figure 4.8 Does your organization have a chief information security officer?



Most of the responses (68.8%) revealed that organizations had a chief information officer with only 31.3% of them revealing that they didn't have a chief information officer.

Who does the chief information security officer report to?

Figure 4.9 Who does the chief information security officer report to?



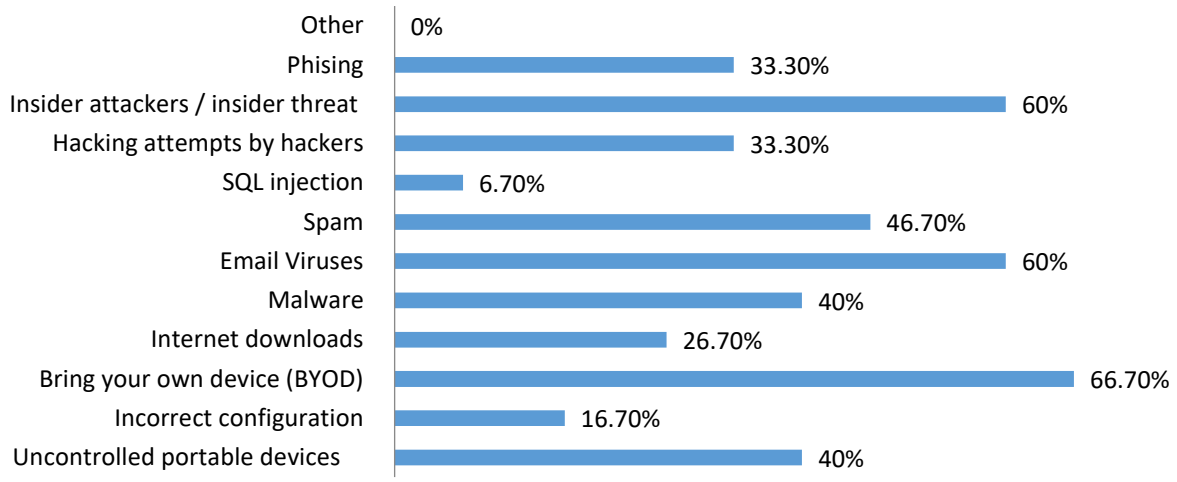
That data reveals that 42.9% of the responses indicated that the chief information security officer reports to the chief executive officer, 28.6% of the responses indicated that the chief information security officer reports to the chief information officer while 21.4%indicated that the chief information security officer report to anyone available.

From the analysis above, the Cyber security management is under a department which is headed by the chief information security officer who reports mainly to the chief executive officer.

What gaps exist in the Cyber security management of financial institutions in regards to ICTs?

Gaps in the cyber security management

Figure 4.10 Gaps in the cyber security management

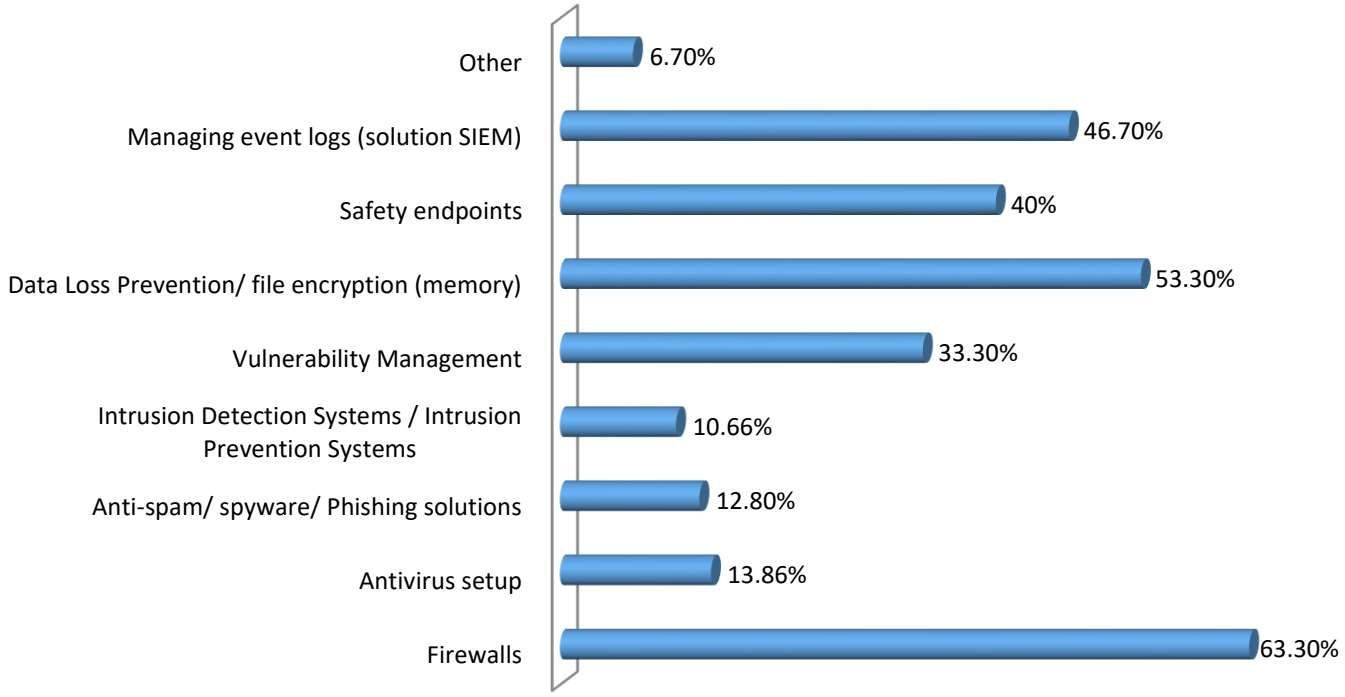


Most of the responses (66.7%) revealed that bringing in your own device is the greatest risk in the Cyber security management of financial institutions in regards to ICTs, 60% of the responses indicated insider attackers/ inside threat and email viruses as the greatest cyber security risks. 46.7% and 40% indicated spam and malware as the greatest cyber security risks.

Employees bringing in own devices expose the ICTs to viruses, theft of software and above all leads to exposure of the software to the outside world which may lead to hacking of systems.

What measures can be set in place to improve the Cyber security management within in financial institutions?

Figure 4.11 Cyber security measures being implemented

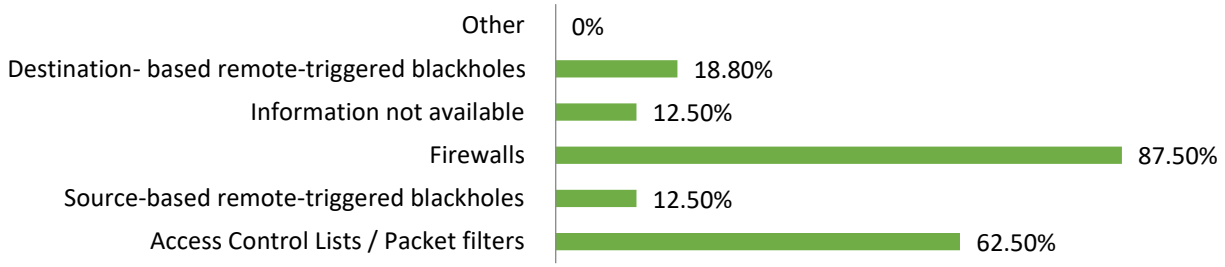


The data reveals that most of the responses (63.3%) of the in ICT department indicated that setting up firewalls would be the best measure to improve on cyber security management, 53.3% indicated that data loss prevention/ file encryption (memory) would improve on the cyber security management with 46.7% revealing that management of event logs (solution SIEM)is the best measure. 40% of the responses indicated safety of endpoints and 33.3% believed in vulnerability management as measures to improve on cyber security management.

The use of firewalls blocks all unauthorized communications between the machines within the organization and the outside world thus ensuring that ICT is secure for use.

Measures usually taken to mitigate cyber security attacks targeted at organization's infrastructure / customers

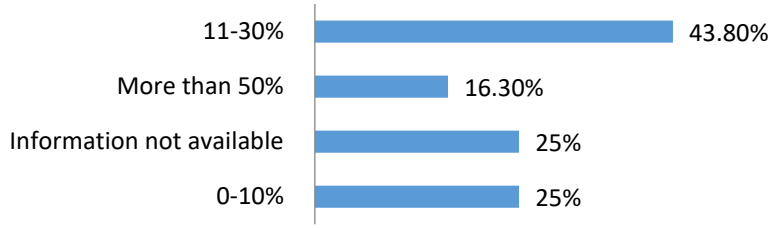
Figure 4.12 Measures usually taken to mitigate cyber security attacks targeted at organization's infrastructure / customers



Most of the responses (87.5%) revealed that setting firewalls would mitigate cyber security attacks targeted at organization's infrastructure / customers, 62.5%indicated that the use of access control lists/ packet filters with only 18.8% indicating the use of destination-based remote-triggered black holes as cyber security mitigation measures.

Budget allocation to the ICT department

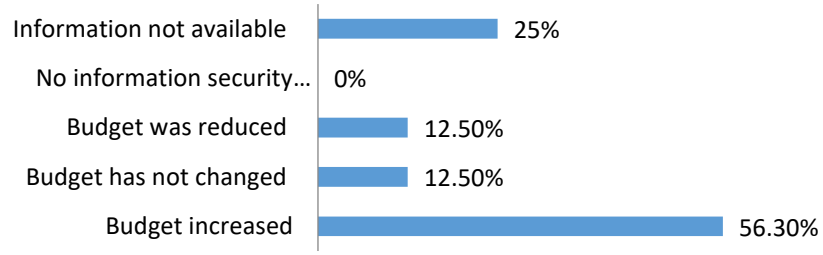
Figure 4.13Percentage of IT-budget spent on security in the last 12 months



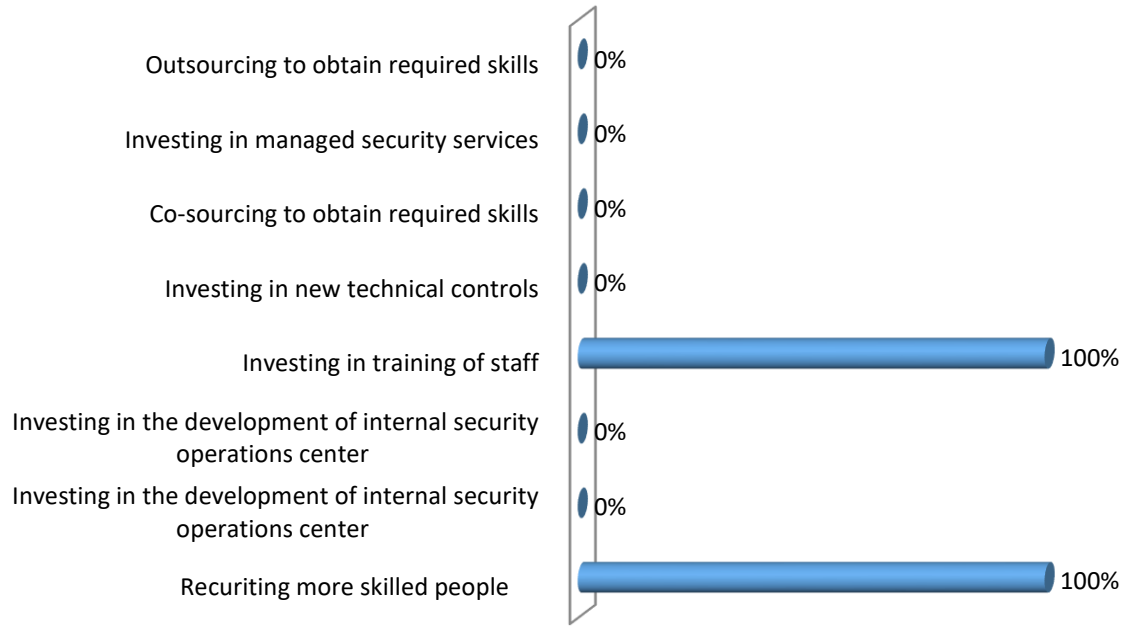
The data reveals that most of the responses (43.8%) indicated that the IT-budget spent on security in the last 12 months was 11-30% with only 16.30% indicating that the percentage was more than 50%. 25% of the responses show that there was no information available.

