UNIVERSITY OF GHANA BUSINESS SCHOOL

CYBERSECURITY PRACTICES AMONG FOREIGN BANKS IN GHANA

BY

CHRISTIAN AFFUM

(10090463)

A LONG ESSAY SUBMITTED TO THE UNIVERSITY OF GHANA, LEGON IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF MASTER OF BUSINESS ADMINISTRATION IN FINANCE

DEPARTMENT OF FINANCE

JULY 2019

DECLARATION

I, Christian Affum, author of this long essay do hereby declare that, except for the references which have been duly cited, the work titled, *"cybersecurity practices among foreign banks in Ghana"* was entirely done by me in Finance Department of University of Ghana Business School, Legon from August 2018 to July 2019. This work has never been presented either in the whole or in part for any other degree in this University or elsewhere.

Signature…….. Date……/……/……..

CHRISTIAN AFFUM (10090463)

(STUDENT)

CERTIFICATION

I hereby declare that the principal work and presentation of the long essay was supervised by me in accordance with guidelines on supervision of dissertation laid down by the University of Ghana.

Signature…….

Date……/……/……

DR. JONATHAN WELBECK

(SUPERVISOR)

DEDICATION

This work is dedicated to God almighty, my entire family and all who in diverse ways supported me.

ACKNOWLEDGEMENTS

I will like to express my profound gratitude to my supervisor Dr. Jonathan Welbeck for his guidance in the writing of this thesis

I will also like to acknowledge Nana Baffour Abbam for his diverse contribution and suggestions in the writing of this thesis

Finally, I will like to acknowledge my wife, Mavis Nana Yaa Affum and children for their support

ABSTRACT

The main aim of the study was to investigate the level of awareness, practices and compliance level to the cyber-security directive of the central bank among the foreign banks operating in Ghana. A multistage sampling technique was used to arrive at the final respondents for the study. The study had a total of 46 respondents from 13 foreign owned banks in Ghana. All respondents indicated they knew there was a policy on cybersecurity. To verify the knowledge of the respondents to their organization's cybersecurity policy, we sort to know the standards or framework adopted. Majority indicated that they had no idea of the standards their organization was using. Most respondents who were staff of foreign banks knew there was a cybersecurity policy and were aware of it. But a further probe showed they did not have much information on the policy. Knowledge regarding the standards and framework used was not readily known by most respondents. Internal Audits was the main means to detect cyber security threats followed by formal risk analysis and penetration test. Over half of respondents said they could remotely access the cyber system of the organization. But however, most devices apart from the organization's computers were not allowed on the system. This improves security and prevents threats. To keep staff updated with cyber security issues and systems, routine training programs, seminars or conferences should be held. Both the bank and the central bank has to make it mandatory for every bank staff to undergo some level of cyber training. Drills and exercises in instances of cyber-attacks are an important step towards dealing with a cyber-attack. This would relatively improve the level of preparedness for a cyber threat. Cyber systems need to be audited internally and more frequently to expose loop holes or threats in the systems being used by the banks. This could also be augmented with external audits and risk analysis.

TABLE OF CONTENT

LISTS OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS/ACRONYMS

BoG- Bank of Ghana

IT-Information Technology

ICT-Information Communication Technology

CSI- Computer Security Institute

CHAPTER ONE

OVERVIEW OF THE RESEARCH

1.1 Introduction

Chapter one presents the overview of the study. The initial section of this chapter presents the background of this study which is cybersecurity. This is followed by the problem statement which seeks to situate the problem this study is investigating. This is followed by the research objective and questions the study asks. The significance of the study is presented in the next section followed by the scope and limitations of the study. The last section discusses how the rest of report has been organized.

1.2 Background to the study

In the wake of information and communication technology advancement and knowledge-based economy and society, most sectors in the economy have taken advantage to improve their services and reach more target customers (Driga, I., 2014). The banking sector is no exception and has undergone profound changes during the past decades. Recently, the financial sector relies on cyber-related systems and networks to conduct many of its operations.

The role of cyber-related systems in the financial industry is ever expanding and the frontier being moved day in day out in order to meet client needs and refine operations. The use of cyber-systems has led to improvement of the quality of services, reduce operational cost in some cases of process transactions, speed up communications and transactions as well as transfer of funds and reach more customers. This phenomenon has been embraced by banks all over the world

including banks operating in Ghana. The adoption and use of cyber systems in the banking sector has made it attractive for criminals to launch cyber-attacks on these systems.

Cybercrime is a form of crime often traditional crime (e.g. fraud, identify theft, child pornography) which is executed through the unauthorized access, damage and interference to a computer system. (Broadhurst, 2006). Cybercrime is the act of committing crime or an illegal act through the use of computer systems (Chambers, 2010). This is usually by fraud, impersonating, illegally accessing and interference with a computer system. In simple terms cybercrime can loosely be referred to as any criminal activity that involves the use and manipulation of a computer, networked device or a network. While most cybercrimes are carried out to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them. The issue of cybercrime has become a topical issue for most banks now as some fraudsters use dubious means to get access to the banks E-banking system to commit crime.

According to a survey of 522 financial institutions in the United States of America by the Computer Security Institute (CSI), there was an average of $500,000 annual loss to cyber fraud or cybercrime per annum (Richardson, 2008). This suggests that cybercrime has become a big threat to the financial industry requiring huge expenditure to prevent or control it. These technological advanced threats have transformed the way and manner in which financial institutions operates or transact business with their cyber systems. A very common example is the electronic banking (e-banking) system adopted by almost all banking, and most financial institutions. However, these advancements are said to have exacerbated the rate of cybercrime on financial institutions (Chambers, 2010). Due to the increased or virtually the total use of computer systems in financial institutions one mode of attacking these institutions are through

cyber-attacks. Financial institutions are no exception to this phenomenon due to their adoption of ICT in their operations.

In order to combat such crimes, institutions need to put in place cyber security measures to prevent or control them. Von Solms & Van Niekerk (2013) provided a comprehensive definition of cyber security which they said was providing security for information, information sources, assets and human beings through computer systems. This definition goes beyond the definition that cyber security only targets to protect information. The authors posit that cyber security protects the human being and assets which can also be targeted but not just information per the traditional definition.

1.3 Problem Statement

Financial institutions, especially banks are considered to be high-profile targets for cyber criminals hence the need for them to dedicate resources into securing their cyber systems. Since they possess and transact huge amount of money, they become targets to cyber-attacks. There is a thin line between ensuring utmost security as well as balancing it with efficient and reliable operations devoid of cumbersome procedures for their customers.

In Ghana, cybercrime industry has involved the unauthorized access to the financial system of firms and individuals by unauthorized parties both internal and external of the institutions, email fraud and other forms of crime carried out mainly through internet banking and other localized payment and mobile banking platforms. A 2018 report by the Bank of Ghana on banking fraud indicated that cybercrime had the highest percentage of attempted fraud which was about 58%.

This phenomenon is however not exclusive to only the banking institutions but also the non-bank financial institutions.

Cybercrime pose a great threat to the financial sector considering the monetary losses, loss of data as well as loss in customer confidence in the ability of financial institutions to protect their information. To prevent or control cybercrimes financial institutions adopt various mechanisms and strategies. It is however important for financial institutions to safeguard themselves against cybercrimes during their operations. This warrants the need to investigate the cyber security practices of banks in Ghana.

The central bank of Ghana in October 2018 released a document which provides a framework for establishing Cyber and Information Security protocols and procedures for; routine and emergency scenarios, delegation of responsibilities, inter and intra company communication and cooperation, coordination with government authorities, establishment of reporting mechanisms, physical security measures for IT Datacentres and Control Rooms, and assurance of data and network security. The guide or protocol is aimed at standardizing and providing a base for cyber security practices. This is meant to be adopted by banks to control cyber-attacks.

Banks are expected to hold training for their staff in order for them to be aware of the directive and practice it where applicable. In order to determine the compliance level of the various banks, it would be prudent to first of all find out the awareness of various staff to the Bank of Ghana's new directive. It is however important to determine the various practices among banks in Ghana, this would compare their practices as benchmarked against the industry standards set by the central bank. This would also inform their level of compliance to the new directive which seeks to prevent and save guard against cyber-attacks.

Hence this study would seek to delve into the practices of financial institutions in Ghana to prevent cybercrime. This study would however be situated to foreign banks operating in the Ghanaian financial industry.

1.4 Aim of Study

The main aim of this study is to delve into the practices, awareness and compliance level to the new cyber-security directive among the foreign banks operating in Ghana. This would assess the prevailing cybersecurity practices and compliance. To achieve this aim, the following specific objectives have been outlined.

1.4.1 Specific Objectives

1. To assess the level of awareness of Cyber Security among Foreign banks?
2. To assess the practices of cyber security risk management among Foreign banks?
3. To assess the level of compliance to the Cyber Security directive among Foreign banks?

1.5 Research Questions

In order to achieve these objectives, the following questions have been asked:

1. What is the level of awareness of Cyber Security among Foreign banks?
2. What are the practices of Cyber Security risk management among Foreign banks?
3. What is the level of compliance to the Cyber Security directive among Foreign banks?

1.6 Justification of Study

Knowing the awareness of the cyber security directive among banking staff of the various foreign banks would help to determine the knowledge level and best practices to avoid cyber-attacks. This would inform measures on how to educate or inform banks on the new directives to secure themselves.

It is however important to investigate various practices in the financial institutions to aid policy makers to better standardize the practices where needed and improve it if the need be. This study would provide a better insight into the nature of cyber security practices among the foreign banks in Ghana. This would help policy makers and decision makers to better tailor their cyber security measures to avoid these cybercrimes.

Compliance which is adherence to the new directive would be a measure of how foreign banks are implementing or accepting the new directive. Knowing the level of compliance would inform policy makers on how to formulate future directives, how to help banks implement these directives and finally adhere to them at all times. Also, this study would add to literature in the area of cybersecurity and cybercrime. This would delve into the Ghanaian financial sector and practices which is currently lacked in research.

1.7 Scope and Limitation of the Study

This study seeks to understand the awareness of cybersecurity practices among foreign banks in Ghana. This study however does not cover local banks and other financial institutions. This

might not capture the awareness or the state of knowledge of the entire financial industry hence it would be problematic to generalize based on this.

1.8 Organization of Report

Chapter one introduces the study. This includes the background to the study as well as the problem statement which seeks to present the case for the study. This is situated in relevant literature and prevailing industry occurrence. This leads to the objective of the study and the research questions accompanying the objectives. After, a clear justification of the study is presented followed by the scope and limitation of the study which seeks to draw or address the boundaries of the study.

The literature review is presented in Chapter two, it discusses the critical issues and relevant topics associated with Cybersecurity among banks. It seeks to touch on empirical studies on Cybersecurity practices and some theories which back it. This chapter reviews work done by others within this field of research. The sources of these studies were from academic journals, published books and other authorities in the field.

The next chapter presents the methods used for the study. It provides an insight into the methods used to arrive at the results discussed in the study. It includes data and sampling techniques as well as data analysis methods. Chapter four presents the results and discussions from the study. The final chapter (Chapter five), provides a summary, conclusion and recommendations of the study.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

In this chapter, there would be a review of literature in the field of cyber security in financial institutions. This would first of all try to delve into the operations of financial institutions and how they make use of technology. This would lay a foundation to the cyber security practices in the industry. The review would be from books, articles and journal both published and unpublished.

2.2 Ghana's Financial Industry

The Ghanaian financial industry is mainly made up of depository and non- depository-taking institutions. The depository institutions include universal banks and non-bank financial institutions (NBFIs) such as savings and loans and microfinance institutions. The non-depository institution also includes finance houses, forex bureaux and among others. As of 2019, Ghana has a total of 23 universal banks which is a sharp decrease from 37 as of June 2017. This is due to the recent reforms and cleaning up of the banking sector after the minimum stated capital of the banks was raised to GH¢400 Million.

As of June 2017, there were 141 licensed rural and community banks, 564 microfinance institutions and 37 savings and loans companies (BoG, 2017). Also, there are about 23 and 26 life and no-life insurance companies respectively in Ghana as at Dec 2016. The National Pensions Regulatory Authority have also granted 78 companies to operate as Pension Fund

managers as at 2017. Critical to the Ghanaian financial sector is mobile money which is operated via telecommunications operators. Included are MTN Mobile money, Vodafone cash and Airtel Tigo Cash. These developments and diversification of the financial sector has been necessitated to satisfy the growing needs of the country and create a system to promote healthy competition. This has also given opportunity to create avenues where various strata of the population can be reached with financial services.

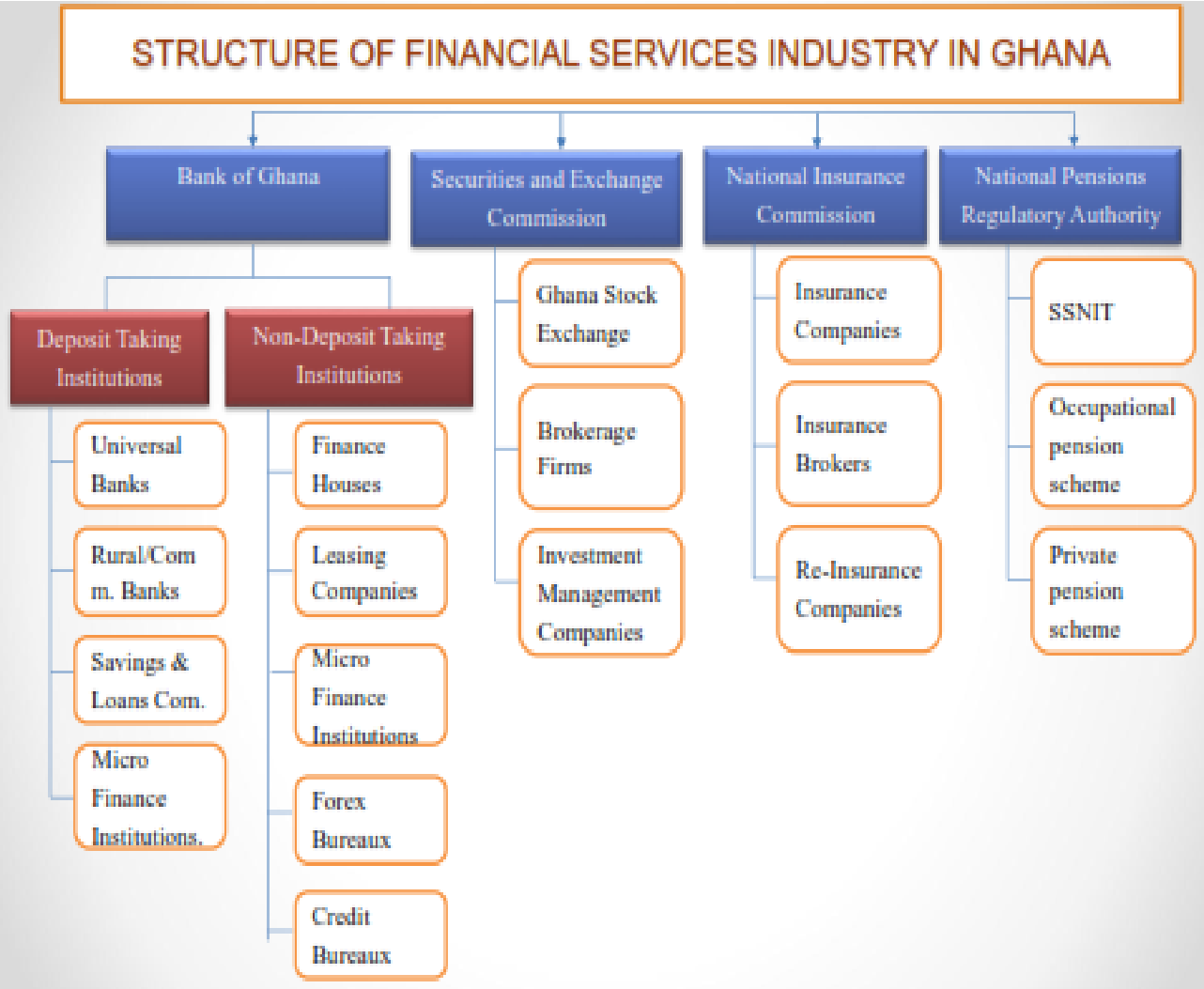

Figure 1: A diagram of the structure of the Ghanaian Financial Service Industry

For the purpose of this study, only universal foreign banks under the regulation of the bank of Ghana would be considered. These banks have certain basic requirements, most important among them is a minimum capital requirement of GH¢400 million.

2.3 Use of Technology in the Financial Industry

In the wake of information and communication technology advancement and knowledge-based economy and society, most sectors in the economy have taken advantage to improve their services and reach more target customers (Driga, I., 2014). The financial sector is no exception and has undergone profound changes during the past decades. Financial institutions rely heavily on cyber-related systems. Financial institutions have adopted and invested into ICT infrastructure to deliver various banking products and services via the internet as well as manage their internal day to day operations. This they do to improve the quality of services, reduce operational cost in some cases and reach out to more customers. This phenomenon has been embraced by banks all over the world including banks operating in Ghana. Since they use cyber-systems to transact and transfer funds, they have become attractive targets to cyber criminals.

2.4 Cybercrime in the Financial Sector

First of all, this study would lay boundary to what can be termed as cyber. Cyber as used mainly as a prefix for a number of terms can be described as items, actions or new things that make use of the computer or network to work. In other hands it is facilitated by the computer. Some examples are, cyber systems, cybercrime, cyber-attacks, cyberspace and cyber security. Hence a crime perpetuated via the computer or using IT as cybercrime (Longe & Danquah, 2012).

For the purpose of this study we would basically define cybercrime as any form of crime that is perpetuated using or targeted at a computer or a network (Moore, 2005). Halder et al (2012) provided a more comprehensive definition which said cybercrime is any offense or crime carried out on an organization or a person to gain unlawful access to information, damaging systems and interfering with the operations of a computer or network system. These definitions however indicate that the systems could be the target or the tool for carrying out the wrong doing in the case of cybercrime. Cybercrime has become a global security issue since criminals of all sort use it to champion their course. In a 2014 report by Reuters, the global economy lost about US$445 Billion to cybercrime activities in the form of direct money lost and damages. To properly understand the nature of cybercrime, there has been a comprehensive categorization of cybercrimes. Even though some crimes overlap more than one category, this seeks to put cybercrime in types based on the nature of the crime.

Financial Fraud Crimes - these are mainly targeted at financial institutions or transactions by dishonest misrepresentation and illegal access of systems to acquire funds under false pretence. Examples are bank fraud, using false identity and extortion.

Cyber terrorism - In recent times, terrorists have begun to perpetuate their action by the use or targeted at computer or network systems. The most common form is by spreading false information on possible attacks and hacking to steal information or disrupt a system. This is mostly carried out on a large group of people and or an organization. This is done to show power from the terrorist organization.

Cyber extortion - Extortion carried out or demanded through emails, social media or other cyber systems by acquiring certain information with threats to spread it is known as cyber extortion.

Computer as a target- with this form of cybercrime the computer or network is the target of the crime. In this case there could be damage, disruption and unpermitted access into a cyber-system.

Computer as a tool- On the other hand there is the cybercrime where the computer or network is only used as a tool or means to perpetuate the crime. In this case there is a target who could be an individual or an organization who would be attacked using a cyber system.

Cyberwarfare- a typical example of cyberwarfare would be the accusation levelled against Russia involving attacks on USA and Ukraine. This is a battle which occurs through cyberspace with the aim of disrupting entire national cyber systems or accessing some information with national security implications.

Other cybercrimes- under this category some new but not well-defined cyber activities such as cyberbullying, cyberstalking, online predating and internet troll.

Cyber criminals take advantage of certain instances before they can perpetuate their activities. It is however important to discuss and review what these weaknesses are. Experts have opined that before there is a cyberattack there are some preconditions which are taken advantage of by cybercriminals (Pfleeger 2003). This they termed as vulnerability of the cyber system. A cyber system vulnerability is a weakness in design, implementation, operation or internal control which could be taken advantage of by cyber criminals. Due to the severity of cybercrimes, commonly known vulnerabilities have been documented for other industry persons to take note and guard against them. These include but not limited to backdoor, denial-of-service attacks, direct-access attacks, eavesdropping, multi-vector, polymorphic attacks, phishing, privilege escalation, spoofing and tampering.

Even though there are several forms of cybercrime, financial fraud or cybercrimes targeted at financial institutions or transactions have been found to cost an average of US$ 500,000 in the United States. This was reported by the CSI Computer Crime & Security Survey. Other countries have also reported that losses from financial cybercrimes are the highest among the forms of cybercrimes. This is a major security and financial threat to the financial sector as a whole. This has led to the injection of huge resources to control or prevent cybercrime in this sector. All financial players-regulators, financial institutions and consumers- have all been engaged in the fight against cybercrime.

Generally, the financial sector has been a target for criminals and with the rise of cybercrime, the industry has become a main target. According to Ofanson et al., (2010) the introduction and advancement of digital technology in the financial sectors has led to an increased customer satisfaction, speed up transactions and improved efficiency in financial institutions. This has worsened considering the fact that in their quest to improve efficient and customer service, financial institutions have embraced the use of modern ICT. The dependence on these systems has created a target for cyber criminals. Chau and Lai V., (2003) in their study revealed that the competition in the financial sector was the main reason for technological innovation. This has also resulted in the surge in cyber-attacks and crimes targeted at these cyber systems based technological innovations.

2.5 Cyber Security in the Financial Sector

The rise in cybercrimes has necessitated the development of security measures to counter these attacks. This has led to the new concept of cybersecurity. This is a new area but yet a very

important one considering the way humans and organizations make use of cyber systems in their day to day activities and transactions. Cybersecurity has evolved due to the ever-changing nature of technology as compared to other forms of security (Adeyinka, 2008). The International Telecommunications Union defines cybersecurity as technical and non-technical actions and measures which are directed towards preventing and protecting cyber systems such as computers, networks, software, data and other devices from possible dangers and threats. This definition seeks to go beyond only the technical information technological measures used to combat cyber-attacks to some non-technical aspects. Schatz et al., (2017) also defined cybersecurity as security for computer systems which seeks the protection of computer and network systems against theft, damage or disruption to their hardware, software and data. From these two definitions it can be concluded that cybersecurity is a system employed to protect cyber systems from unwarranted actions and threats.