However, 56.30% of the responses indicated that the budget increased year to year, with only 12.5% indicating that the budget was reduced and has not changed. 25% of the responses indicate that there was no information available as shown below,

Figure 4.14 Description of year-to-year spending in terms of your cyber /information security budget

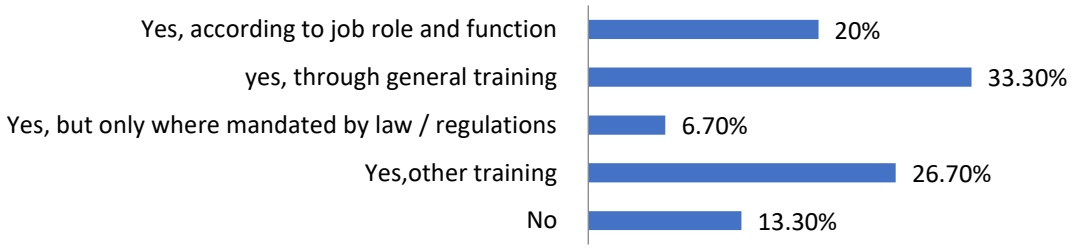


The results above show that banks and financial institutions keep on increasing their budget for cyber security; this makes it possible for the ICT department to have the best qualified employees, equipment, software and infrastructures necessary for ensuring that Cyber security management is efficient and effective.



The data reveals that 100% of the responses indicated that investing in training of staff and recruiting more skilled labour were the cyber security expenditures that dominated the budget according to the respondents from the procurement department. However, according to the finance department.

Figure 4.15Employee training to raise cyber security awareness

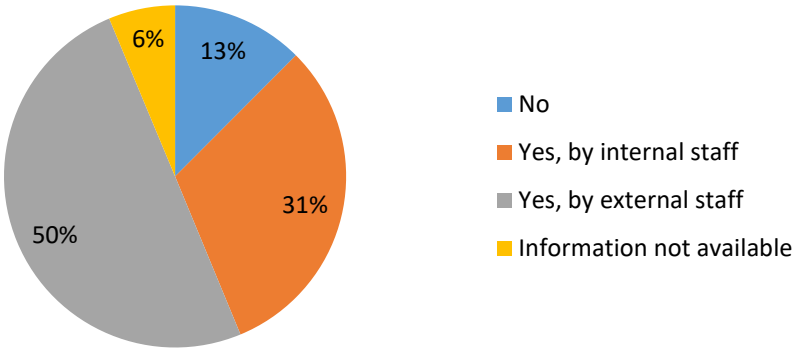


A reasonable portion of the responses (30%) indicated that employees are trained through general training with 26.7% indicating that they are trained through other trainings to raise cyber security awareness. 20% of the responses reveal that employees are trained according to job role and function with only 13.3% revealing that employees are not trained.

Training of the employees equips them with skills and knowledge of handling the latest software, equipment, threats, breaches, hacker tactics and also builds confidence in workers; this enables greatly improves on the cyber security management.

Performing vulnerability Assessment and Penetration Testing

Figure 4.16performing vulnerability Assessment and Penetration Testing

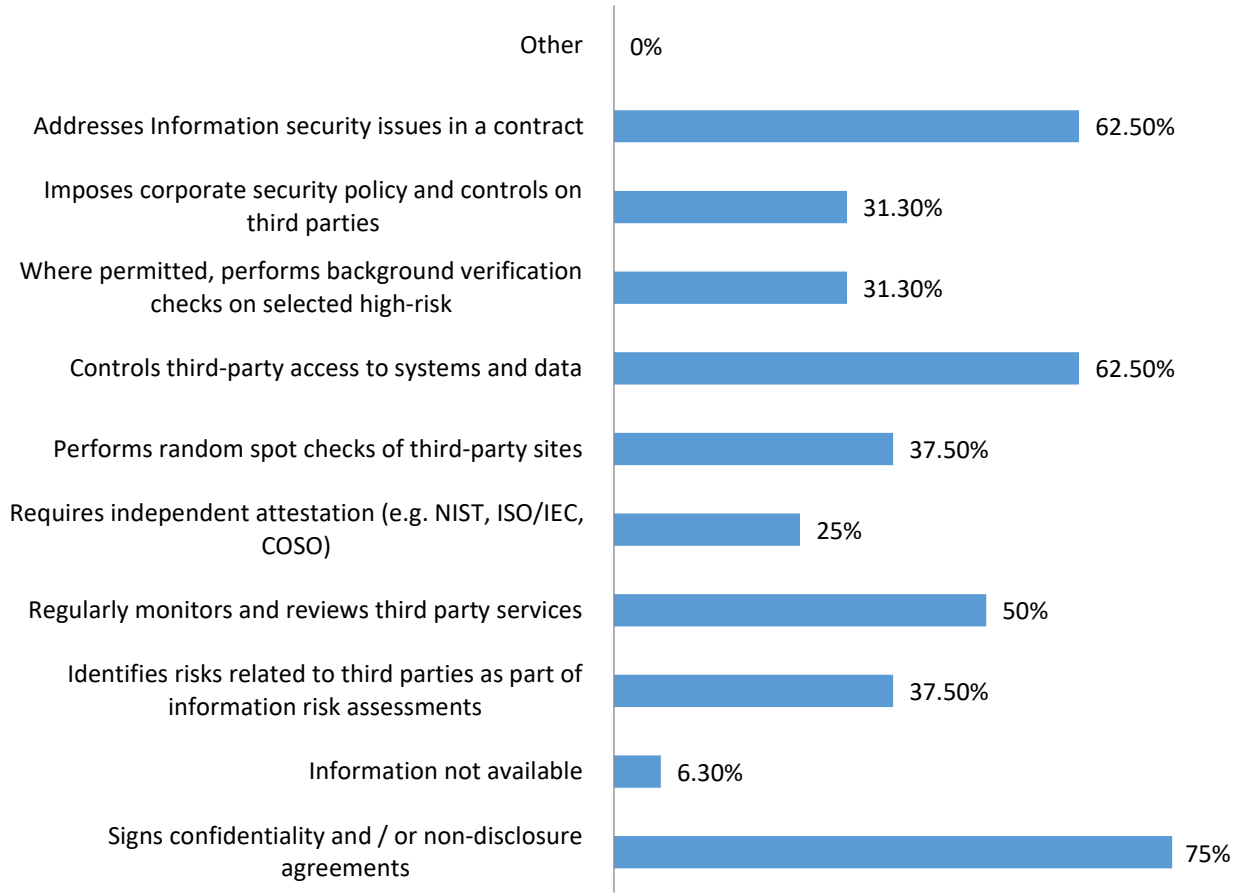


Most of the responses (50%) revealed that their organizations perform vulnerability Assessment and Penetration Testing using an external staff, 31% revealed that their organizations perform vulnerability Assessment and Penetration Testing but using an internal staff with 13% revealing that there was no information available and only 6% saying no.

This indicates that most organizations perform vulnerability Assessment and Penetration testing which enables them to identify all the possible weaknesses in and ways of accessing their security systems which may lead to breach of confidentiality, and integrity of the system. However, there is need to train more of the internal staff so that the testing is done internally to increase confidentiality and avoid leakage of information outside the organization.

Ensuring an adequate and appropriate level of cyber security over third parties

Figure 4.17Ensuring an adequate and appropriate level of cyber security over third parties

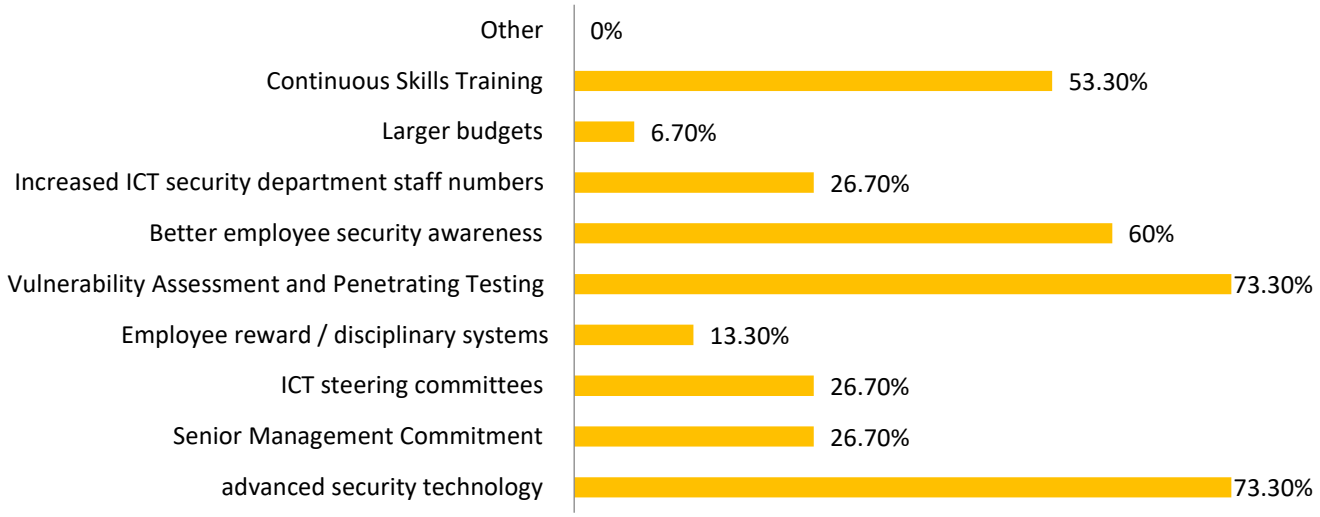


The data reveals that 75% of the responses indicated that third parties sign confidentiality and/ or non-disclosure agreements, 62.5% of them indicate that their institutions control third party access to systems and data, these also indicated that the institutions address information security issues in contracts as measures to improve on their Cyber security management. 50% of the responses indicated that institutions regularly monitor and review third party service

Despite the fact that all the above were measures setin place to improve the Cyber security management within in financial institutions when placed on balance; most of the responses

(73.3%) indicated the use of advanced security technology and performing vulnerability assessment and penetrating testing as the best way of improving on Cyber security management within in financial institutions. Relatively high responses (60%) and (53.3%) indicated better employee security awareness and continuous skills training respectively as shown by the figure 15 below.

Figure 4.18Best ways of improving on Cyber security management within in financial institutions.

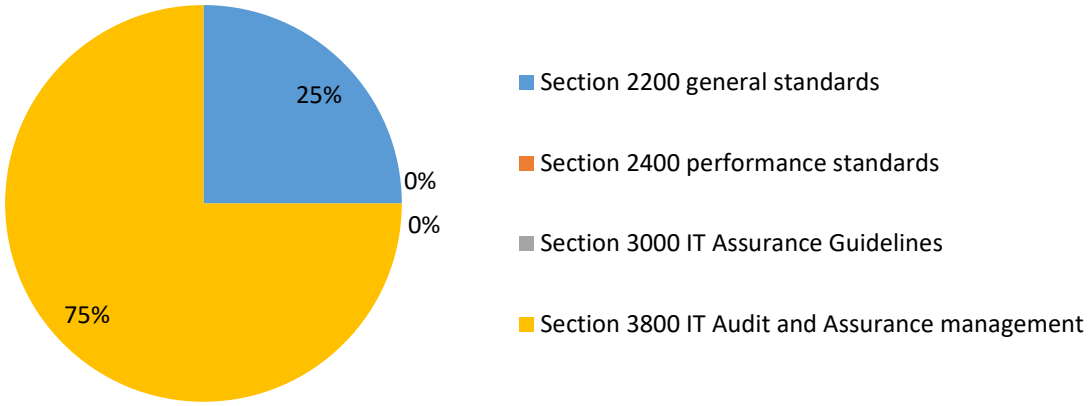


Which Cyber security frameworks are used in the Financial Institutions in developing countries?

AUDIT DEPARTMENT

Tools used to carry out audit in the organization

Figure 4.19Tools used to carry out audit in the organization

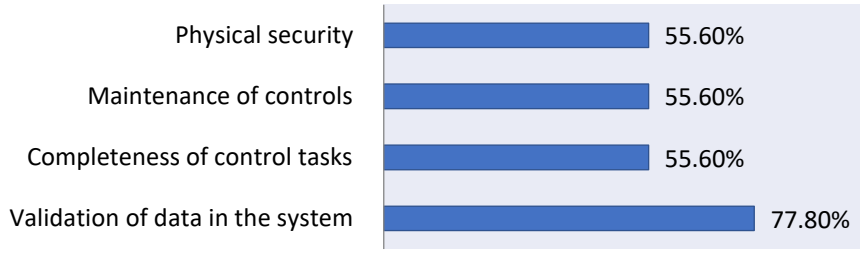


Majority of the responses (75%) indicated that section 3800 IT Audit and Assurance management was the tool used to carry out audit in the organization while 25%indicated that section 2200 general standards was the tool.

FINANCE DEPARTMENT

Financial policy;

Figure 4.20Guidelines in the financial policy for mitigating cyber security risks



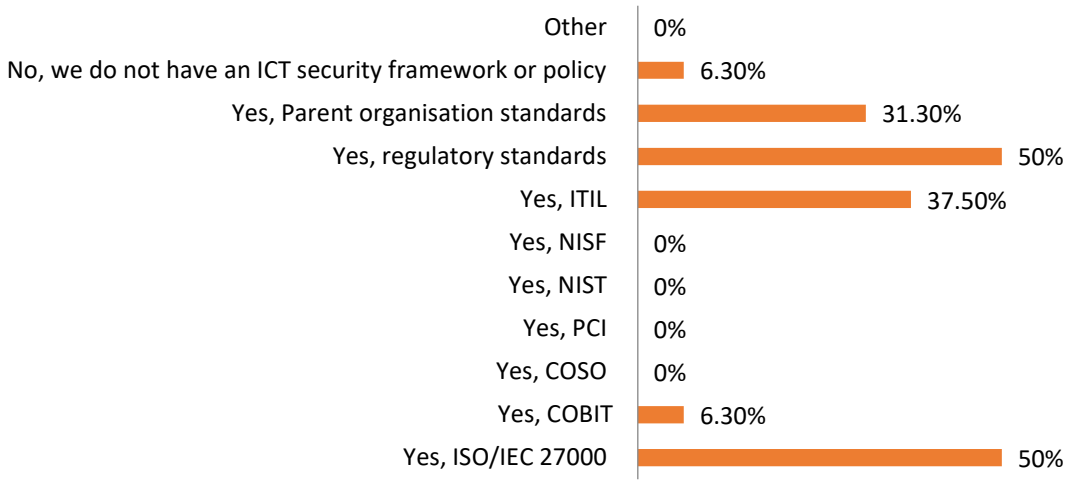
The data reveals that most of the responses (77.8%) indicated that the financial policy uses the guideline of validation of data in the system as way of mitigating cyber security risks. 55.6% of the responses indicated physical security, maintenance of controls and completeness of control tasks as ways of mitigating cyber security risks.

Validation of data in the system is proof and justification that the data in the system is accurate and secure from risks.

ICT DEPARTMENT

IT process or Security frameworks and / or standards

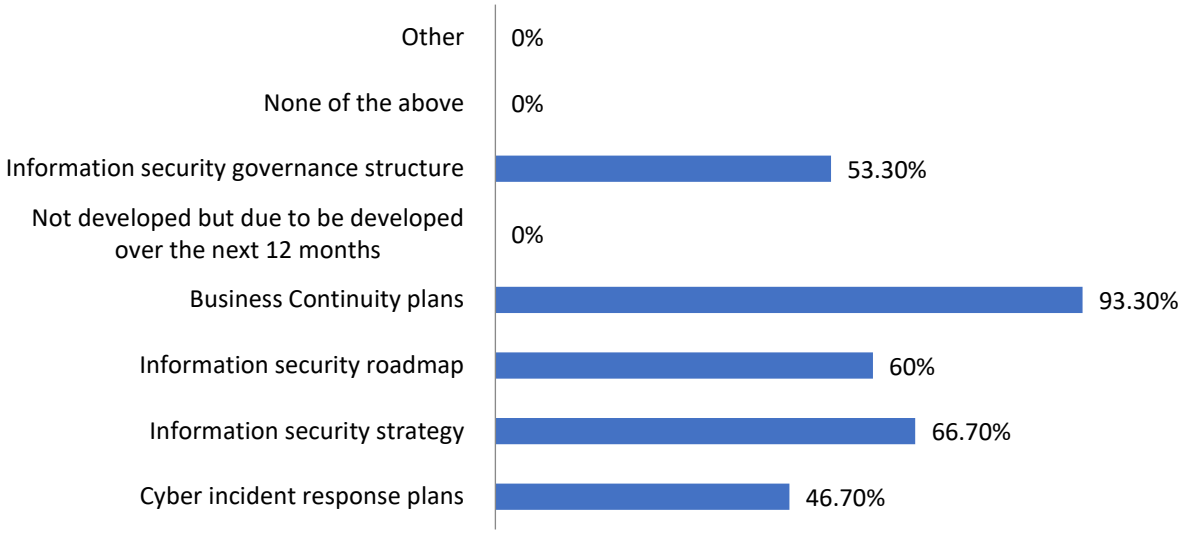
Figure 4.20IT process or Security frameworks and / or standards



The data reveals that 50% of the responses indicated that ISO/IEC 27000 and regulatory standards are the security frameworks and standards adhered to by their organizations. 37.5% and 31.3% indicate that ITIL and parent organization standards were the security frameworks and standards adhered to by their organizations.

Policies and procedure documented and approved by organizations

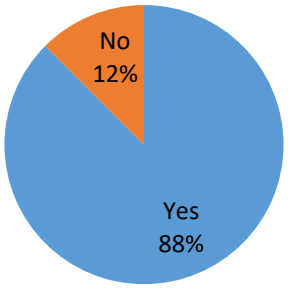
Figure 4.21Policies and procedures documented and approved by organizations



Majority of the responses (93.3%) revealed that having a documented and approved business continuity plans as the Policy and procedure documented and approved by organizations. 66.7% and 60% indicated that having information security strategy and information security roadmap respectively were the Policies and procedure documented and approved by organizations the must be approved .

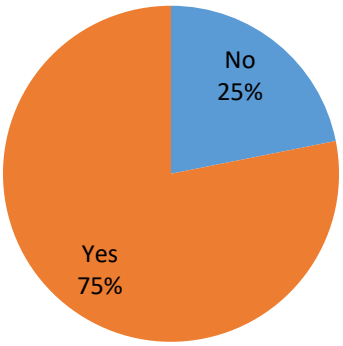
Disaster recovery plan been tested

Figure 4.22Are there cyber incident scenarios incorporated in the financial institutions' business continuity and disaster recovery plans?



The data reveals that 87% of the responses were in favour of cyber incident scenarios being incorporated in the financial institutions' business continuity and disaster recovery plans with only 13% indicating that it's not incorporated in the financial institutions' business continuity and disaster recovery plans. In addition to the above majority of the responses (75%) indicated that the cyber incident scenarios incorporated in the disaster recovery plan had been tested as shown by figure 21 below;

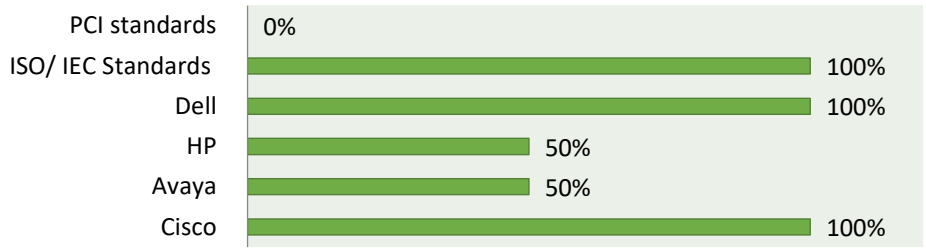
Figure 4.23Have the scenarios incorporated in the disaster recovery plan been tested?



PROCUREMENT DEPARTMENT

Standards and certified companies used when carrying out checks to confirm that ICT suppliers are certified

Figure 4.24Standards and certified companies used when carrying out checks to confirm that ICT suppliers are certified



The data reveals that 100% of the responses indicated that ISO/IEC standards, Dell and Cisco as the standard and certified companies that the procurement department use when carrying out checks to confirm that ICT suppliers are certified. 50% of the responses indicated that HP and Avaya as the standard and certified companies.

4.3 Discussion and Analysis of Findings

How have banks and microfinance institutions moved towards securing use of ICTs and mitigating risks?

Microfinance institutions through the audit department regularly reviews controls pertaining to cyber security and always keep the registry audit tool up-to-date on the latest developments including cyber security, related issues enables them to trace for any irregularities within the use of ICTs.

Through the procurement department microfinance institutions identify and evaluate the security risks related to the outsourcing or offshoring before approving contracts for critical infrastructure and services, recognize that they retain accountability for managing their information risks even where they outsource ICT systems and services to third parties and fully acquainted and compliant with the ICT policies and the organization impact assessment processes for ICT suppliers.

Microfinance institutions have prepared a cyber-budget which is sufficient to enable them to have the required expertise, equipment, software and infrastructures necessary for securing the use of ICTs and mitigating risks.

Microfinance institutions follow and implement a financial policy which includes Validation of data in the system, physical security maintenance of controls and completeness of control all these eliminates any possibilities of insecurities and risks.

Through the human resource department microfinance institutions ensure that individuals agree and abide by all the policies, standards and guidelines for protecting information and physical assets against security threats regardless of type of origin, all employees, accessing and/ or operating critical infrastructure sign declaration forms acknowledging their obligation to abide 1by related industry standards and also that the organizations carry out Recruitment checks.

Microfinance institutions have setup firewalls with an aim of blocking all unauthorized communications between the machines within the organization and the outside world thus ensuring that ICT is secure for use.

At which level is Cyber security management placed with the Governance structure of financial institutions?

The Cyber security management is under a department which is headed by the chief information security officer who reports mainly to the chief executive officer.

Gaps in the Cyber security management of financial institutions

Employees bring in their devices and insider attackers/ inside threat were the predominate gaps which existed in Cyber security management of financial institutions this is in line with Hamin (200) who stated that insiders are in an advantageous position to misuse organizational Information systems, due to their familiarity with the system structures and potential weak spots in security administration. Further according to Colwill (2009) security incident perpetrated by an insider can impact an organization in various ways. Potential results of insider threat incidents could be negative impact on the public image of an organization, negative impact on the revenue of an organization or litigation due to disclosure of confidential.

Measures set to improve the Cyber security management

The findings show that performing vulnerability assessment and penetrating testing was the best way of improving on Cyber security management within in financial institutions which was most probably because the testing enables them to identify all the possible weaknesses in and ways of accessing their security systems which lead to breach of confidentiality, integrity of the system, availability, access control and, non-repudiation which are the five quality attributes compose a system's (*Lehtinen, Rick et al 2006*).

The findings reveal that procurement departments ensure that third parties sign confidentiality and/ or non-disclosure agreements, have controlled access to systems and data and that their services are regularly monitored and reviewed.

The findings show that employees are trained; this equips them with skills and knowledge of handling the latest software, equipment, threats, breaches, hacker tactics and also builds confidence in workers; this enables greatly improves on the cyber security management.

The results show that banks and financial institutions keep on increasing their budget for cyber security; this makes it possible for the ICT department to have the best qualified employees, equipment, software and infrastructures necessary for ensuring that Cyber security management is efficient and effective.

The findings reveal that setting firewalls and use of access control lists/ packet filters would mitigate cyber security attacks targeted at organization's infrastructure / customers. The use of firewalls blocks all unauthorized communications between the machines within the organization and the outside world thus ensuring that ICT is secure for use.

Cyber security frameworks

The findings show that ISO/IEC 27000 and regulatory standards were the most used Cyber security frameworks which is in agreement with Rajendra et al., 2016 who noted that the most widely used frameworks for cyber security included ISO27000 series. The predominate use of the ISO/IEC 27000 and regulatory standards might have been attributed to its efficient and effective requirements which include Security policy, Organization of information security, Asset management Human resources security, Physical and environmental security, Communications and operations management , Access control, Information systems acquisition, development and maintenance, Information security incident management, Business continuity management systems, Compliance and Risk assessment (ISO/IEC 27001-2 & Yigezu, 2011)

The findings reveal that Dell and Cisco were the certified companies that most procurement departments preferred to use for their cyber security. "*We use Dell or Cisco because they are the suppliers of IC's and cheaper compared to others" (INTERVIEW, participant – Naturinda Hosea).*

The findings reveal that most of the banks and financial institutions have cyber incident scenarios incorporated in their documented / approved business continuity and disaster recovery plans. In addition, the cyber incident scenarios incorporated in the plans have been tested.

The data reveals that most banks and financial institutions use the guidelines of validation of data in the system, physical security, and maintenance of controls and completeness of control tasks in their financial policy as tools for mitigating cyber security risks

The findings indicate that most of the audit departments use section 3800 IT Audit and assurance management as tools for carrying out audit in the organization.

CHAPTER FIVE

CONCULUSION AND RECOMMENDATION

5.0 Proposed maturity model

Using a combination of the ESG Cybersecurity maturity model the researcher was able to assess and determine and measure the level of cybersecurity adoption and use within the financial sector.

The researcher mainly focused on the ESG model since it mainly looked at the four most crucial categories within the research and these were; Philosophy, People, Processes and Technology.

The model also looks at Organisations within three main categories; Basic Organisations, Progressing Organisations and Advanced Organisations. This is because while these categories focus on all various organizations and sizes the researcher was able to show that they exhibit similarities with regards to their cybersecurity philosophies, their people as well as the processes and technology behavioral patterns. This was seen by the researcher in the responses that were acquired during the analysis of the research through the questionnaires, interviews and respondents feedback.