There are two main types of cybersecurity, these are the passive and active cybersecurity measures (Cole et al., 2008). This classification is based on the nature of the security activity. A cyber security activity which aims to put in systems and measures to strengthen a cyber system in order to prevent or withstand all cyber threats is said to be passive cyber security. These are mainly in the area of anticipating and preventing the attacks before they are initiated. But the active cyber security is the form of cyber security where there are constant activities to control and retaliate all incoming cyber threats or attacks. It is however important to note that according to the authors, (Cole et al., 2008) in order to build a robust cyber security system there is the need to employ both types of cyber security.

2.6 Cyber Security in the Ghanaian Financial Sector

Financial institutions in Ghana have become a major target for cyber criminals. A Myjoyonline report also indicated that as at August 2018 Ghana lost US$97m due to cybercrime in the financial sector. Apart from the huge financial losses there has been some other form of losses such as a decrease in the confidence in the sector. In order to curb this, the regulator and financial institutions employ various measures. This is necessary to be ahead of the ever-changing world of technological innovations.

At the highest level, the BoG has been at the forefront of the fight against cybercrime. In order to standardize the cyber system for all financial institutions, the BoG develops frameworks and directives with the aim of safeguarding the entire industry against the threats of cybercriminals. Internally, financial institutions are expected to adhere to the basic directives and if possible, improve or upgrade their systems to be ahead of cybercriminals. This is important for these institutions, so they are able to protect their customers and prevent losses of money as well as clients.

The Bank of Ghana in 2018 released the Cyber & Information Security Directive under the powers conferred by Section 92(1) of the Banks & Specialized Deposit Taking Institutions Act, 2016 (Act 930). The directive is targeted at all banks operating in Ghana. The main objective of this directive is to;

1. Create a secure environment within the cyberspace for the financial services industry and generate adequate trust and confidence in ICT systems as well as transactions in the cyberspace;

2. Create an assurance framework for design of security policies and for promotion of compliance to global security standards and best practices by way of cyber and information security assessment;
3. Strengthen the Regulatory framework for ensuring a secure environment within cyberspace;
4. Enhance the protection and resilience of the financial systems' operation and provide security practices related to the design, acquisition, development, and use of operation information resources;
5. Improve the integrity of ICT products and services by establishing infrastructure for testing and validation of security of these products and services;
6. Promote continuous cyber and information security risk assessment;
7. Promote awareness creation and ensure human resource security.

The directive also seeks to provide guidelines to cyber security governance, appointment of chief information security officer, management of cyber security risk, asset management, cyber defence, cyber response, employee access to cyber ICT systems, electronic banking services, training awareness and competence, external connections, cloud services, physical security, human resource management, procedure for termination of employee appointment and contractual aspect of cyber security.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

Chapter three of this study focuses on the methods used. The chapter includes an overview of the study area, the sampling procedure, the data & data collection tools and the analytical techniques used. It presents a justification for the selection of the methods and how they help in achieving the set objectives of the study.

3.2 Research Approach

The quantitative study approach was mainly used for the study. This was however augmented with qualitative analysis where necessary. This combination is necessary since the data collected were both qualitative and quantitative in nature. This made data collected exhaustive in nature to capture details which might have been lost if the study approach was restricted to one approach.

The use of qualitative information involves analysing data which is usually related to human actions and the grounds behind them. Qualitative research is mostly used in behavioural sciences (Salkind, 2003). Results from quantitative analysis are mostly limited since they provide numerical descriptions rather than detailed narrative and generally provide less elaborate accounts of human perception (Pickard, 2007). However, an advantage of this research method is the ability to examine given phenomena with respect to multiple human perspectives. The free nature of research allows a richer input that might contribute to a more specific learning outcome (Pickard, 2007). Qualitative research is noted to be more ideal for human oriented study research. The lack of quantitative scoring gives freedom of choice on both questions and answers

and can offer a great input of knowledge to the study. A great disadvantage in comparison with quantitative research however, is that data cannot always be quantified. Collection of data for this study was done through face to face interview personally by the researcher.

3.3 Study Area

The Greater Accra Region is the capital of Ghana. It is bounded by the Eastern, Central and Volta Regions. It is also bounded by the Gulf of Guinea to the south. Even though the study sought to investigate the cyber security practices of foreign banks operating in Ghana, the study limited its scope to Greater Accra Region. Since it's the capital of Ghana, all multinational firms such as banks are represented here. They have their head offices in this region as well as other branches of operation. This made data collection within the region convenient and representative.

3.4 Data Collection Approach

A cross-sectional data for bank's operations were collected from selected staff of banks (respondents of this study) by administering a well-structured questionnaire. The questionnaire collected data on the banks' cyber security practices, their compliance, and knowledge of the cyber security directive from the central bank as well as certain professional characteristics of the respondents. A pilot or pre-test of the questionnaire was conducted on a selected few industry members to fine tune it. A revised form of the questionnaire with inputs from the pre-test was used for final data collection. This questionnaire has been attached as Appendix I of the study report.

3.5 Sampling Procedure and Sample Size

Multistage sampling technique was used to arrive at the final respondents for the study. All foreign banks operating in Ghana were censused. Since all foreign banks operate in the Greater Accra Region, they all were selected. The region was selected purposively because it is the capital of Ghana and all banks operating in the country are represented in this region. The banks censused numbered about 13 in total.

The next stage was to randomly select which branch of these banks were to be visited but data was collected from some head offices. Respondents who were staff of these banks were selected based on the role they played in the banks. Respondents who worked with cyber security systems were also selected. At least one person was selected from all foreign banks, but some banks had multiple respondents.

Respondents included in the sample were selected to meet specific criteria. The respondents had to meet the following criteria to be included in the sample.

They should:

- have worked at a foreign bank for at least 1 year
- be mentally sound in order to consent to participation
- be willing to participate
- be of either sex or any race

3.6 Method of Data Analysis

In collecting and analyzing the data, Google Data analytics was used. The questionnaire was designed and administered electronically using the Google Survey tool. This helped in reducing

the difficulty associated with physical method of administering and retrieving questionnaires. In determining the level of awareness, compliance and practices of cybersecurity, descriptive statistics such as mean, mode and standard deviation will be used. Qualitative responses would be also be presented.

3.7 Ethical consideration

Research does not only require expertise and diligence, but also honesty and integrity. To render the study ethical, the rights to self-determination, obscurity, confidentiality and informed consent were observed. This was done to recognize and protect the rights of the respondents.

The respondent's consent was obtained before the questionnaires were administered. As defined by Burns and Grove (1993:776), consent is the prospective subject's agreement to participate voluntarily in a study, which is reached after assimilation of essential information about the study. The respondents were notified of their rights to either consent or decline to participate in responding to the questionnaire. They were further informed about the purpose of the study and assured that there were no potential risks or costs involved. Anonymity and confidentiality were maintained throughout the study. As defined by Burns and Grove (1993:762) anonymity is when subjects cannot be linked, even by the researcher, with his or her individual responses. This study ensured anonymity by not revealing the respondent name on the questionnaire and research reports and detaching the written consent from the questionnaire.

When respondents are promised confidentiality, it means that the information they provide will not be publicly reported in a way which identifies them (Polit & Hungler 1995:139). Confidentiality was maintained in this study by keeping the collected data confidential and not

disclosing the subjects' identities when reporting or publishing the study (Burns & Grove 1993:99). No identifying information was entered onto the questionnaires.

The respondents were treated as independent agents and allowed to willingly choose to participate or not. This was to ensure the ethical principle of self-determination was also maintained. Lastly, information was provided about the researcher in the event of further questions or complaints. When conducting a research scientific honesty is viewed as a very important ethical responsibility. Dishonest conduct includes manipulation of design and methods, and retention or manipulation of data (Brink 1996:47). In this research effort was made to avoid any form of dishonesty by capturing honestly the answers of the subjects

CHAPTER FOUR

DATA ANALYSIS AND DISCUSSIONS

4.1 Introduction

This chapter focuses on the results and discussion from the study. This starts with the demographics, and then followed by the findings relating to the level of awareness, practices and compliance to the Bank of Ghana Cyber Security directive. It further seeks to find out how demographics influence cybersecurity awareness, practices and compliance before ending the chapter with some concluding remarks.

4.2 Demographics

4.2.1 Positions Held by the Respondents

The study had a total of 44 respondents from the foreign owned banks in Ghana. The positions of the respondents are an important demographic which can be linked to the authority, level of knowledge, legitimacy and responsibility. This is important to ensure the responses provided are valid in achieving the goals and objectives of the study. Even though each staff of the bank is expected to be abreast with the cyber security directive, it is however expected that the leaders and management of bank should have more cyber security knowledge to help trigger the awareness and practices down to other officers in the bank. The positions were generally classified as officer grade and managerial.

Table 1: Frequency Distribution of Positions Held by Respondents

Position	No. of Respondents	Percentage
Officer Grade	28	74
Manager	16	36

Source: Author's own computation from field date, 2019

In terms of the frequency distribution analysis of the respondents, with respect to position there were 16 managers, representing 36% each, and 28 respondents at the officer level of the banks, representing 74%. Above results indicates that the majority of the respondents, representing 74% in total were from the officer grade of the foreign banks. The results are quite representative of a banking structure with many officers and a few managers in charge of the officers.

4.2.2 Experience Analysis

Experience in a profession is a critical consideration in every sector especially the banking sector as it can be related to the knowledge in the sector.

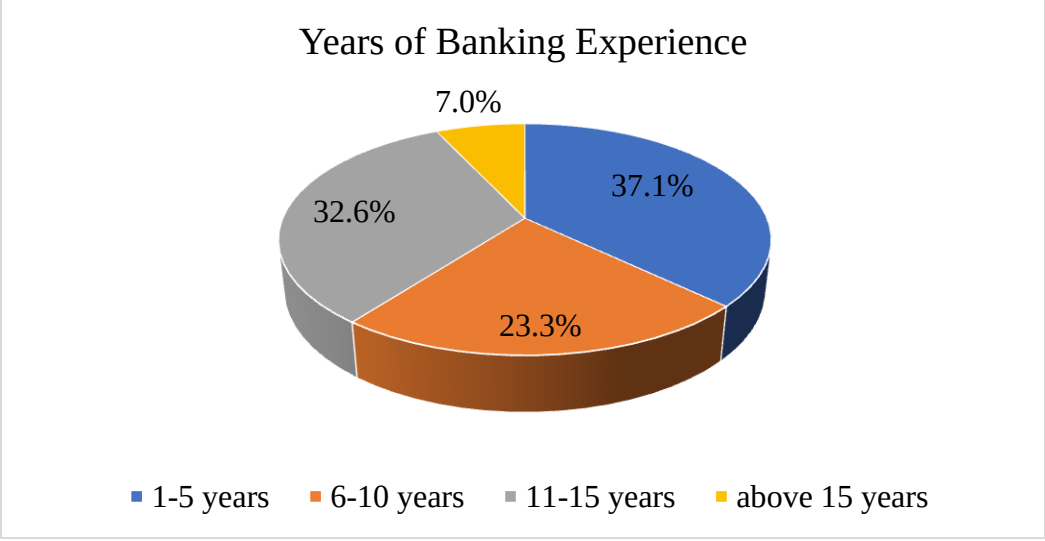

Figure 2 Percentage Distribution of Experience in the Banking Industry

The experiences of the respondents were categorized into five (5) groups. From the pie chart as shown in Figure 2, only 2.2% and 7.0% had less than one and more than 15 years of experience working respectively in the banking sector. Since the majority fell between above 1 to 15 years working experience it can be concluded that the sampled respondents were experienced bankers and had good knowledge of the cybersecurity practices and operations within the banking sector.