During the analysis, the researcher was able to estimate that 30 % of the financial sector players fell under the basic organizations (Limited maturity level), 60% of the financial players fell under the progressing organizations while 10% of the financial players had actually attained the advanced Organisations (Optimizing)

Table 5.0 the ESG Cybersecurity Model

Category	Basic Organisations	Progressing Organisations	Advanced Organisations
Philosophy	Cybersecurity is a "necessary evil"	Adoption and use of Cybersecurity must be more integrated into the business	Cybersecurity is part and partial of the cultural norms
People	CISO reports to IT. Small security team with minimal skills. High chances of not achieving the goals set by the organization and minimal to poor turnover.	The CISO reports to COO or other non-IT manager. Larger security team with some autonomy from IT. Workload is still overwhelming since the staff are minimal and not skilled enough	CISO reports to the CEO and is active with the board. CISO is looked at a business executive. Large well organized staff with good working environment. Skills and staff problems persist due to the global cybersecurity skills shortage.
Process	Very informal and ad-hoc subservient to IT	Better Coordination with IT processes even though they are informal, manual, and dependent upon individual stakeholders	Well documented and formal policies and guidelines with an eye towards more scalability and automation.
Technology	Elementary security technologies with simple configurations. De-centralized security with limited	More advanced use of security technologies and adoption of new tools for incident detection and security	Building an enterprise security technology architecture. Focusing on incident prevention, detection,

	coordination across functions. Focus is on prevention and regulatory compliance.	analytics.	through penetration testing and response. Adding elements of Cybersecurity adoption and use.

Source: Enterprise Strategy group, 2014

Looking at the maturity model the researcher was able to further analyize the current level of cybersecurity adoption and use within the financial sector basing on the analysis from the sample space these where the findings;

Profile of Basic Organizations

As previously mentioned, about 30% of organizations fall into the "basic" category. These firms can be described as follows: **Philosophy: Information security is a "necessary evil."** Basic organizations have a history of dismissing "good security" and adopting "good enough security." In other words, they tend to cut corners in terms of security investment as much as possible, opting for only what's absolutely necessary. These decisions reflect the fact that basic organizations really don't understand the relationship between IT-based business processes and strong security, thus they face a higher level of IT risk than they understand. In many cases, the information security focus at basic organizations tends to skew toward elementary threat prevention and meeting regulatory compliance requirements rather than protecting IT assets, valuable data, and employees or detecting/responding to actual security attacks.

People: Security administrators and compliance wonks. Cybersecurity is considered an IT sub-discipline at basic organizations. As such, they tend to have technology-focused CISOs who report to the CIO or another IT manager (if they have a CISO at all). The security group tends to be lean, with many standard security tasks handled by the IT staff. Since basic organizations consider security a low priority, they can't recruit top talent, and those security professionals they do hire tend to be overworked and frustrated. Not surprisingly, basic organizations experience high turnover within the security staff.

Processes: Tend to be informal and manual. Since the security team is understaffed and under-skilled, they tend to spend a lot of time dealing with the emergency Du Jour. This leaves

little room for planning, skills development, or creating an appropriate security strategy. Security processes tend to be ad hoc as security professionals have limited ability to influence the IT staff at large. All security activities depend upon individual skills and techniques rather than formal processes. This creates a visible security gap when key personnel leave the organization.

Technology: No-frills point tools in logical areas. Basic organizations implement pedestrian security technologies like firewalls, endpoint antivirus software, IDS/IPS, and perhaps log management tools. Advanced security features are eschewed for fear that they might impact performance or disrupt the business. Each tool is implemented and managed on its own with little to no interoperability across technology silos. Security monitoring is done on a sporadic basis and is skewed toward compliance reporting and auditing rather than situational awareness. This leaves basic organizations with visibility gaps between scans and no way to assess their overall security status across the entire organization.

Profile of Progressing Organizations

Over the last few years, the 60% of organizations making up the "progressing" segment have likely had some type of cybersecurity awakening. It's not unlikely that these firms experienced a security breach or witnessed a breach at another similar organization in their industry. Whatever the motivation, progressing organizations are much more serious about cyber risk than the basic crowd. These distinctions are exhibited in the following ways:

Philosophy: We need to get more engaged around cybersecurity. Progressing organizations recognize that cybersecurity issues can impact them at any time and cause an undue amount of harm. This leads to a number of proactive steps. First, cybersecurity risk issues reach a business level, although executive management and board members may not know much beyond the fact that they have to pay attention. Progressing companies are motivated to "do something" so they tend to proceed beyond incident prevention to incident detection by adding additional layers of security defenses and management tools. While this may lead to some security improvements, it can add overhead and additional operational complexity as well.

People: Establish a real cybersecurity group. Progressing organizations will typically have a CISO or similarly titled individual leading the security effort and reporting to a COO, risk officer, or other non-IT manager. While this person typically has a technology background, business executives willingly work with the CISO to bridge the business/cybersecurity divide.

The security team at progressing organizations tends to have good skills, and the ability to provide input and security oversight over the IT team. Nevertheless, there are communications issues where security is "out of the loop," especially with regard to new IT initiatives like cloud and mobile computing. While progressing organizations place an emphasis on infosec, they still find it difficult to recruit top talent, which translates into an IT security team that is over worked, understaffed, and lacking some critical skills.

Processes: Sort through confusion and finesse toward formal processes and automation. In spite of their commitment and enthusiasm, progressing organizations often make the mistake of adding new security technologies with little compensatory effort to re-engineer security processes. It is not unusual for progressing companies to improve processes based upon the skills and size of the security organization, but incremental progress is often diluted as progressing organizations implement more sophisticated hands-on security tools. Ultimately, security operations complexity becomes an issue as progressing organizations realize that they aren't able to capitalize on all of their new security technology capabilities. This ultimately leads to focused grassroots projects to document, formalize, and automate security processes.

Technology: Implement advanced tools at all costs. As previously mentioned, progressing companies move beyond the basics, get more engaged with the security capabilities of existing technologies, and dabble with newer tools. For example, progressing companies are more likely to enable real-time protection features in endpoint security software or build a hierarchical network architecture using VLANs, ACLs, and firewall rules. Progressing organizations also understand that security analytics should go beyond compliance reporting, so they are more likely to deploy SIEM, NBAD, or other types of tools. As part of the advancement from prevention to detection, progressing organizations are also likely to deploy some type of advanced malware gateway, albeit in passive mode only. Finally, progressing organizations often organize their personnel and security tools into some sort of SOC, although it may be nothing more than a common room for people and monitors. Progressing companies deserve kudos for their technology efforts, but they frequently discover that they are in over their heads sooner than anticipated.

Profile of Advanced Organizations

The remaining 10% of organizations can be considered "advanced" as they possess the best cybersecurity skills, resources, and technologies. It is important to note, however, that advanced organizations are often the most attractive targets for cyber adversaries, so they develop strong security hygiene and best practices because they have to. Advanced organizations are characterized as follows:

Philosophy: Cybersecurity is part of the organizational culture. Advanced organizations understand that security must be "baked-in" to business processes as they align more closely with IT. Consequently, business leaders and corporate boards are directly involved in IT risk assessment and cybersecurity strategy, while CISOs often report directly to the CEO and are treated as business executives rather than IT geeks. This may explain why CISOs at advanced organizations are passionate about making strong security a business enabler. Business leaders act as cybersecurity champions and all employees go through awareness training on a regular basis. While advanced organizations have the highest InfoSec budgets, they tend to remain diligent about the threat landscape and are willing to address new, unanticipated risks sooner rather than later. Finally, advanced organizations tend to manage cybersecurity with a series of metrics in order to gauge whether they are improving and if so, by how much.

People: The best and brightest—if we can find them. Advanced organizations recruit and hire the best talent they can find, from the CISO to junior administrators. They also pride themselves on creating the right work environment for cybersecurity professionals. For example, many advanced organizations are willing to invest in continuous education programs and give their top cybersecurity staff members leeway to work with industry ISACs, present at security conferences, and interact with engineers working for security technology partners. In spite of these organizational efforts, advanced organizations are impacted by the acute global cybersecurity skills shortage and still have difficulty recruiting and retaining security professionals. This may explain why advanced organizations are also the most aggressive when it comes to working with professional and managed providers for security services. CISOs at advanced organizations are smart enough to know when they need professional services for a particularly esoteric security skill set and when they can outsource mundane security tasks.

Processes: Strive for military precision. While progressing organizations realize that they need to do something about security complexity, advanced organizations are already

streamlining all they can. For example, many advanced organizations are focused on various workflows to improve collaboration between security and business managers on one hand, and the security team and IT on the other. Advanced organizations also realize that even the best and brightest security teams can't possibly keep up with the scale and scope of cybersecurity threats. Consequently, they are leaning on advanced intelligence and technology integration to help them automate processes for risk management and incident detection/response. Finally, advanced organizations collect and analyse as much data as possible so they can adjust their tactics and prioritize their workloads effectively and efficiency. They also use data analysis to gauge their performance and make improvements when needed.

Technology: Identity, integration, and data security. Like progressing organizations, advanced firms know they need new security technologies for defense-in-depth and security analytics. They too have SOCs, but they differ from progressing organizations in that they realize that additional point tools will solve old problems and create new ones simultaneously. To alleviate this conflict, advanced organizations are moving in a different direction by building an integrated security technology architecture that spans the enterprise. This type of architecture features central command-and-control, distributed enforcement, cloud-based threat intelligence, application-layer message exchange, and a massive data collection, processing, and analysis effort. Advanced organizations are also taking a leadership role in two other areas: identity and access management (IAM) and data security. On the IAM front, they are making identity a foundational component of security by using disparate identity attributes (i.e., user, role, device, network, location, time-of-day, etc.) to create and enforce granular access policies that can enable business processes while managing IT risk. Advanced organizations are also doubling down on data security to discover, classify, lockdown, and monitor their most sensitive and valuable data. This emphasis on IAM and data security is especially important as internal IT gives way to the dynamic and distributed worlds of computing.

The Bigger Truth

The ESG maturity model adopted by the researcher provides the financial sector with some guidelines on where they are today, where they need to go, and the best ways to proceed while avoiding inevitable detours. As a final thought, ESG offers these recommendations for basic, progressing, and advanced organizations:

Basic organizations should seek immediate help. Those basic organizations that "see the light" must realize that they are woefully behind and may be too far gone to dig themselves out of their cybersecurity holes alone. Rather than focus on InfoSec skills, basic organizations may be better served by working on their contract management and legal skills. Armed with these strengths, they should then seek out the best managed security service providers with industry knowledge and comprehensive coverage.

Progressing organizations need to think in terms of the big picture. Progressing organizations often face a paradoxical situation where they are so busy that nothing gets done. Rather than lots of starts and stops on tactical initiatives, progressing organizations must take the counterintuitive step of slowing down. Start with an assessment, some penetration testing, and an effort to align cybersecurity with business and IT initiatives. This should help identify some obvious weaknesses but the security team must remember to connect all the dots between technologies along the way. Finally, CISOs at progressing organizations must concentrate on process automation for attaining operational efficiency or all other efforts will be marginal at best.

Advanced organizations need a three-to-five year plan. In the 1990s, many enterprise organizations replaced departmental applications with integrated ERP systems. This effort was more difficult than many firms anticipated and was fraught with pitfalls, but those organizations that persevered were able to reap rich benefits in terms of business intelligence, agility, just-in-time supply chains, and automated business processes. ESG sees this situation as analogous to the current transition with enterprise security. CISOs need to recognize that cybersecurity technology integration won't be easy, but if done right, it will be well worth the effort. To proceed properly, large organizations should create a three- to five-year cybersecurity integration plan encompassing all aspects of their security technology. The plan should outlined with time frames and project phases as well as define milestones and metrics to assess progress. Project

objectives should adhere to what ESG calls the CISO triad: security efficacy, operational efficiency, and business enablement.

5.1 Conclusion

In today's technological and social environment, cybersecurity adoption and use is a very important part of a banking system. Business partners, suppliers, customers, and vendors require high cyber security assurance from one to another, particularly when providing mutual network and information access. Banks' ability to take advantage of new opportunities often depends on its ability to provide open, accessible, available, and secure network connectivity and services. Having a reputation for safeguarding information and the environment within which it resides enhances a bank's ability to preserve and increase market share. Recognizing this fact, this research work was aimed at assessing the current level of adoption and use of cyber security practices within the financial sector, and to propose viable solutions to the gaps within the sector. In this work, attempts were done to examine and compare the available cyber security frameworks and best practices. This research combines ISO frameworks, theories based on adoption and use of cybersecurity and researcher's own experience to assess the cyber security practices in banking industry. Both qualitative and quantitative research approach were used with majority of the focus being on the qualitative analysis due to the limitation in the sample size and sensitivity of the topic. Data collection was carried out by using tools like; questionnaire survey, document analysis, and interviews. To analyze the data SPSS tool and SATA were employed. To develop the Cyber Security Assessment scholars use different research approaches. Some scholars design their research in the following order: literature review Case study or Assessing Propose a conceptual Cyber Security tool (Are, 2007). Others follow: literature review Propose Cyber Security reviewed by professionals and tested in the real banking environment (Munirul et al., 2011). However, the student researcher employed the following approach; Literature review Assessment the level of cybersecurity adoption and use within the financial sector by using the ESG maturity model which allows organizations compare their capabilities to one another, and enables leaders make better well informed decisions about how to support progression and what investments to make in regards to the adoption and use of cyber security in the financial sector. Findings of the assessment based on the fact finding techniques employed, such as questionnaire survey, document analysis, and interviews, show

that current Cybersecurity management in the surveyed banks, generally lack a formalized comprehensive framework-based cyber security policy. The developed Cybersecurity measures for the banking system can be used as a starting point for banking sector to manage their security by developing guidelines and implementing controls to protect banking information assets from the threats identified in literature reviews.

The proposal has two major components for cyber security requirement identification mechanism which is the combination of assessments, and Cybersecurity maturity model with supporting template and counter measures (controls). Further, there are a few Cybersecurity frameworks and theories that guide adoption and used and they are identified in this research. And these further grouped under three categories which are Administrative, Technical, and Physical & Environmental security. The proposition is an integration of all available framework components discussed and derived from literature review as well as encompassing the proposed ESG cybersecurity maturity model so as to fully optimize the adoption and use of Cybersecurity within the financial sector. The suggested approach is based on the world standard theories and frameworks that are already being used in the banking sector both in the developing and developed countries. There is a need and urgency to have detailed policies and procedures formulation and comprehensive tests in the real banking environment if a framework is to be proposed and formulated. From the foregoing, it can be concluded that a framework based on the assessment results is valid and applicable in the banking industry to address the challenges related to cyber security. This can be seen in the future works and proposals of the research.

5.2 Recommendation

A cyber security maturity model can be adopted and used as an initial effort for technical specialists in the financial sector industry to manage and measure the level cybersecurity adoption and use. This as a result can be able to show the financial sector their current gaps and as a result provide them with a better understanding on how best to tackle the gaps noted through the adoption and use of Cybersecurity. The results from this research also imply further works for researchers and academicians.

5.3 For Future Researchers

- The Research can serve as a guideline for managers to formulate policies and procedures and come up with a suitable cyber security framework serving as a guideline for developers to develop cyber security systems and measures and thus enabling the financial sector have a common cyber security platform, so that experts can share skills and knowledge easily via body of knowledge.

5.3.1 Areas for Further Research

Some aspects of Cyber Security that are beyond the scope of this thesis research are recommended for future research. These are:

a. Look into how to measure security management effectiveness in the context of bank security strategy, and develop metrics to be used against security goals, and objectives.
b. Determine the impact level of trust, ethical conduct, and culture on the process of Cyber Security development and implementation in the world.
c. How do banks develop a Cybersecurity culture?
d. Enhancing the same research by considering all sectors and aspects of the Financial Sector.
e. Further detail research will be made on the identified areas that require policies and procedures

REFERENCES

Anderson, D.J. & Eubanks, G., Leveraging Coso across the Three Defense Lines.

Davis, O. and Pandey, A. (2015). *Hackers Steal $1 Billion In Biggest Bank Heist In History: Could They Take Down The Whole System Next Time?* [Online] International Business Times. Available at: http://www.ibtimes.com/hackers-steal-1-billion-biggest-bank-heist-history-could-they-take-down-whole-system-1818010.

Malakata, M. (2015). *Africa's effort to tackle cybercrime gains momentum*. [Online] PCWorld. Available at: http://www.pcworld.com/article/2981739/africas-effort-to-tackle-cybercrime-gains-momentum.html.

Clark, A. et al., 2014. Threats to the Financial Services Sector: Financial Services Sector

Analysis of PwC's 2014 Global Economic Crime Survey. *PWC*. Available at:

https://www.pwc.com/en_GX/gx/financial-services/publications/assets/pwc-gecs-2014-threats

to-the-financial-services-sector.pdf.

Schwartz, M. (2016). *Bangladesh Bank Attackers Hacked SWIFT Software*. [Online] Bankinfosecurity.com. Available at: http://www.bankinfosecurity.com/bangladesh-bank-attackers-hacked-swift-software-a-9061?rf=2016-04-25-eb&mkt_tok=eyJpIjoiT1dZNFl6RTBOMk5qTW1aayIsInQiOiJlQ3ZtRHcwTEJ6MUxodjNEQk83R1dOYmc5Wlk1RXFwTGh6VWJzSXpcL2VxUVo1XC9nQkdcL1duXC93QVlycnhzd0c2Rk9NUHZwdmMxXC92OTA2NThIZFA5MEoreWlKRlUxR2gyZ0Jid0VFbEVwWGVnPSJ9 .

Shevchenko, S. and $951m, T. (2016). *BAE Systems Threat Research Blog: Two bytes to $951m*. [Online] Baesystemsai.blogspot.ug. Available at: http://baesystemsai.blogspot.ug/2016/04/two-bytes-to-951m.html .

Banks likely to remain top cybercrime targets. (2012). 1st ed. [ebook] 350 Ellis St. Mountain View, CA 94043 USA: Symantec Corporation. Available at: https://www.symantec.com/content/en/us/enterprise/other_resources/b_Financial_Attacks_Exec_Report.pdf.

The Many Faces of Corruption Tracking Vulnerabilities at the Sector Level. (2007). 1st ed. [ebook] Washington Dc: The World Bank. Available at: http://actoolkit.unprme.org/wp-content/resourcepdf/399850REPLACEM101OFFICIAL0USE0ONLY1.pdf.

Oladipo, T. (2015). *Cyber-crime is Africa's 'next big threat', experts warn - BBC News*. [Online] BBC News. Available at: http://www.bbc.com/news/world-africa-34830724.

Ict.go.ug. (2016). *Infomation Security | Ministry of ICT*. [Online] Available at: http://www.ict.go.ug/initiative/infomation-security.

Nnanna, O. (2006). *Nigeria - 419 Coalition 2006 News on Nigerian Scam / 419 Operations*. [Online] 419coalition.org. Available at: http://www.419coalition.org/news2006.htm.

Ict.go.ug. (2016). *Infomation Security | Ministry of ICT*. [Online] Available at: http://www.ict.go.ug/initiative/infomation-security.

Theeastafrican.co.ke. (2016). *Hackers strike Bank of Uganda accounts, try to steal $24m*. [Online] Available at: http://www.theeastafrican.co.ke/news/Hackers-strike-Bank-of-Uganda-accounts-try-to-steal--24m/-/2558/3120684/-/mvpv40/-/index.html.

Ict.go.ug. (2016). *Laws & Regulations | Ministry of ICT*. [Online] Available at: http://www.ict.go.ug/initiative/laws-regulations.

Kai, G. and Schipke, A. (2015). *Financial Liberalization, Innovation, and Stability*. 1st ed. [ebook] China: International Monetary Fund. Available at: https://www.imf.org/external/np/seminars/eng/2015/PBC/ebook.pdf.

Karugaba, M. (2016). Sh28b wired to banks based abroad. *New Vision*, p.3.

Netlingo.com. (2016). *Cyberfraud - NetLingo The Internet Dictionary: Online Dictionary of Computer and Internet Terms, Acronyms, Text Messaging, Smileys ;-)*. [Online] Available at: http://www.netlingo.com/word/cyberfraud.php.

Techterms.com. (2016). *Cybercrime Definition*. [Online] Available at: http://techterms.com/definition/cybercrime#.

TheFreeDictionary.com. (2016). *Computer crime*. [Online] Available at: http://legal-dictionary.thefreedictionary.com/computer+crime.

Von Solms, R. and van Niekerk, J. (2013). *From information security to Cybersecurity*. 2nd ed. [ebook] Port Elizabeth 6031, p.1. Available at: https://www.researchgate.net/profile/Johan_Van_Niekerk2/publication/278325582_From_information_security_to_cyber_security/links/55e052e908aecb1a7cc39eb2.pdf .

Identity and Access Management Solution. (2005). 1st ed. [ebook] Amsterdam: *Interested in learning more about security? SANS Institute.* Available at: https://www.sans.org/reading-room/whitepapers/services/identity-access-management-solution-1640 .

Paganini, +. And Pierluigi Paganini is Chief Information Security Officer at Bit4Id, S. (2016). *Carbanak Cybergang is back and it is not alone*. [Online] Security Affairs. Available at: http://securityaffairs.co/wordpress/44342/cyber-crime/carbanak-2-cybergang-is-back.html .

allAfrica.com. (2016). *Uganda: Soldiers Named in Shs 200 Million Bank of Africa Bullion Van Heist*. [Online] Available at: http://allafrica.com/stories/201601190468.html.

Static6.businessinsider.com. (2016). [Online] Available at: http://static6.businessinsider.com/image/54e21cedeab8eab162e3dce1-960/screen%20shot%202015-02-16%20at%2011.36.33%20am.png

Bain.com. (2012). *The digital challenge to retail banks*. [Online] Available at: http://www.bain.com/publications/articles/digital-challenge-to-retail-banks.aspx.

Techcabal.com. (2016). *Shared passwords almost cost the Bank of Uganda 24 million dollars | TechCabal*. [Online] Available at: http://techcabal.com/2016/03/19/shared-passwords-almost-cost-the-bank-of-uganda-24-million-dollars/ .

Uganda Radio Network. (2016). *Soldiers involved in Bank of Africa Robbery*. [Online] Available at: http://ugandaradionetwork.com.dedi3883.your-server.de/story/4-updf-soldiers-involved-in-bank-of-africa-ugx200m-robbery.

Uganda Drone. (2015). *centenary bank forced into ATM crisis; millions feared lost*. [Online] Available at: http://drone.teratechuganda.com/hackers-force-ugandas-centenary-bank-into-atm-crisis-millions-of-shillings-feared-lost/ .

Waswa, S. (2014). *Centenary Bank Suspends All PINs Amid ATM Fraud Scandal*. [Online] http://www.chimpreports.com. Available at: http://www.chimpreports.com/centenary-bank-suspends-all-pins-amid-atm-fraud-scandal/ .

Mail Online. (2016). *Qatar National Bank 'hacked and data of hundreds of customers leaked'*. [Online] Available at: http://www.dailymail.co.uk/news/article-3561651/Qatar-National-Bank-hacked-data-ruling-family-national-intelligence-agency-Al-Jazeera-journalists-leaked-online.html.

PCI DSS Compliance. (2016). *Best Practice for Implementing PCI DSS in to Your Organization | PCI DSS Compliance*. [Online] Available at: http://pcidsscompliance.net/implementing-pci-dss/best-practice-for-implementing-pci-dss-in-to-your-organization/.

PCI DSS Quick Reference Guide Understanding the Payment Card Industry Data Security Standard version 2.0. (2010). 2nd ed. [ebook] Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.419.8070&rep=rep1&type=pdf .

SWIFT. (2016). *SWIFT comments on malware reports*. [Online] Available at: https://www.swift.com/insights/press-releases/swift-comments-on-malware-reports .

Thwarting Insider Threat at Financial Institutions. (2007). 1st ed. [ebook] Lexington: imprivata. Available at: http://f6ce14d4647f05e937f4-4d6abce208e5e17c2085b466b98c2083.r3.cf1.rackcdn.com/thwarting-insider-threat-for-financial-institutions-pdf-w-170.pdf .

Mutegi, L. (2015). *Cybercrime increasing across Africa's financial Sector due to digital explosion - CIO East Africa*. [Online] Cio.co.ke. Available at: http://www.cio.co.ke/news/main-stories/cybercrime-increasing-across-africa's-financial-sector-due-to-digital-explosion.

Susanto, H., Almunawar, M.N. & Tuan, Y.C., 2011. Information Security Management System Standards : A Comparative Study of the Big Five. , (October).

Anon, 2016. 1st Interview Noah_Baalessanvu.

Clark, A. et al., 2014. Threats to the Financial Services Sector: Financial Services Sector Analysis of PwC's 2014 Global Economic Crime Survey. *PWC*. Available at: https://www.pwc.com/en_GX/gx/financial-services/publications/assets/pwc-gecs-2014-threats-to-the-financial-services-sector.pdf.

Journal, I., Computer, A. & Ijact, T., a Technological Transformation in Banking Services : a Revolutionary. *International Journal of Advanced Computer Technology IJACT)*, (i), pp.69–73.

Framework, A., 2014. Cyber Essentials Scheme. , (June).

Processes, E. & Information, E., 2013. COBIT 5 Online Collaborative Environment Selected Guidance from the COBIT 5 Family.

Anon, 2003. CHAPTER 3 Research design and methodology. , pp.51–77.

Guldentops, E., 2011. Guest Editorial: Where Have All the Control Objectives Gone? *ISACA Journal*, 4, pp.6–9.

Frameworks, M.I., Integrated, G. & Cobit, I., 2012. Taking Governance Forward (TGF). , pp.1-2.

All, I., 2012. ISACA ® Journal. , pp.1–4.

Cycle, L. & Practices, G., 2013. : Enabling Processes. , pp.9–12.

ISACA, 2012. COBIT 5 Professional Guides.

Implementation, C., 2013. For Governance Objective : Value Creation COBIT 5 COBIT 5 Professional Guides COBIT 5 Online Collaborative Environment Selected Guidance from the COBIT 5 Family Processes for Governance of Enterprise IT Generic Process Capability Attributes.