4.2.3 Length of stay in current bank Analysis

It is however important to note that since this study wants to investigate the various cybersecurity practices within foreign banks, the number of years of experience in the specific current bank of the respondent has to be known. This would give a general idea of how the respondents know the organization they are speaking about. Furthermore, this would provide an understanding on the knowledge of the individual in their organisation with regards to cyber security practices. From the pie chart as shown in Figure 3, 61% of the respondents had been with their current organization between 1-5 years, 13.6% between 6-10 years, 20.5% between 11 to 15 years and 4.9% above 15 years. It can be inferred that the respondents had been with their current organization for a reasonable amount of time to make pronouncements of their cybersecurity practices.

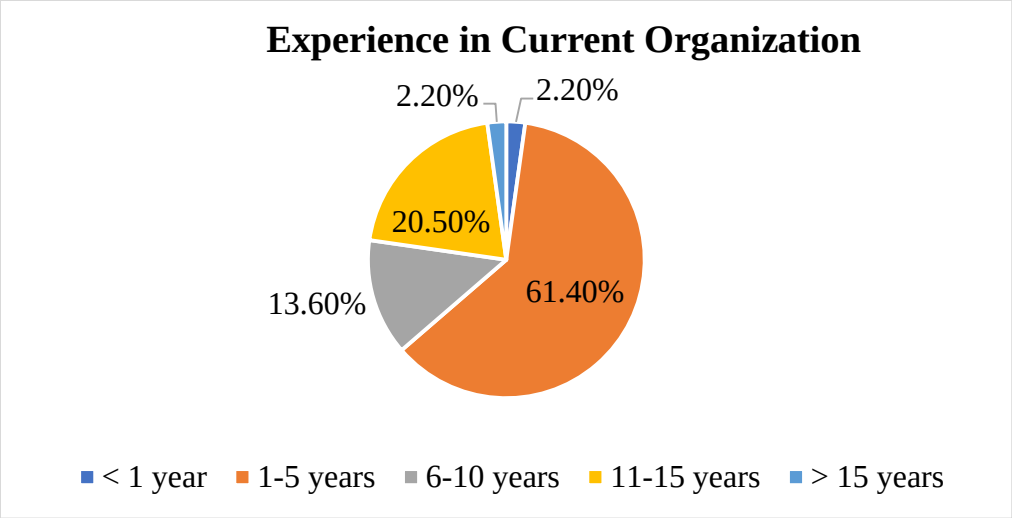

Figure 3: Frequency Distribution of Experience in Current Organization

4.3 The level of awareness, understanding and knowledge of Cyber Security issues

The first objective of this study sort to investigate the awareness of the cybersecurity among the respondents. To achieve this objective, certain key questions pertaining to cybersecurity were posed to the respondents. Further to the awareness some other questions were asked to bring out the knowledge and understanding of the prevailing cybersecurity issues.

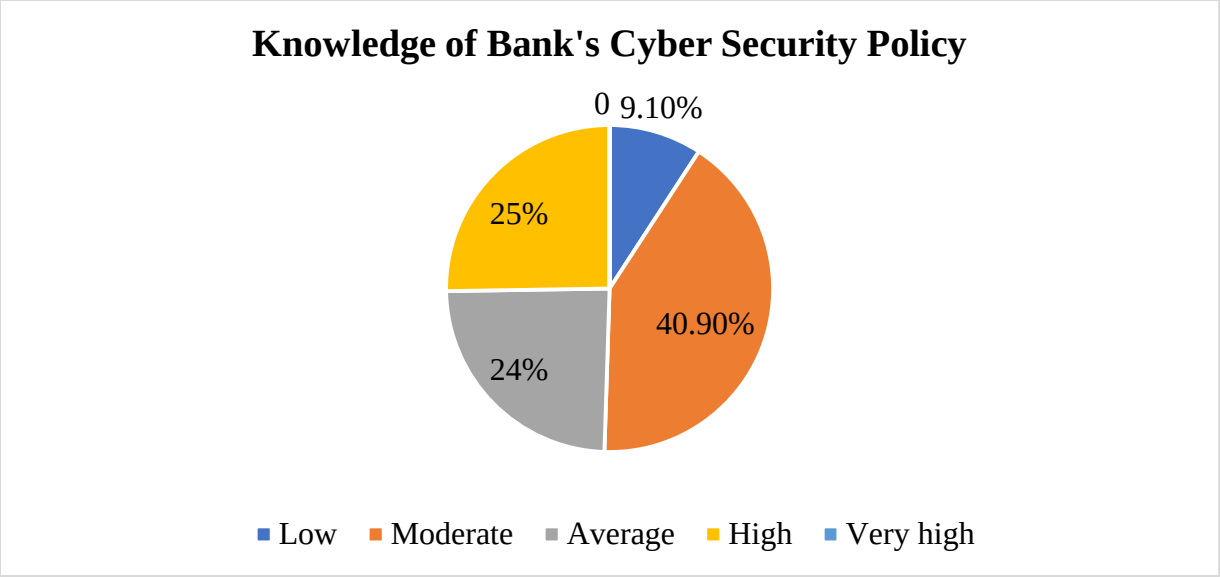

Figure 4: Distribution of Respondents Knowledge of Cybersecurity Policy

First of all, respondents were asked if they knew their organizations had a cybersecurity policy addressing all cyber related issues and practices. All respondents indicated they knew there was such a document or policy. A further question was asked to determine the extent to which they had knowledge of the policy. This was ranked into 5 stages from low to very high. It is interesting to know that none of the respondents indicated that they had a very high knowledge because they said the policy was a bit technical. From Figure 4 it can be noted that a total of 25% of the respondents said they had high knowledge followed by moderate, average and low knowledge which recorded 24%, 40.9% and 9.10% respectively. From the results it can be said most respondents had a fair idea of the cybersecurity policy but lacked in-depth knowledge. This is relatively on the lower side considering how important issues of cybersecurity have become

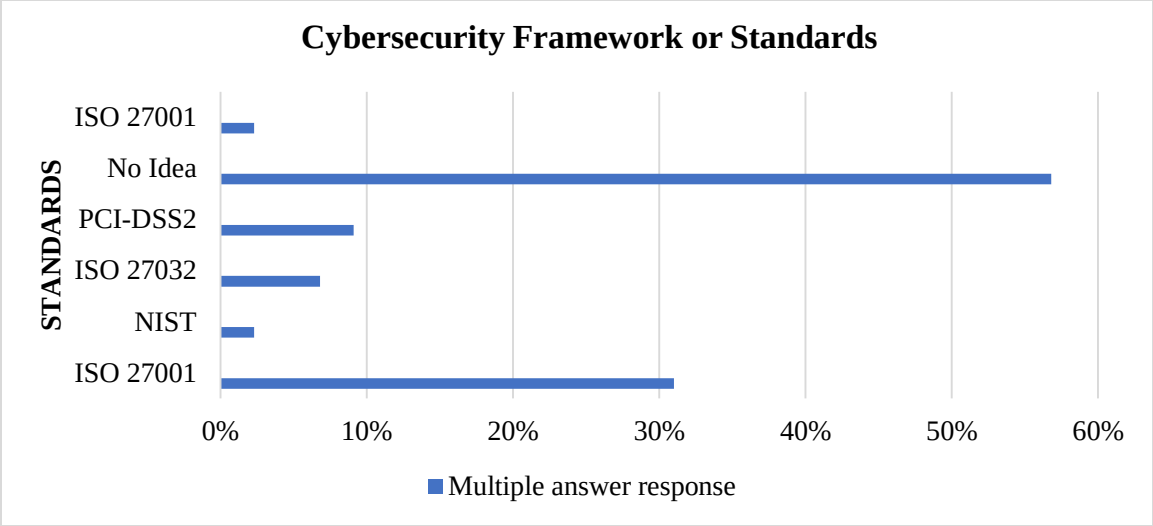

Figure 5: Distribution of Existing Cybersecurity Framework or Standards

To verify the knowledge of the respondents to their organization's cybersecurity policy, we sort to know the standards or frameworks adopted. About 57% indicated that they had no idea of the standards their organization was using. The rest indicated that their organizations adopted ISO 27001, PCI-DSS2, ISO 27032, NIST and ISO 27001 by 3%, 9%, 7%, 2% and 32% of respondents respectively. Some respondents indicated that their organizations used more than one standard or framework. From the results it can be inferred that more than half of the respondents had no idea of the particular standard adopted by their organization hence confirming the earlier results that respondents only had a fair idea of the policy but not an in-depth knowledge.

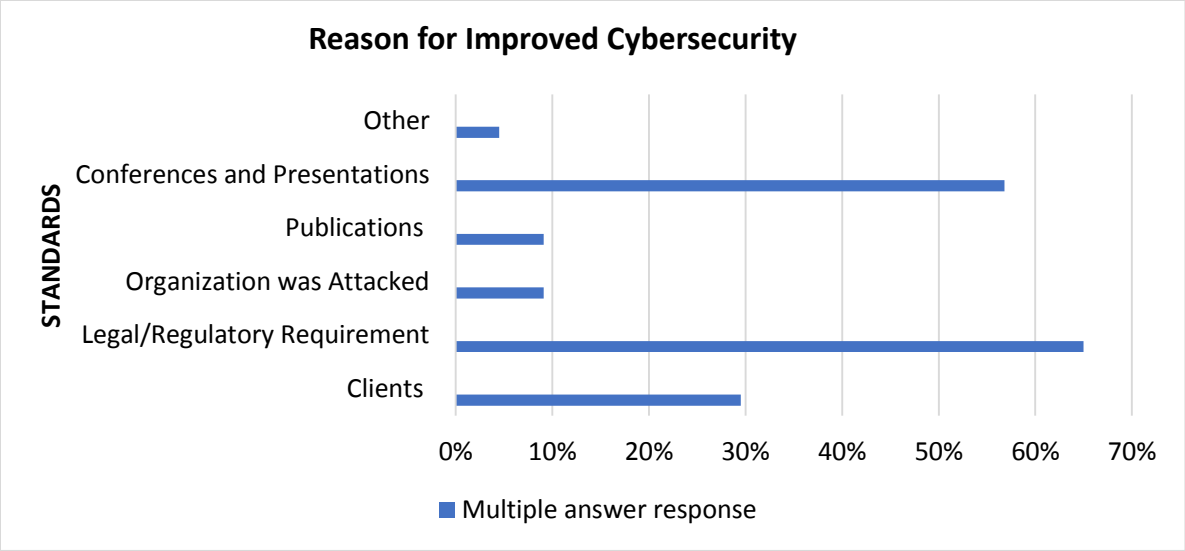

Figure 6: Distribution of Reasons for Increased Awareness of Cybersecurity Threats

When the issue of cybersecurity threats was raised among the respondents, all indicated that they were aware of the imminent threat of cyberattacks. A further question to know the reason for the awareness or what caused the awareness, 65% of the respondents indicated that the regulator required all banks to safe guard against cyberattacks. 57% indicated they got the awareness from presentations, seminars and conferences they had attended. About 30% indicated clients had raised the issues. Some 9% had indicated that they had read about through publication and another 9% and 2% had experienced cyberattacks and through other means not stated. Clearly as shown in Figure 6 above, the regulator and other organization who organizes seminars and conferences have played an integral part in creating an awareness of the threats of cyberattacks.

4.4 Cyber Security Risk Management Practices

From the study, 65.9% of respondent said they were not aware of a BYOD (Bring your own device) provision. A total of 55.8% of the respondents said they had been involved in a cybersecurity drill in the past. The remaining indicated they had never been involved in such an exercise. This indicates that generally drills are not carried out by all organizations. This is usually a simulation of a cyberattack and the response towards it. This demonstrates the readiness and actions to foil a cyberattack. There is a need to know if the organization shares information on cyberattacks with third party such as the media or other external parties. 53.5% of the respondents indicated that issues of cyberattacks are not shared with third party with the reason of causing fear among clients and damaging the reputation of the institution. The rest indicated the organization shared such information with the police and other authorities. When it came to the use of access token to access all departments, 84.1% indicated they could use their tokens to access all departments and the rest indicated they could not.

Table 2: Distribution of Cybersecurity Awareness

Questions	Yes (%)	No (%)	Not Applicable
Are you aware of a BYOD (Bring your own device)	34.1	65.9	-
Have you been involved in a cybersecurity drill in the past	55.8	44.2	-
Does your organization share information on security attacks with third party?	18.6	53.5	18.6
Are you able to use your access token (card, biometric, etc) to access all departments	15.9%	84.1	-
Does your organization use a biometric access control system	81.8	18.2	-
If yes is it the only access control mechanism used	45.2	54.8	

Source: Author's own computation from field date, 2019

A much more modern access control adopted by banks is the use of biometric access control. 81.8% of respondents indicated they use this access control at their organization and the remaining respondents indicated no. This meant the majority of respondents had this access control system at their organization. 54.8% of the respondents indicated that the use of the biometric access control was not the only access control used in their organizations, but it was used in combination with other access control systems. These can be seen from table 2 above.

The study sought to find out the stage of the maturity of the organization's cybersecurity practices. A total of 54% of respondents indicated their practices were optimised, meaning they were focused on continuous improvement and innovation in order to meet the growing concern and threats. 29.5% indicated that their cybersecurity practices were managed meaning they are effective benchmarking process, effective management control, adaptation without losing. 9.1% of respondents indicated that their practices were fixed, meaning, a set of defined and documented standard processes, some degree of improvement over time. The rest of the respondents indicated that there was no information available, basic and repeatable. Hence from the results in Figure 7 below, it can be said that most organizations were at a matured stage where good practices were being carried out.

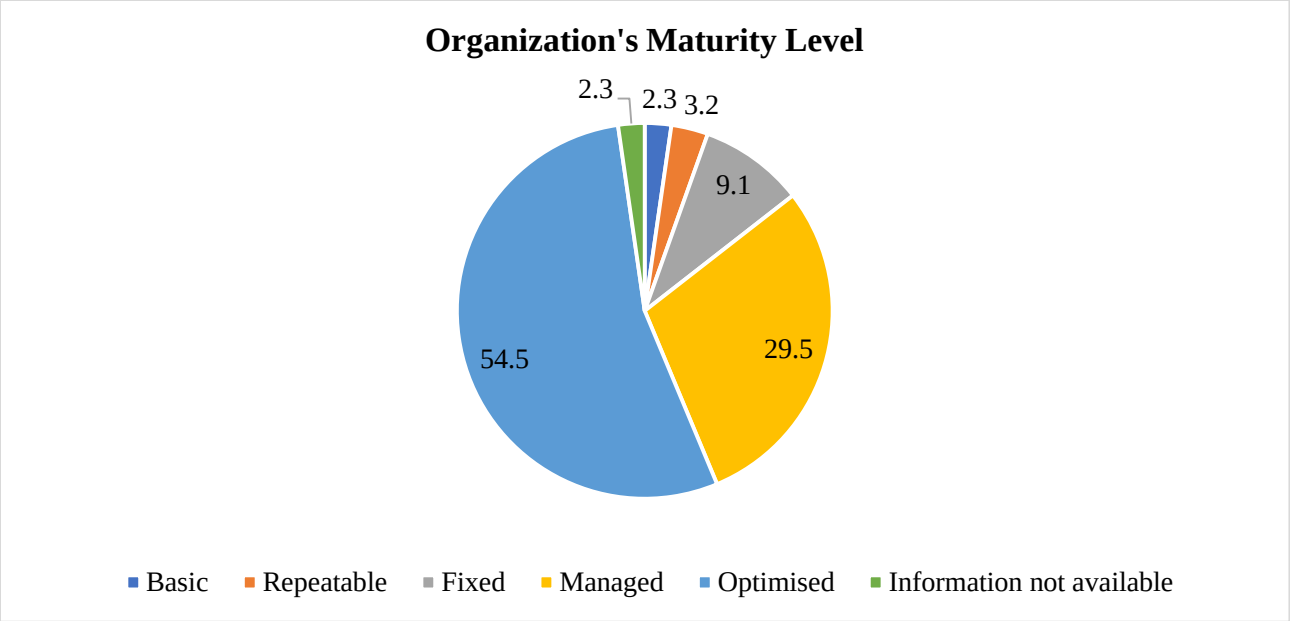

Figure 7: Distribution of Organization's Cybersecurity Maturity Level

It is important for any cyber system to be tested to ascertain the strength or resilience of the system. The results from the study indicated that most (55.8%) of the respondents did not know the effect of such penetrating test and therefore did not recognize the need as to 41.9% who indicated this was a needful trial. A further 2.3% did opine that the penetrating tests were damaging and could destroy the systems and make them prone to more attacks.

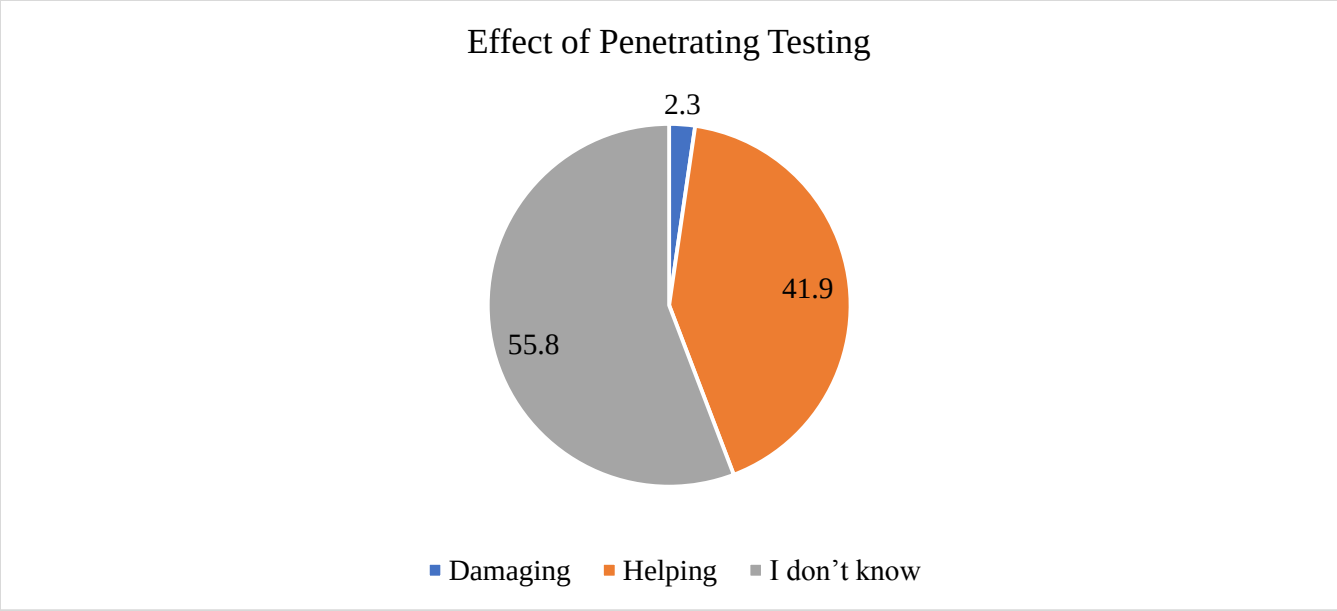

Figure 8: Distribution of whether penetration testing used helps or damages a system

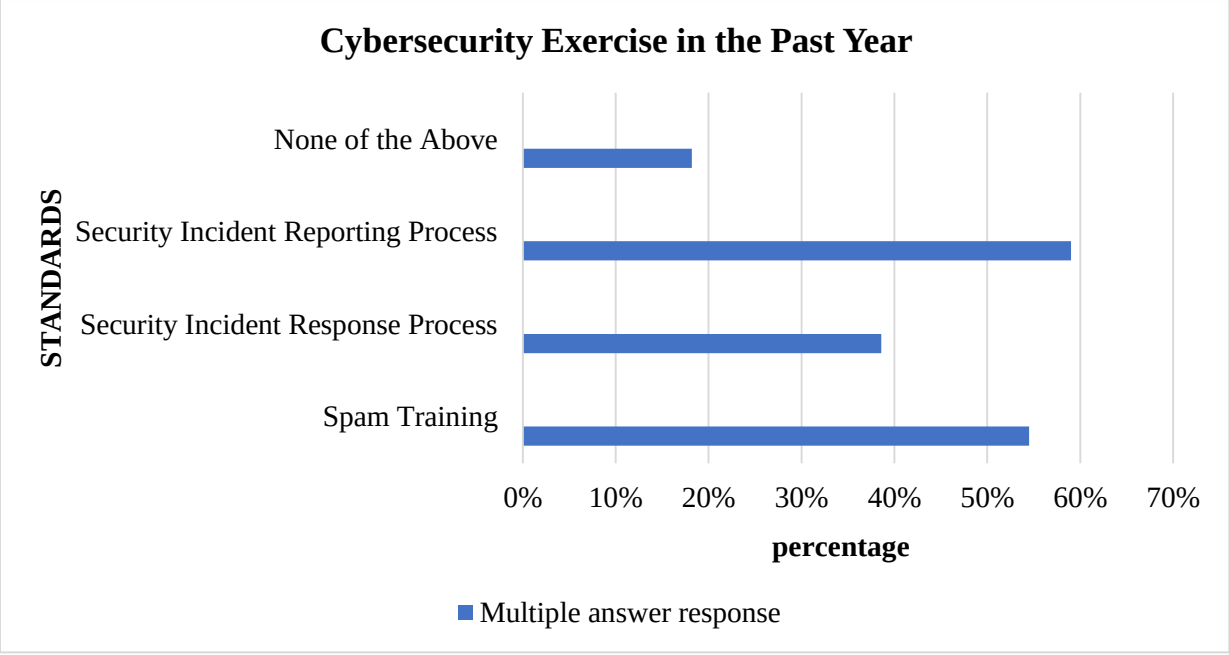

Figure 9: Distribution of Cybersecurity Exercises Carried out in the Last Year

The study further sought to find out if other cybersecurity exercises were carried out in the past year at the various organizations as shown in Figure 9. A total of about 60% indicated they had undergone security incident reporting process exercise which was intended to train staff on how to report a cyberattack. Also, about 55% of respondents said they had undergone training on how to manage spam when communicating via emails. This is a common way to get into a cyber system when not managed well. About 38% indicated they had undergone training on how to respond when there is a cyberattack. This involved reporting and action needed to control the attack before the designated staff comes in to address the issue.