Questions, F.A. & Questions, C., 2013. : Enabling Information.

Van Grembergen, W., Saull, R. & De Haes, S., 2004. Linking the IT balanced scorecard to the business objectives at a major Canadian financial group. *Strategies for information …*, p.27. Available at: http://books.google.com/books?hl=en&lr=&id=hWBtjNVnj8YC&oi=fnd&pg=PA129&dq=Linking+the+IT+Balanced+Scorecard+to+the+Business+Objectives+at+a+Major+Canadian+Financial+group&ots=wzjcBfqNRM&sig=pgQa3oxb4hnSittlBwEyQ5zbasQ.

Engineering, B.I.O., 2002. Addis Ababa University. *Orang utan Biology*, (February), pp.145–154.

Enterprises, M., 2015. No Title.

Information, C. et al., 2013. COBIT ® 5 Implementation — Supplemental Tools and Materials Table of Contents. , pp.2–4.

Anon, Cybersecurity : The changing role of audit committee and internal audit Contents.

Anon, 2016. 2nd Interview with Naturinda Hosea.

Anon, the data gap Cyber crisis in the insurance industry management : Readiness,response, and recovery.

Anon, Assessing cyber risk Critical questions for the board and the C-suite Risk powers. , pp.1–16.

Horváth, G.K., 2013. Information Security Management for SMEs: Implementing and Operating a Business Continuity Management System (BCMS) Using PDCA Cycle. *Proceedings of FIKUSZ*, pp.133–141.

Deloitte (2014), Transforming cybersecurity new approaches for an evolving threat landscape for Financial Services.

Gorra, A., 1999. Chapter 3 Research Methodology Grounded theory methodology - an overview. *PHD - Grounded Theory*, pp.86–115. Available at: http://www.leedsbeckett.ac.uk/inn/alic/agorra/3_Chapter3_Methodology_AndreaGorra.pdf.

James, W., Doyle, T. & Rex, B., 2005. *P s y c h o l o g y*,

Jones, C.M. et al., 2010. Utilizing the Technology Acceptance Model to Assess the Employee Adoption of Information Systems Security Measures. *Issues in Information System*, XI (1), pp.9–16.

ITU, 2013. 2013 ITU survey on measures taken to raise awareness on cybersecurity. , (August), pp.1–27. Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/22survey.pdf.

Rowe, B.R., 2006. Private Sector Cyber Security Investment Strategies: An Empirical Analysis *. , (April), pp.1–23.

Salman, A. et al., 2014. ICT acceptance among Malaysian urbanites: A study of additional variables in user acceptance of the new media. *Malaysian Journal of Society and Space*, 6(6), pp.86–96.

Selamat, Z., Jaffar, N. & Abd Kadir, H., 2011. ICT Adoption in Malaysian SMEs. In *Management and Service Science*. pp. 135–139. Available at: <Go to ISI>://WOS:000303218400025.

Apulu, I., 2012. Developing a Framework for Successful Adoption and Effective Utilisation of ICT by SMEs in Developing Countries: a Case Study of Nigeria. , (February), pp.3–369. Available at: http://wlv.openrepository.com/wlv/handle/2436/249899.

Integrated, A. et al., 2013. Malaysia' S National Cyber Security Policy. *An Integrated Approach for Cyber Security and Critical Information Infrastructure Protection*, (September).

Kong, H., 2004. Research Methods. *Notes on Research Methods*, pp.44–49. Available at: http://nccur.lib.nccu.edu.tw/bitstream/140.119/33962/6/33021106.pdf.

NHTSA, 2014. A Summary of Cybersecurity Best Practices. , (October). Available at: http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash Avoidance/Technical Publications/2014/812075_CybersecurityBestPractices.pdf.

Pagani, M., 2006. Determinants of adoption of High Speed Data Services in the business market: Evidence for a combined technology acceptance model with task technology fit model. *Information and Management*, 43(7), pp.847–860.

Poon, W., 2007. Users' adoption of e-banking services: the Malaysian perspective. *Journal of Business & Industrial Marketing*, 23(1), pp.59–69. Available at: http://www.emeraldinsight.com/10.1108/08858620810841498.

Security, H., 2016. Financial Services Sector Coordinating Council.

Turner, D. et al., 2013. N12429 n112429.

Wu, M.Y. et al., 2011. TAM2-based study of website user behavior-using web 2.0 websites as an example. *WSEAS Transactions on Business and Economics*, 8(4), pp.133–151.

Zaremohzzabieh, Z. et al., 2015. A Test of the Technology Acceptance Model for Understanding the ICT Adoption Behavior of Rural Young Entrepreneurs. *International Journal of Business and Management*, 10(2), pp.158–169. Available at: http://search.proquest.com/docview/1657330771?accountid=44542\nhttp://search.proquest.com/docview/1657330766?accountid=44542.

Adesina, A.A. & Ayo, C.K., 2010. An empirical investigation of the level of users' acceptance of e-banking in Nigeria. *Journal of Internet Banking and Commerce*, 15(1), pp.1–13.

Amrin, N., 2014. The Impact of Cyber Security on SMEs. Available at: http://eprints.eemcs.utwente.nl/24978/.

Council, D.P., 2012. Uganda medical and dental practitioners council, P. O. Box 16115, Kampala tel/fax 256 41 345844. , pp.1–5.

Darnton, A., 2010. "Methods and Models" Andrew Darnton at the Lancaster Working PARTY! #2 6th January 2010. *Economic Theory*, (January).

Feily, M., Shahrestani, A. & Ramadass, S., 2009. A survey of botnet and botnet detection. In *Proceedings - 2009 3rd International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2009*. pp. 268–273.

Lule, I. ; Omwansa tonny K. & Mwololo Waema, T., 2012. Application of Technology Acceptance Model (TAM) in M-Banking Adoption in Kenya. *International Journal of Computing and ICT Research*, 6(1), pp.31–43.

PWC, 2014. Framework. , (May). Available at: pwc.com/cybersecurity.

Harris, S., 2013. *All in one CISSP*,

Kim, Y. & Crowston, K., 2011. Technology adoption and use theory review for studying scientists' continued use of cyber-infrastructure. In *American Society for Information Science and Technology Annual Meeting*. pp. 1–14.

Pwc, 2013. UK CYBER SECURITY Research Report - Survey. , (November), p.105.

Waema, P.T.M. & Omwenga, B., 2014. Cloud Computing in Kenya University of Nairobi. , (April).

Anon, 1993. CH.3. methodology. , pp.22–30.

Anon, 2014. Department of Homeland Security Cybersecurity Capability Maturity Model White Paper.

Anonymous, 2012. Cybersecurity Policy Making at a Turning Point. *OECD Digital Economy Papers*, (211), pp.0_1, 2, 4–56. Available at: http://search.proquest.com.library.capella.edu/docview/1223514107?accountid=27965\nhttp://wv9lq5ld3p.search.serialssolutions.com.library.capella.edu/?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ABI/INFORM+Global&rft_val_fmt=info:ofi/f.

Colias, M., 2004. Cyber security. *HOSPITALS & HEALTH NETWORKS*, 78(5), p.60+.

CREST, 2014. A Guide to the Cyber Essentials Scheme. Available at: http://www.crest-approved.org/wp-content/uploads/Crest-Cyber-Essentials-Guide-final.pdf.

Framework, I., 2015. COSO & Cybersecurity.

Galligan, M.E., Rau, K. & Deloitte, 2015. *COSO in the cyber age*, Available at: http://www.coso.org/documents/COSO in the Cyber Age_FULL_r11.pdf.

Iiroc, F. & Members, D., Cybersecurity Best Practices Guide for IIROC Dealer Members.

Sagar, T., 2014. The Critical Security Controls for Effective Cyber Defense. , p.106.

Anon, 2015. White Paper the Chicago School of. , (July).

Computing, C., 2016. Cloud Computing - Cyber Security Challenges for the Financial Sector Standards in the Cloud Area.

Cyber, D. & Management, R., 2015. Cybersecurity Maturity. , (June), pp.19–57.

Dhillon, G. & Backhouse, J., 2001. Current directions in IS security research : towards socio-organizational perspectives. *Information Systems Journal*, 11(1), pp.127–153. Available at: http://disc.brunel.ac.uk/isj/.

E&Y, 2015. Cybersecurity and the Internet of Things. *E&Y*, (March).

Framework, J. & Title, J., Health Financing Voucher Manager Health Financing Voucher Manager.

Falessi, N. (ENISA) et al., 2012. National Cyber Security Strategies - Practical Guide on Development and Execution. , (December), p.45.

Leather, A. & Consultant, S., 2014. Cyber Security in Critical National Infrastructure Today's Presenter. , (August).

Minami, J. et al., 2010. Factors Influencing the Adoption and Usage of Online Services in Saudi Arabia. *The Electronic Journal on Information Systems in Developing Countries*, 14(12), pp.1421–1425.

Ssewanyana, J. & Busler, M., 2007. Adoption and usage of ICT in developing countries: Case of Ugandan firms. (Undetermined). *International Journal of Education & Development using Information & Communication Technology*, 3(3), p.49B–59. Available at: http://search.ebscohost.com/login.aspx?direct=true&db=eue&AN=508006029&site=ehost-live&scope=site.

Sherman, P., 2006. Preventative Maintenance (PM).

Security, I.F., Interested in learning SANS Institute InfoSec Reading Room Improving Firewall Security post Acquisition l r.

Keung, H., 2006. Information Security Controls. , 86(2), pp.1–3.

Interest, C.O.F., Sample 1. , pp.1–9.

Journal, G., Business, O.F. & Evans, O., 2008. Ict and Nigerian banks reforms: analysis of anticipated impacts in selected banks. , 2(2), pp.67–76.

Master, E., Kent, K. &Ph., D., 2008. Guidelines for Writing a Thesis or Dissertation. *Writing*.

Niang, I., Scharff, C. & Wamala, C., 2014. *Conference on M4D Mobile Communication for Development*, Available at: http://kau.diva-portal.org/smash/get/diva2:709233/FULLTEXT03.pdf.

Tshinu, S. M., Botha, G., and Herselman, M., 2008. An Integrated ICT Management Framework for\nCommercial Banking Organisations\nin South Africa. *Interdisciplinary Journal of Information, Knowledge, and Management*, 3.

Anon, Industry Letter - Thematic Review of Cyber-Security and Operational Risk.pdf.

Anon, H139963.pdf.

Byron, Lord & Green, H.S., 38 ©1981–2004,

Kerian, K., 2014. Authorised Signature. , p.16150.

Longe, O. et al., 2010. Information & Communication Technology Adoption among Adults in South Western Nigeria: An Assessment of Usage-Phobia Factors. *Journal of Information Technology Impact*, 10(1), pp.65–86.

Point, D., Report İso 27032.

Requirements, Q., 2012. International Standard Iso / Iec. , 25021.

Robinson, J., 2010. Triandis' theory of interpersonal behaviour in understanding software piracy behaviour in the South African context. , 2008(2009), pp.1–108. Available at: http://hdl.handle.net/10539/8377.

Samah, 2011. Can Technology Acceptance Model be applied on the Rural Setting: The Case of Village Development and Security Committee in Malaysia?*Journal of Social Sciences*, 7(2), pp.113–119.

Systems, K.B., 1965. Cyber Security and Threat Detection.

Melorose, J., Perroy, R. & Careas, S., 2015. No Title No Title. *Statewide Agricultural Land Use Baseline 2015*, 1, pp.48–70.

Crabbe, M. et al., 2009. An adoption model for mobile banking in Ghana. *International Journal of Mobile Communications*, 7(5), pp.515–543.

Onut, S., Erdem, I. & Hosver, B., 2008. Customer Relationship Management in Banking Sector and a Model Design for Banking Performance Enhancement. In *Unifying Themes in Complex Systems IV*. pp. 370–378. Available at: http://link.springer.com/10.1007/978-3-540-73849-7_41.

Fulfillment, W.O. & Overview, L., 2006. Online File W10. 1 Order Fulfillment and Logistics — an Overview Order Fulfillment and the Logistics Process. , pp.1–14.

Idowu, H.A., 2014. MASTER' S THESIS Security Awareness and Challenges in VoIP Technology.

Keogh, M., 2012. NARUC. , (June).

Lallmahamood, M., 2007. An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia and the Influence of This on Their Intention to Use E-Commerce : Using An Extension of the Technology Acceptance Model. *Journal of Internet Banking and Commerce*, 12(3), pp.1–26. Available at: http://arraydev.com/commerce/JIBC/2007-12/Muniruddeen_Final.pdf.

Luka, M.K. & Frank, I.A., 2012. The Impacts of ICTs on Banks a Case study of the Nigerian Banking Industry. *International Journal of Advanced Computer Science and Applications*, 3(9), pp.145–149.

Mary, B. et al., 2014. Privacy and Information Governance NIST Releases First Cybersecurity Framework, but Questions Remain for Implementation.