Figure 10 below shows the objective of the various cybersecurity exercises carried out in the various organizations. Confidentiality and integrity of the system and information were the main objectives for carrying out cybersecurity exercises both recording 93% and 91% respectively. Situational Awareness and indicating availability of a cybersecurity policy were the nest reason with 53% and 50% of respondents choosing these objectives. In all ensuring the integrity and confidentiality of the system are the main reason and most important objective for carrying out cybersecurity exercises in a bank.

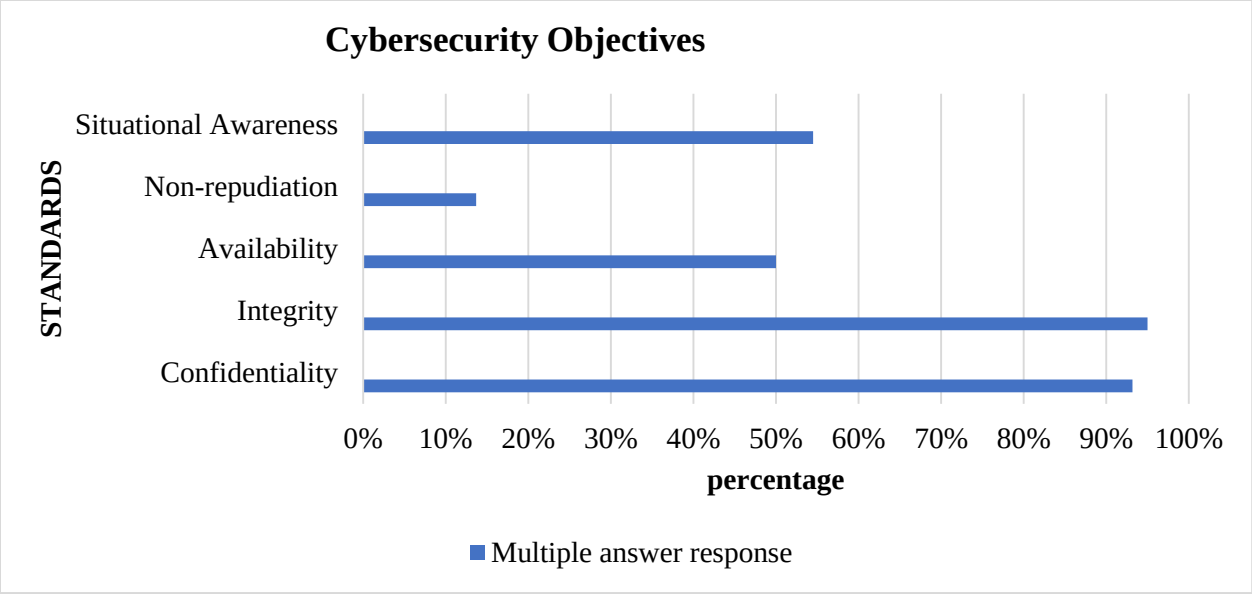

Figure 10: Distribution of Objectives of Cybersecurity Exercises

4.5 Level of Cyber Security Compliance and Practices

The final objective of the study was to establish the level of practices and cybersecurity compliance among foreign banks in Ghana vis a vis the new cybersecurity directive issued by Bank of Ghana in 2018. To find out the level of compliance and practices some important questions pertaining to the BoG's directive were asked and presented after analysis.

From the cybersecurity directive of the central bank, all the banks need to document their cybersecurity policies and procedures. This makes it simple to refer to without any ambiguity. from figure 11 below, about 81% indicated that the situational awareness was document. This was the most document, followed by information security strategy, cyber incident response plans, information security governance, information security roadmaps representing 77%, 75%, 60% and 36% of respondents respectively. This indicates that most banks whose staff responded had either one or more of these cybersecurity documents available.

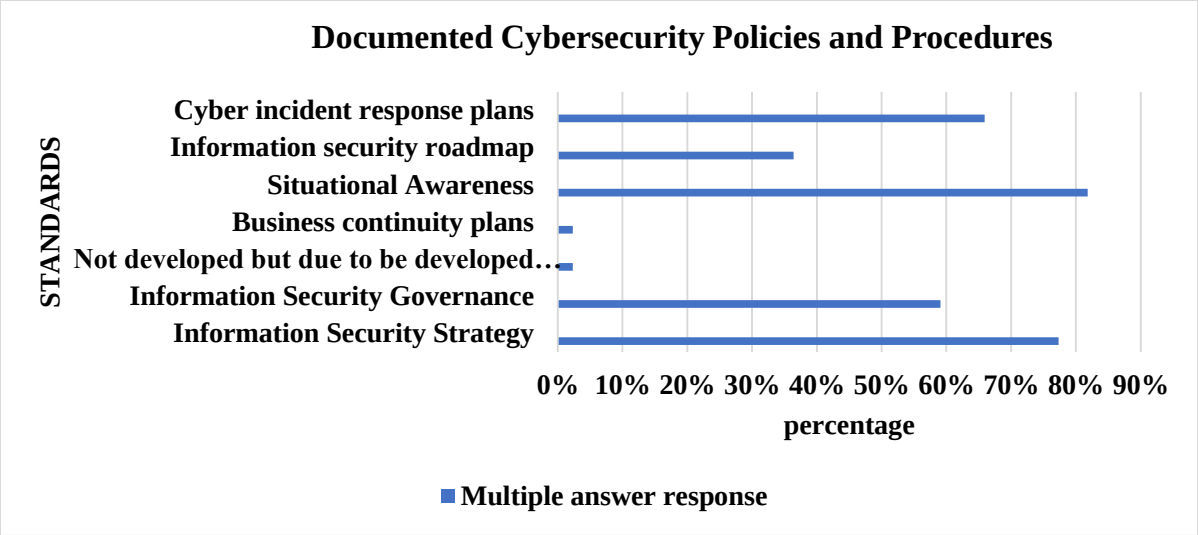

Figure 11: Distribution of Documented Cybersecurity Policies

When an issue of cyber threat occurs, it is important to report the incident to an appropriate superior who has the authority and knowledge to deal with it without escalating. From the results of the study, 37% of respondents indicated they reported issues of cybersecurity to their chief information officer (CIO). Another 37% reported it to the Head of IT, in this case some banks said the Head of IT was similar to a CIO or they had no CIO in their ranks. A total of 9% also report to the chief operating officer. From the Figure 12 below it can be inferred that staff reported issue of cyber threats to appropriate authorities.

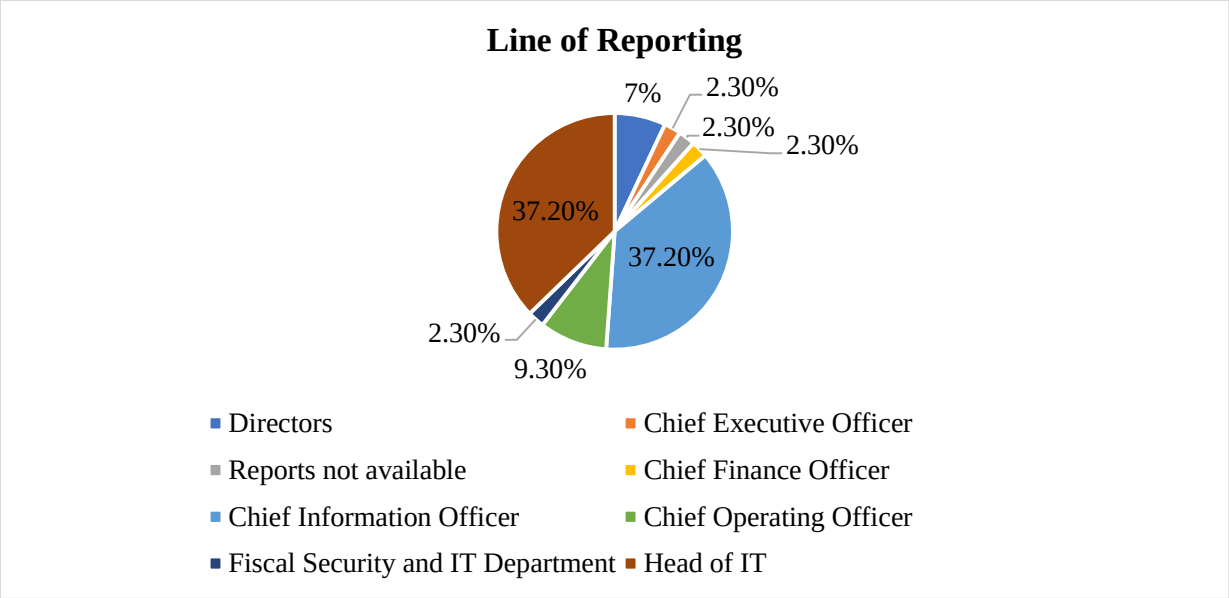

Figure 12: Distribution of Superior to Report Cybersecurity Threat

The main process for discovering or uncovering flaws in the cyber system is through internal audit. 65% of respondents indicated that this was how flaws in their cyber system was found. 40% of respondents indicated that formal risk analysis exposed some loopholes in the systems. About 30% of respondents also said penetration tests, external audit, informal risk analysis and regulatory works was the process by which flaws were uncovered. A total of 20%, 15% and 10% indicated that input from peers, input from vendors and other reasons respectively were the means by which flaws were discovered. From this it can be observed that flaws are discovered through a mix of ways but it is important to note that deliberate actions to review the systems such as audits, risk analysis and penetrating tests are the most important ways.

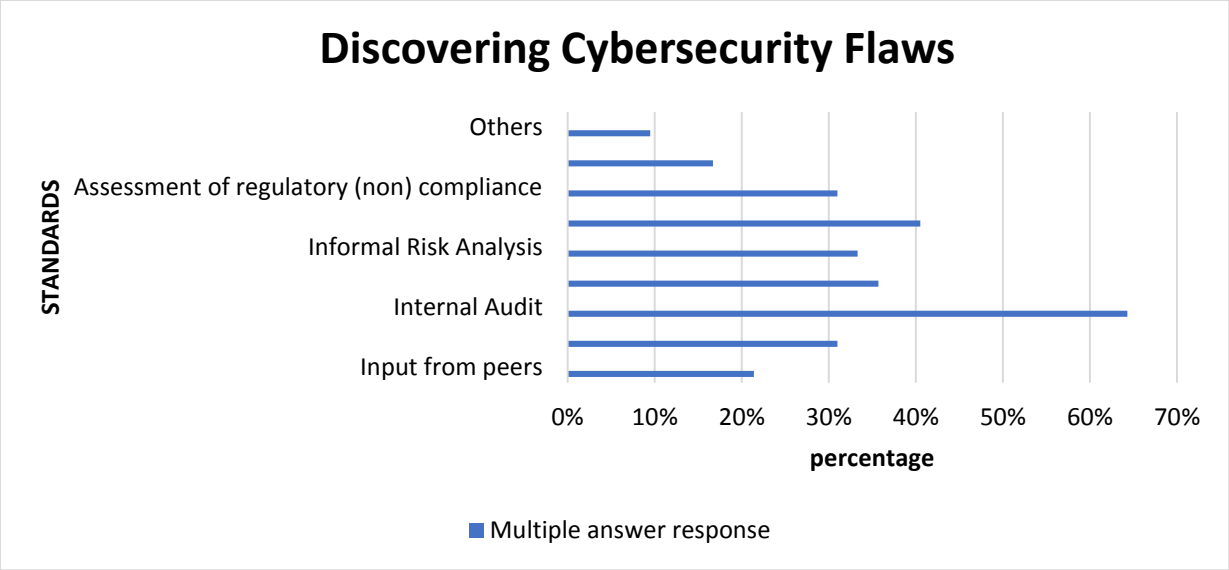

Figure 13: Distribution of How Cybersecurity Threats are Discovered

Emails have become a common way of communicating at the workplace in recent times due its instantaneous nature and confidentiality as well as ability to use it as a means to track corresponding. Due to this, it has become a means to attack cyber systems when precaution is not taken while using. 16% of respondents indicated that they always made sure emails were from, a known or secured source before opening the mail or an attachment to the email. Whiles 84% indicated that they opened it if it was a corporate email address or they knew the sender. From the figure below it can be observed that much precaution is not taken when it comes with dealing with emails.

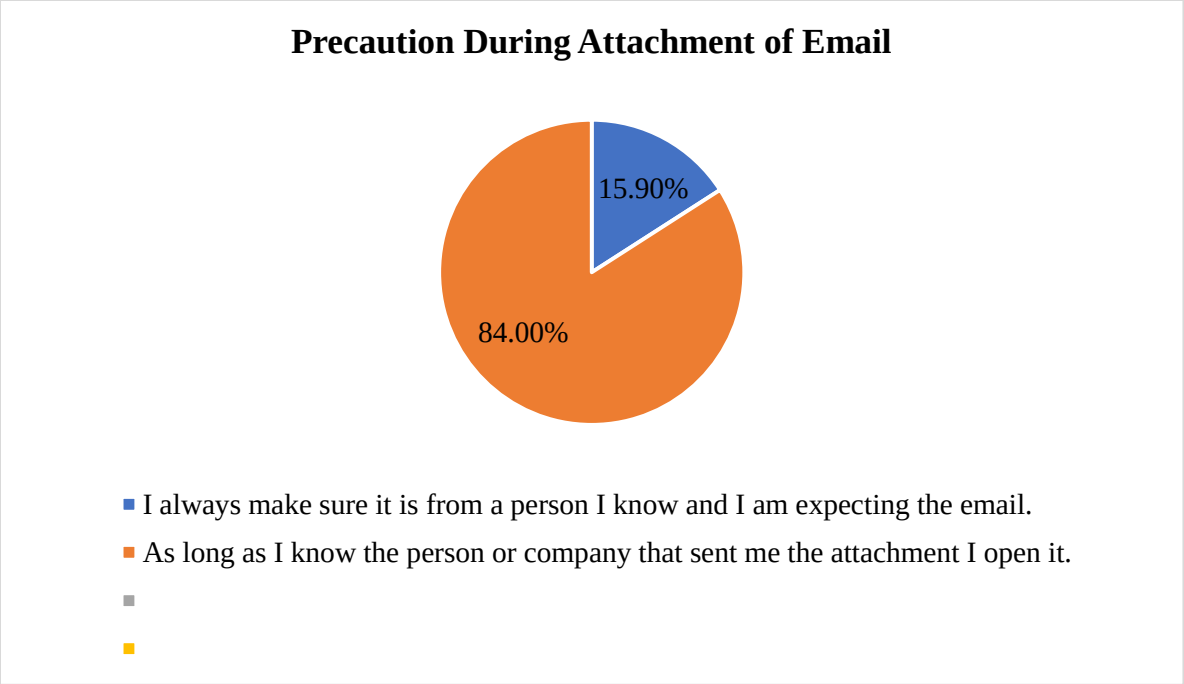

Figure 14: Distribution of Precaution Taken When Attaching on an Email

Accessing connection to a cyber system is an important component of cyber security practices. The device to connect to and the place of connection (internal or remote) is very critical. With remote connections the connection could be insecure since the system would be exposed to threats and have no security as the premises.

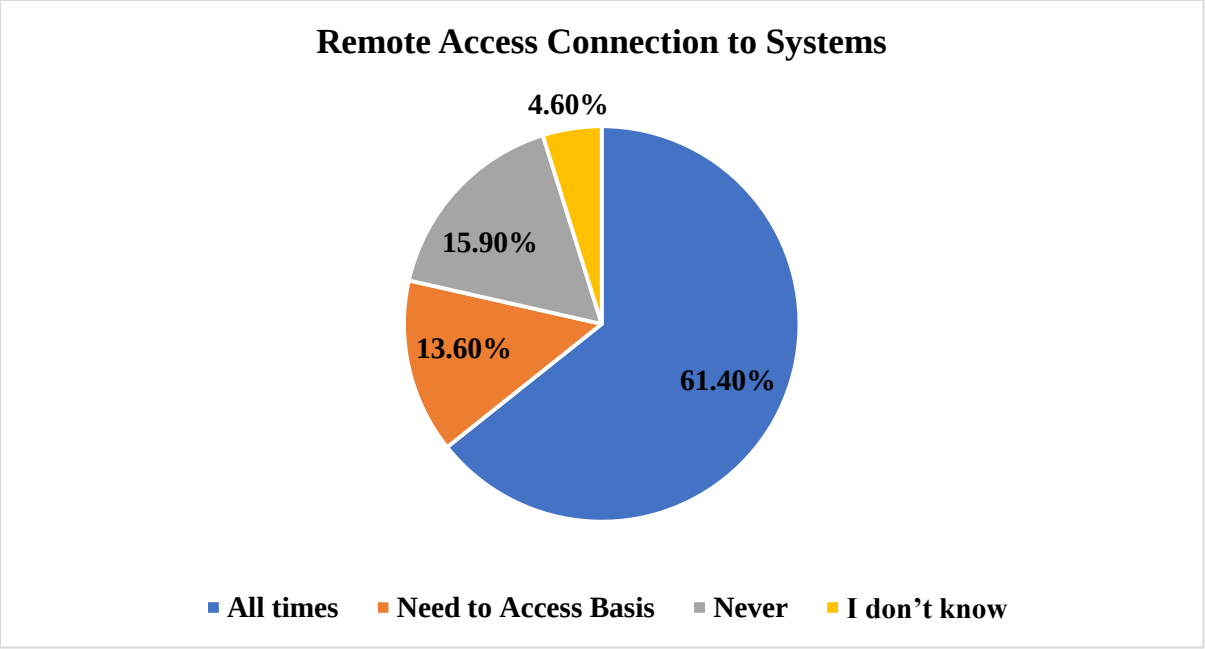

Figure 15: Distribution of Accepted Remote Access Connections

From Figure 15 above majority of the respondents representing 61% indicated that they could access their cyber system remotely all the time. 14% indicated that it was dependent on the need to access while 16% indicated that they could never access it remotely. This shows that generally staff access their banking systems remotely most often.

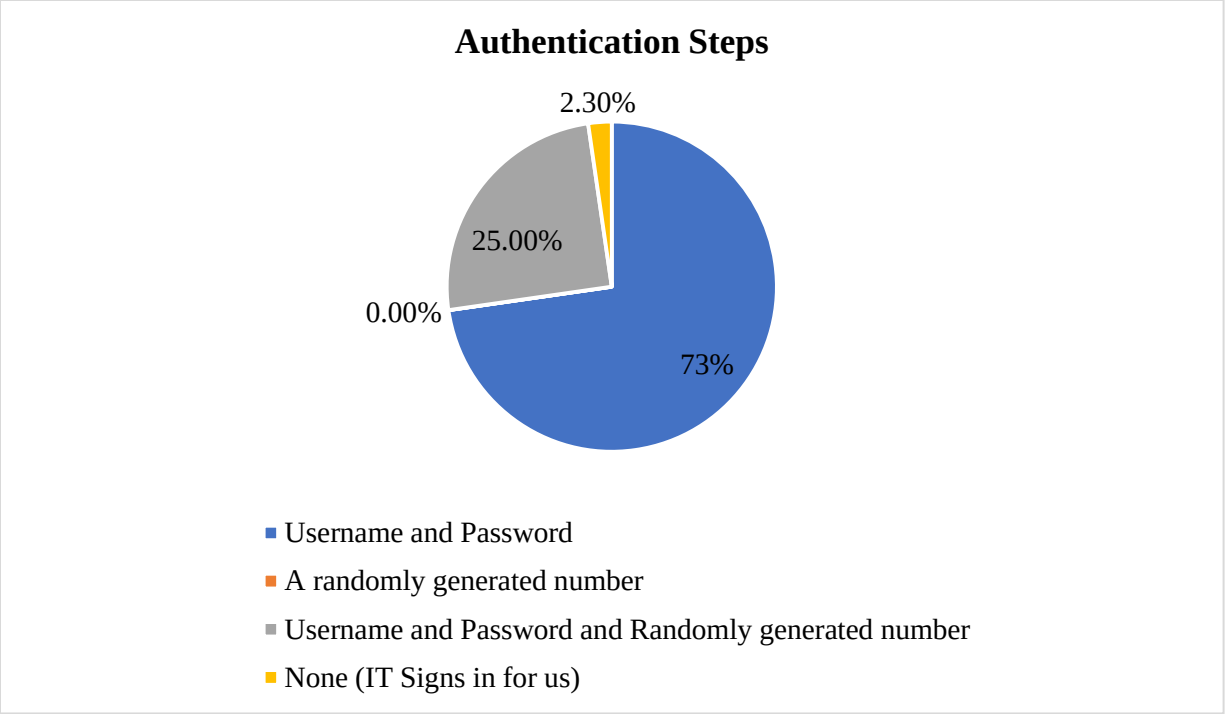

Figure 16: Distribution of Authentication Steps

In order to access a system, there is a need to authenticate the user. A total of 73% of respondents indicated they use their username and password to obtain access. 25% indicated they use a combination of username and password with a randomly generated number. 2.3% indicated that the IT personnel obtained access for them.

Devices allowed on a bank's cyber system is very important. Devices other than the banks protected devices are not supposed to be put on the cyber system. The study found that almost 80% of its respondents indicated that no device was allowed to be put on the cyber system of their organizations. However, some respondents, representing 15%, 13% and 7% said their laptops, phones and tablets respectively were allowed to be put on their corporate or banks cyber system or network.