Miron, W., 2015. Adoption of Cybersecurity Capability Maturity Models in Municipal Governments.

Technology, C., Efficiency, C. & Africa, S., 2014. The impact of information and communication technology (ICT) on commercial bank performance : evidence from South Africa. *Problems and Perspectives in Management*, 12(3), pp.59–68. Available at: http://businessperspectives.org/journals_free/ppm/2014/PPM_2014_03_Binuyo.pdf.

Infrastructure, E.S.T., E-Commerce Systems Technology Infrastructure.

Ponemon Institute LLC, 2015. 2015 Global Megatrends in Cybersecurity. , (February).

Reports, V.I. et al., NIST Cyber Security Framework And IT Operations staff By Henry Amadi , CISSP , CISRCP , MSc CSF IDENTIFY (ID) CORE FUNCTION By Henry Amadi , CISSP , CISRCP , MSc.

Ricker, B.F.R. & Kalakota, R., 1995. The Hidden Key to e-Commerce Success.

Roos, C.J., 2012. Governance responses to hacking in the banking sector of South Africa : an exploratory study. Available at: https://ujdigispace.uj.ac.za/handle/10210/8642.

Upton, D.M. & McAfee, A.P., 2000. A path-based approach to information technology in manufacturing. *International Journal of Technology Management*, 20, p.354.

Biggam, J., 2012. Succeeding with your Master's Dissertation: A step-by-step handbook. , p.116.

Institute, S., 2004. Interested in learning SANS Institute InfoSec Reading Room In too, anll r go. *Worm Propagation and Countermeasures*, p.36.

Li, H. & Lee, K.C., 2010. Behavior participation in virtual worlds: A Triandis model perspective. *PACIS 2010 - 14th Pacific Asia Conference on Information Systems*, pp.950–961.

Wang, W. & Lu, Z., 2013. Cyber security in the Smart Grid: Survey and challenges. *Computer Networks*, 57(5), pp.1344–1371. Available at: http://dx.doi.org/10.1016/j.comnet.2012.12.017.

Agboola, A., 2007. Information and Communication Technology (ICT) in Banking Operations in Nigeria – An Evaluation of Recent Experiences. *African Journal of Public administration and Management*, XVIII (1), pp.1–21.

Created, C.F., 2015. Some Cyber Security Frameworks are based on rigid processes of the past – prone to failure. Some Cyber Security Frameworks are based on antiquated control frameworks of the past – prone to failure. Definition of nexus : a relationship or. , pp.2014–2016.

Egmond, C. & Bruel, R., 2007. Triandis' Theory of Interpersonal Behaviour. *Analysis of theories and a tool for developing interventions to influence energy-related behaviour*. Available at: http://www.cres.gr/behave/pdf/paper_final_draft_CE1309.pdf\nhttp://www.cres.gr/behave/pdf/Triandis_theory.pdf.

Framework, T. & Clear, P., 2014. The Cybersecurity Framework in Action : An Intel Use Case. *Intel*.

Kallioranta, S.M. & Vlosky, R.P., 2004. A Model of Extranet Implementation Success Effects on Business Performance.

Sector, S. & Itu, O.F., 2015. ITU-T.

Banking, I., 2006. Regulating Internet Banking In Nigeria : Some Success Prescriptions – Part 2. , 11(1), pp.1–13.

Choejey, P. et al., 2015. Cybersecurity Practices for E-Government : An Assessment in Bhutan. *The 10th International Conference on e-Business (iNCEB2015)*, pp.1–8.

Example, G., 2014. Chapter 7 : Linear Momentum and Collisions. , pp.1–30.

Kaya, M.M., 2013. Trust and Security Risks in Mobile Banking. , (March).

Sohrabi Safa, N., Von Solms, R. & Furnell, S., 2016. Information security policy compliance model in organizations. *Computers and Security*, 56, pp.1–13. Available at: http://dx.doi.org/10.1016/j.cose.2015.10.006.

Udotai, B., 2005. Securing the "WEAKESTLINK" of the.

Coyle, M., Wolcott, R. & Gittleman, S., Cyber Crime : the Fast-Moving Menace — a Special Report Reporting Team.

Kumar, V. et al., 2007. Factors for successful e-government adoption: a conceptual framework. *Electronic Journal of E-government*, 5(1), pp.63–76. Available at: http://issuu.com/academic-conferences.org/docs/ejeg-volume5-issue1-article89.

Von Solms, R. & van Niekerk, J., 2013. From information security to cyber security. *Computers & Security*, 38, pp.97–102. Available at: http://dx.doi.org/10.1016/j.cose.2013.04.004.

Hoffman, L.J., Heller, R. & Conference, S.M.A., 2016. Exploring Ways to Give Engineering Cyber Security Students a Stronger Policy and Management Perspective Costis Toregas Exploring Ways to Give Engineering Cyber Security Students a Stronger Policy and Management Perspective. , pp.1–13.

Horne, R., 2014. The cyber threat to banking Foreword. *PWC*. Available at: https://www.bba.org.uk/wp-content/uploads/2014/06/BBAJ2110_Cyber_report_May_2014_WEB.pdf.

Tobergte, D.R. & Curtis, S., 2013. No Title No Title. *Journal of Chemical Information and Modeling*, 53(9), pp.1689–1699.

Castel, M.E., 2012. International and Canadian Law Rules Applicable to Cyber Attacks by State and Non-State Actors. *Canadian Journal of Law and Technology*.

Larson, S., The Cyber Security Fair : An Effective Method For Training Users To Improve Their Cyber Security Behaviors ? , 2(1), pp.11–19.

Shaji. N. Raj, 2015. Evaluation of Cybercrime Growth and Its Challenges as Per Indian Scenario. *International Journal of Informative & Futuristic Research*, 2(9), pp.3120–3128.

Anon, Map of Carbanak Targets.

Bouwman, H. et al., 2005. *Information and Communication Technology in Organizations: Adoption, Implementation, Use and Effects*,

ISO/IEC, 2013. ISO/IEC 27002:2013.pdf. *Iec*, 2013, p.90. Available at: www.iso.org.

Protiviti - Risk & Business Consulting Internal Audit, 2013. The Updated COSO Internal Control Framework: Frequently Asked Questions (second edition). , p.29. Available at: www.protiviti.com/en-US/Documents/Resource-Guides/Updated-COSO-Internal-Control-Framework-FAQs-Second-Edition-Protiviti.pdf.

Store, R.I.S.O., 2013. ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements. , 2013.

Anderson, D.J. & Eubanks, G., Leveraging Coso across the Three Defense Lines.

House, C. et al., Licensed commercial banks in Uganda. , pp.1–4.

Bode, P., CHAPTER 2 QUALITY ASSURANCE AND QUALITY CONTROL.

Control, Q., QUALITY ASSURANCE AND QUALITY CONTROL. , pp.1–17.

Valenzuela, D. & Shrivastava, P., Interview as a Method for Qualitative Research.

WP, E.D.S.P. & Deliverable, E.D., SECUR-ED Cyber-security roadmap for PTOs.

Anon, COBIT Framework.

Anon, COBIT5-ExecSummary.

Anon, Certificate in e-Governance and Cyber Security Cyber Attacks and Counter Measures : User Perspective.

Anon, Thwarting Insider Threat at Financial Institutions.... Before it's Too Late.

Garsoux, M., COBIT 5 ISACA's new framework for IT Governance, Risk, Security and auditingan overview.

Hunstad, N.L., 2011. Small Businesses and Organizations this page intentionally left blank.

Portable, F.O.R. & Video, H.D., FOR PORTABLE HD VIDEO CALLING AND.

Reich, J., Ph., D. & Webster, J., 2004. Quality Control Measures. , pp.1–12.

Response, S., 2016. Financial threats 2015.

Saint-Germain, R., Information Security Management Best Practice Based on ISO/IEC 17799.

Threat, I. & Guidance, M., Interested in learning SANS Institute InfoSec Reading Room.

Anon, Quality control methods for medicinal plant materials World Health Organization Geneva.

Ag, B., 1998. Quality Assurance for Research and Development and Non-routine Analysis Quality Assurance for Research and Development and Non-routine Analysis. , (November).

Eloff, J.A.N., 2003. Information Security Management – A New Paradigm. , pp.130–136.

Fox, A.C., Architect, B.T.E. & Warfare, C., 2015. Breaking the banks;the threat landscape in the financial sector.

Miller, R. & Maxim, M., 2015. I Have to Trust Someone. … Don't I ? Dealing with insider threats to cyber-security. , (January).

Anon, L05_DataQualityControlAssurance.

Anon, COBIT5-Introduction.

Humphreys, E., Heath, M. & Ip, S., 2008. Information security management standards : Compliance, governance and risk management. *Information Security Technical Report*, 13(4), pp.247–255. Available at: http://dx.doi.org/10.1016/j.istr.2008.10.010.

Nicho, M. &Ph., D., 2013. Using COBIT 5 for Data Breach Prevention. , 5, pp.1–8.

Personnel, P. et al., 6 quality control procedures.

Sureview, T. & Threat, I., The Financial Industry and the Insider Threat : Total Awareness Leads to Secured Enterprise.

Technology, I., Technikon, P.E. & Elizabeth, P., Information security management : why standards are important. , pp.50–57.

Anon, 2015. The comparison qualitative and quantitative research 1. , 5, pp.1111–1117.

Anon, COBIT5-and-GRC.

Yan, Y. et al., 2012. A Survey on Cyber Security for Smart Grid Communications. *IEEE Communications Surveys and Tutorials*, 14(4), pp.998–1010.

Clark, A. et al., 2014. Threats to the Financial Services Sector: Financial Services Sector Analysis of PwC's 2014 Global Economic Crime Survey. *PWC*. Available at: https://www.pwc.com/en_GX/gx/financial-services/publications/assets/pwc-gecs-2014-threats-to-the-financial-services-sector.pdf.

Sahlfeld, M., 2007. How does ICT work for development? A review of the challenges and opportunities. *ATDF Journal*, pp.22–36. Available at: http://atdforum.org/IMG/pdf_ICT_works_for_development_Sahlfeld.pdf.

NISP, 2014. National Information Security Policy

_____.

Market, C.S., 2012. Cyber Security Market in India September 2012 Executive Summary. , (September).

Anon, 2014. Cybersecurity-Framework-021214.

Guide, R. & Executives, B., CYBERSECURITY A Resource Guide for BANK EXECUTIVES Executive Leadership of Cybersecurity.

APPENDIX

AppendixI:Online Questionnaires

Dear respondent,

My name is Elizabeth Busingye, I am pursuing my masters in ICT Management, Policy and Architectural Design from Uganda Martyrs University. I am currently carrying out a survey to evaluate the Adoption and Use of Cyber Security in the Financial Sector in Developing Countries.

Your organization is one of the few that were selected for this research so as to help determine the gaps within the ICT department of your organization.

As well as come up with possible solutions to help improve the ICT department and in turn promote strategic alignment and growth between the ICT department and the business.

Your response to this survey will be highly appreciated.

Best wishes

Elizabeth Busingye

ICT Questionnaire

Evaluating the state of cyber security Adoption and Use within the Ugandan Financial Sector for Information Assurance Improvement.

1. What is your sex?

Male

Female

2. What vertical market best describes your Organization?

Banking Sector

Microfinance Sector

Telecom sector

3. Is your company a:

Small to Medium-sized business (i.e., 1-500 employees)

Mid-sized enterprise (i.e., 500-1000 employees)

Large enterprise (1000+ employees)

4. What is your Title in the organization?

Executive (CEO, VP, Managing Director)

Management

Operations

Other: _____

5. How many people do you have in your ICT department employ?

1-2
3-5
6-10
11-15
>15

6. Have you suffered a breach in the last 15 months (Multiple answers possible)?
Malware
Phishing
Virus attacks
Hacker attacks
Weaknesses highlighted during testing
Information not available
Lost Assets (Lost/ stolen laptops and ICT equipment)
We were not exposed to any form of hacking
Other

7. Does your organization adhere to the IT process or Security frameworks and / or standards, and if so, which ones (multiple answers possible)?
Yes, ISO/IEC 27000
Yes, COBIT
Yes, ITIL
Yes, COSO
Yes, NIST
Yes, PCI
Yes, regulatory standards
Yes, Parent organization standards
No
Other

8. How secure do you think your organization's network is?

Sufficiently Secure
Secure to a certain extent
Information not available
Not secure
Highly secure

9. Which of the following (policies and procedures) has your organization documented and approved (multiple answers possible)?

Cyber incident response plans
Information security roadmap
Business Continuity plans
Not developed but due to be developed over the next 12 months
Information security governance structure
Information security strategy
None of the above

10. Does your organization have a (dedicated) department responsible for cyber security?

No
Yes, dedicated department / Unit
Yes, but as part of another department (IT or internal Control department)

11. Does your organization have a chief Information Security Officer?
Yes
No

12. If yes, who does your Chief Information Security Officer report to?

Chief Information Officer
Chief Financial Officer
Chief Executive Officer
Board of Directors
We do not have a Chief Information Security Officer
Reports not available
Other

13. What has raised your awareness of cyber security attacks (multiple answers possible)?

Presentations and discussions at conferences
Publications in magazines, Newspapers, on websites and mailing lists
Legal and / or regulatory requirements
The infrastructure of our organization was under attack
Clients of our organization were attacked
Other

14. How do you keep informed of new forms of cyber security attacks and threats (Multiple answers possible)?

To date, there is no way our organization can trace cybercrime promptly, but we consider this question
Consulting firms / external consulting
Specific publications
Providers (Vendors)
Social Network /media
Security Conferences
Mailing Lists
Other

15. What do you think will help improve your organization's cyber security levels (multiple answers possible)?

Advanced security technology
ICT steering committees
Employee reward/ disciplinary systems
Vulnerability Assessment and Penetration Testing
Better employee security awareness
Increased ICT security department staff numbers
Larger budgets
Senior Management commitment
Continuous Skills Training
Other

16. What do you consider to be your greatest cyber security risk (multiple answers possible)?
Uncontrolled portable devices
Incorrect configuration
Bring your own device (BYOD)
Internet downloads
Malware
E-mail viruses
Hacking attempts by hackers
Insider attackers / Insider threat
Other

17. Which cyber security measures has your organization implemented (multiple answers possible)?
Firewalls
Antivirus setup
Anti-spam/ spyware/ Phishing solutions

Intrusion Detection Systems / Intrusion Prevention systems
Vulnerability Management
Data Loss Prevention/ file encryption (memory)
Safety endpoints
Management event logs (solutions SIEM)
Other

18. What measures do you usually take to mitigate cyber security attacks targeted at your organization's infrastructure / customers (multiple answers possible)?
Access Control Lists / Packet filters
Source-based remote-triggered blackholes
Intrusion prevention systems
Firewalls
Information not available
Destination-based remote-triggered blackholes
Other

19. What tool does your organization use to detect attacks (multiple answers possible)?
Open Source software
Self-developed tools
Commercial products
Information not available
Other

20. Does your organization provide employee training to raise cyber security awareness

No
Yes, other training
Yes, but only where mandated by law/ regulations
Yes, through general training
Yes, according to job role and function

21. How difficult is it, in your opinion, to convince management to invest in security solutions?

Very Difficult
Somewhat difficult
Easy
Very easy
Information not available

22. What percentage of your IT – budget was spent on security in the last 12 months?
0-10%
11-30%
31-50%
More than 50%
Information not available

23. Can you describe year-to-year spending in terms of your cyber /information security budget?
Budget increased
Budget has not changed
Budget was reduced
No information security budget was allocated
Information Not available

24. How does your organization ensure an adequate and appropriate level of cybersecurity over third parties (multiple answers possible)?
Signs confidentiality and / or non-disclosure agreements
Regularly monitors and reviews third party services
Requires independent attestation (e.g. NIST, ISO/IEC, COSO, PCI).
Performs random spot checks of third-party sites.
Controls third-party access to systems and data
Where permitted, performs background verification checks on selected high-risk

Imposes corporate security policy and controls on third parties

Addresses Information security issues in a contract

Identifies risks related to third parties as part of Information risk assessment

Information not available

Not applicable

Others

25. How confident are you in the cyber security practices of your third parties?

Not confident

Confident to a certain extent

Confident

Very confident

Not applicable

26. Does your organization share information on cyber security attacks with third parties?

Yes

No

Not applicable

27. Does your organization have technical ability to perform network-wide deep-packet inspections?

Yes

No

Information not available

28. How do you highlight cyber security weakness, risks and non-compliance in your organization (multiple answers possible)?

Input from peers

Vulnerability assessment and Penetration testing

Internal audit

External audit

Informal risk analysis

Formal risk analysis

Input from vendors

Assessment of regulatory (non) compliance

Others

Not applicable

29. Has vulnerability Assessment and Penetration Testing ever been performed in your organization?

No

Yes, by internal staff

Yes, by external staff

Information not available

PERSONNEL SECURITY (HR)

Evaluating the state of cyber security Adoption and Use within the Ugandan Financial Sector for Information Assurance Improvement.

1. What is your sex?

Male

Female

2. What vertical market best describes your Organization?

Banking Sector

Microfinance Sector

Telecom sector

3. Is your company a:

Small to Medium-sized business (i.e., 1-500 employees)

Mid-sized enterprise (i.e., 500-1000 employees)

Large enterprise (1000+ employees)

4. What is your Title in the organization?

Executive (CEO, VP, Managing Director)

Management

Operations

Other: _____

5. How many people does your institution employ in the ICT department?

1-2

3-5

6-10

11-15

>15

6. Does your organization require all employees to accept their set roles and responsibilities formally given by the institution?

Yes

No

7. If Yes, what does the acceptance include (multiple answers possible)

Signing acknowledgement letters of the job description and the roles and responsibilities.

Signing acknowledgement letters of the policies and manuals provided to the staff by the organization.

Other _____

8. Does your financial Institution ensure that individuals agree and abide by all organizational policies, standards, protocols and guidelines for protecting information, personnel and physical assets against security threats regardless of type of origin?

Yes

No

9. Does your financial institution confirm that, as part of the HR process all employees, accessing and/ or operating critical infrastructure sign declaration forms acknowledging their obligation to abide by related laws during and after their employment.

Yes

No

10. Does your organization ensure that HR processes do not allow anyone to commence work on critical infrastructure projects without undergoing appropriate recruitment checks and the necessary training?

Yes

No

11. Does your organization verify the identity of the candidate by conducting independent checks using government or third party issued documents such as passports or similar photographic identity documents.

Yes

No

12. Does your organization establish whether the applicant has the right to work in Uganda including meeting residency requirements based on the sensitivity of the position.

Yes

No

13. Does your department check the candidate's employment record validating the completeness and accuracy of the curriculum vitae?

Yes

No

14. Does your department obtain satisfactory character references about the applicant for example; one business and one personal?

Yes

No

15. Is your department able to establish whether the applicant is qualified for the job they applied for by confirming the claimed academic and professional qualifications?

Yes

No

16. Based on risk assessment, is your department able to determine whether the applicant is liable to undergo additional vetting depending on how critical the job they have applied for is?

Yes

No

17. Does your department maintain an up to date personnel records file of all staff/ employees of the organization?

Yes

No

18. Does the human resource department ensure that security clearances undergo regular review and / or when material facts or changes come to light to ensure that records are updated and re-affirm the individual's suitability to hold a security clearance at a given level.

Yes

No

19. Does the Human Resource Department submit individuals to pro-active appraisals, annually and / or when circumstances dictate, during which the vetting subject shall declare changes in professionals and personal circumstances and any security concerns that might materially affect their suitability to retain security clearance at a given level?

Yes

No

20. If yes, how often does your organization carry out these appraisals.

3 months

4 months

5 months

6 months

Other _____

21. As a consequence of a cybersecurity incident has there been and investment in cyber security recently in the last six months? If so, which kind of investment (Multiple answers possible)

Recruiting more skilled people
Investing in training for staff
Investing in new technical controls
Co-sourcing to obtain required skills
Investing in managed security service
Investing in the development of internal security operations center
Outsourcing to obtain required skills
No Change

Finance Questionnaire

Evaluating the state of cyber security Adoption and Use within the Ugandan Financial Sector for Information Assurance Improvement.

1. What is your sex?

Male

Female

2. What vertical market best describes your Organization?

Banking Sector

Microfinance Sector

Telecom sector

3. Is your company a:

Small to Medium-sized business (i.e., 1-500 employees)

Mid-sized enterprise (i.e., 500-1000 employees)

Large enterprise (1000+ employees)

4. What is your Title in the organization?

Executive (CEO, VP, Managing Director)

Management

Operations

Other: _____

5. What percentage of your IT – budget was spent on security in the last 12 months?

0-10%

11-30%

31-50%

More than 50%

Information not available

6. Can you describe year-to-year spending in terms of your cyber /information security budget?

Budget increased

Budget has not changed

Budget was reduced

No information security budget was allocated

Information Not available

7. Does the finance policy stipulate the way forward in case of a cyber-attack on the institution?

Yes

No

8. If Yes, Kindly highlight the steps that are taken by the finance department interms of incident response management after an attack has occurred?

_____

_____

_____

_____

_____

_____

_____

_____

9. Are the cyber incident scenarios incorporated in the financial institution's

business continuity and disaster recovery plans?

Yes

No

10. Have the above Scenarios incorporated in the disaster recovery plans been tested?

Yes

No

11. How secure do you think your organization's network is?

Sufficiently Secure

Secure to a certain extent

Information not available

Not secure

Highly secure

12. As a consequence of a Cybersecurity incident has there been and investment in cyber security recently in the last six months? If so, which kind of investment (Multiple answers possible)

Recruiting more skilled people
Investing in training for staff
Investing in new technical controls
Co-sourcing to obtain required skills
Investing in managed security service
Investing in the development of internal security operations center
Outsourcing to obtain required skills
No Change

13. What is the main driver for information security expenditure?

Audit Questionnaire

Evaluating the state of cyber security Adoption and Use within the Ugandan Financial Sector for Information Assurance Improvement.

1. What is your sex?
Male

Female

2. What vertical market best describes your Organization?
Banking Sector

Microfinance Sector

Telecom sector

3. Is your company a:

Small to Medium-sized business (i.e., 1-500 employees)

Mid-sized enterprise (i.e., 500-1000 employees)

Large enterprise (1000+ employees)

4. What is your Title in the organization?

Executive (CEO, VP, Managing Director)

Management

Operations

Other: _____

5. Does the audit department regularly review controls pertaining to cyber security?

Yes

No

6. Is the registry audit tool always kept up-to-date on the latest developments and does it include related cyber security issues?

Yes

No

7. How do you highlight cyber security weakness, risks and non-compliance in your organization (multiple answers possible)?

Input from peers

Penetration testing

Internal audit

External audit

Informal risk analysis

Formal risk analysis

Input from vendors

Assessment of regulatory (non) compliance

Other _____

Not applicable

Procurement

Adoption and Use of cybersecurity within the Financial Sector in developing countries

1. What is your sex?

Male

Female

2. What vertical market best describes your Organization?

Banking Sector

Microfinance Sector

Telecom sector

3. Is your company a:

Small to Medium-sized business (i.e., 1-500 employees)

Mid-sized enterprise (i.e., 500-1000 employees)

Large enterprise (1000+ employees)

4. What is your Title in the organization?

Executive (CEO, VP, Managing Director)

Management

Operations

Other: _____

5. Does your department identify and evaluate the security risks related to outsourcing or offshoring before approving contracts for critical infrastructure and services?

Yes

No

6. Does your department recognize that they retain accountability for managing their information risks even where they outsource ICT systems and services to third parties?

Yes

No

7. Is the procurement department fully acquainted and compliant with the ICT Policies and the organization impact assessment processes for ICT suppliers?

Yes

No

8. If Yes above, Does the procurement department abide by the ICT policy to identify, document and incorporate security requirements into outsourcing contracts with suppliers and contractors?

Yes

No

9. Does the procurement department follow the security management plan outlining the strategies for reducing security risks when acquiring suppliers?

Yes

No

10. Does the procurement department carry out checks to confirm that the ICT department suppliers are certified as per policy? For example, Cisco certified, HP certified and Dell certified in terms of the equipment they distribute and sell to the organization.

Yes

No

AppendixII:Interview Questions

Dear respondent,

My name is Elizabeth Busingye, I am pursuing my masters in ICT Management, Policy and Architectural Design from Uganda Martyrs University. I am currently carrying out a survey to evaluate the Adoption and Use of Cyber Security in the Financial Sector in Developing Countries

You are one of the respondents that were selected for this research so as to help determine the gaps within the ICT in terms of adoption and use of cyber security in Uganda as well as come up with possible solutions to help improve the ICT and in turn promote strategic alignment and growth between the ICT departments and the business of various organizations.

Your response to this survey will be highly appreciated.

Best wishes

Elizabeth Busingye

1. Do you think that separating the Information security team from other IT staffs structurally under the IT department is advantageous from the security assurance perspective?
2. What Cybersecurity frameworks do you think would best suite the financial sector?
3. What is your opinion towards the incorporation of vulnerability assessment and penetration testing within the financial sector?
4. As the current backbone of National ICT, what mechanisms has NITA setup to protect the Ugandan financial sector from experiencing attacks looking at the context of securing the regulator's ICT infrastructure?
5. In your opinion, would you say that cyber security fits in with the current Ugandan culture in terms of the ways the Ugandan people secure their devices, systems and information?
6. What advice would you give the people in the ICT department in regards to approaching the Board or Top management of an organization when requesting or justifying increase in the ICT budget?
7. In your opinion how would you rate the level of cybersecurity in the Ugandan Financial Sector?

- Sufficiently Secure
- Secure to a certain extent
- Information not available
- Not secure