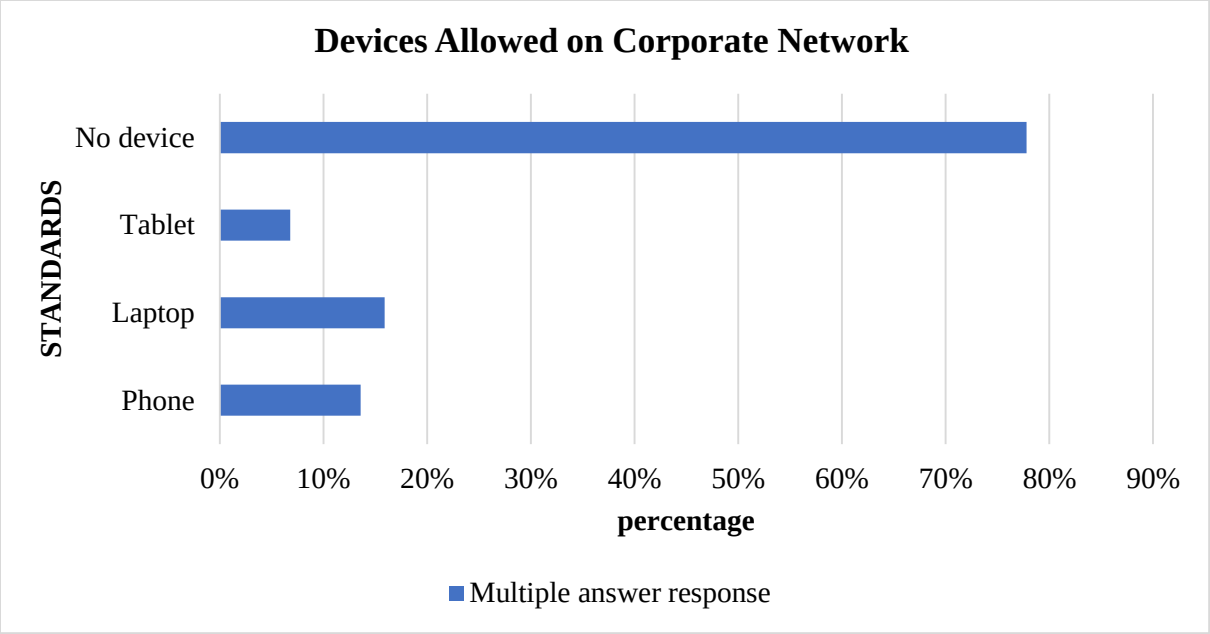

Figure 17: Distribution of Allowed Devices on the Corporate Network

From the study 50% of respondents indicated that their longest server downtime was less than one hour. 20% said it was between 2-5 hours. 9% of respondents each said the longest server down time was between 6-12, about 24 and no server downtime. From the results it can found that servers only go off for a few minutes to hours.

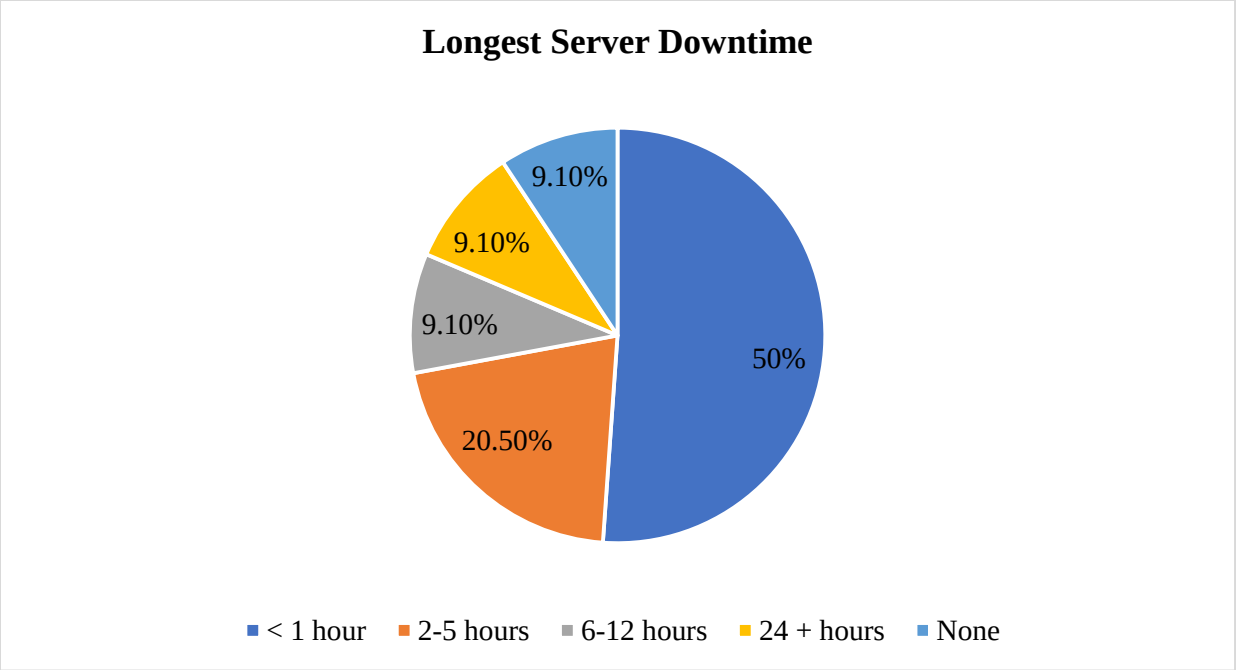

Figure 18: Distribution of Longest Downtime of Server

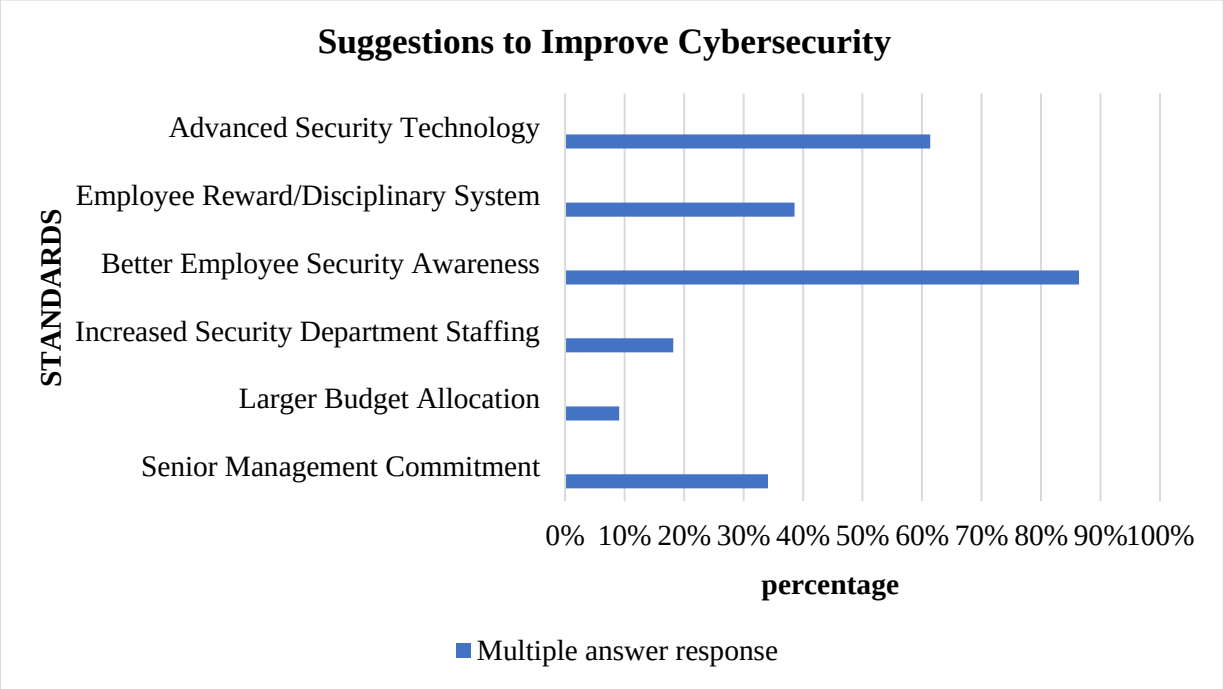

Figure 19: Distribution of Suggestions to Improve Cybersecurity

Finally, the study sought to solicit suggestions from the respondents on how they thought the cybersecurity of their organizations could be improved. About 85% indicated that there was a need to improve the awareness and knowledge level of staff. This would reflect in some of their practices and their adherence to some laid down protocols. 60% also said that there was a need to adopt or acquire advance security technologies due to the rapid change in technologies. About 40% of respondents said Employee reward/Disciplinary system had to be reviewed to increase the incentive to be adhere to protocols and disincentive to disregard the protocols for cybersecurity. Some respondents, representing 32% also indicated that senior management needed to be more committed to cybersecurity. 20% also said the capacity of the security department needed to be improved by employing more staff. Lower that 10% also said there was a need to increase the budgetary allocation for cybersecurity since most of these measures bored down to extra expenditure.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

A summary of the work is presented in this chapter. This is followed by the conclusion and recommendations. Conclusions are based on the research findings and are in line to the research objectives stated in chapter one. At the end of the work some recommendations to the conclusions are provided. These are both policy and research recommendations.

5.2 Summary of major findings

The study sought to delve into the practices of financial institutions in Ghana in dealing with cyber threats and preventing cybercrime. The main aim of the study was to investigate the practices, awareness and compliance level to the new cyber-security directive among the foreign banks operating in Ghana. Specific objectives were **t**o assess the level of awareness of Cyber Security among Foreign banks; assess the practices of cyber security risk management among Foreign banks and finally assess the level of compliance to the Cyber Security directive among Foreign banks.

A detailed review of literature in the field of cyber security in financial institutions was conducted. The qualitative study approach was mainly used for the study. This was however augmented with quantitative analysis where necessary. A cross-sectional data for bank's operations were collected from selected staff of banks (respondents of this study) by administering a well-structured questionnaire by well-trained enumerators. The questionnaire collected data on the banks' cyber security practices, their compliance, and knowledge of the

cyber security directive from the central bank as well as certain professional characteristics of the respondents. A multistage sampling technique was used to arrive at the final respondents for the study. All foreign banks operating in Ghana were censused. Since all foreign banks operate in the Greater Accra Region, they all were selected. The next stage was to purposively select which branch of these banks were to be visited but data was collected from some head offices.

The study had a total of 46 respondents from 13 foreign owned banks. With respect to position of respondents' majority were officers. Majority of respondents had had between one to 15 years working experience. However, most of the respondents had been with their current organization between 1-5 years. This illustrated that most respondents were experienced and had been in their current organization for more than a year hence they knew the systems and procedures well.

All respondents indicated they knew there was a policy on cybersecurity. About a quarter of the respondents said they had high knowledge followed by moderate, and low knowledge respectively. About half of the respondents said they had average knowledge of the cybersecurity policy. In order to verify the knowledge of the respondents to their organization's cybersecurity policy, we sort to know the standards or framework adopted. Majority indicated that they had no idea of the standards their organization was using. The rest indicated that their organizations adopted ISO 27001, PCI-DSS2, ISO 27032, NIST and ISO 27001.

More than half of the respondents indicated that the regulator required all banks to safe guard against cyber attacks. These were followed by those who got the awareness from presentations, seminars and conferences they had attended. About a third indicated clients had raised the issues. A total of 55.8% of the respondents said they had been involved in a cybersecurity drill in the past. From the study, most of the respondents indicated they use biometric access control at their

organization and the rest indicated no. About a half of the respondents indicated that the use of the biometric access control was not the only access control used in their organizations but it was used in combination with other access control systems. Also, (55.8%) of the respondents did not know the effect of such penetrating test and therefore did not recognize the need as to 41.9% who indicated this was a needful trial.

A total of about 60% indicated they had undergone security incident reporting process exercise which was intended to train staff on how to report a cyberattack. Also, about half of the respondents said they had undergone training on how to manage spam when communicating via emails. Some had undergone training on how to respond when there is a cyberattack. Majority of respondents indicated that the situational awareness was document. This was the most document, followed by information security strategy, cyber incident response plans, information security governance, information security roadmaps.

From the results of the study, some of the respondents indicated they reported issues of cybersecurity to their chief information officer (CIO). Others reported it to the Head of IT, in this case some banks said the Head of IT was similar to a CIO or they had no CIO in their ranks. In terms of how to detect flaws, majority of the respondents indicated that, internal auditing was the means used to detect flaws in their cyber system was found. The other means of detecting flaws includes formal risk analysis, penetration tests, external audit, informal risk analysis and regulatory works.

Most respondents indicated that they could access their cyber system remotely all the time. A similar proportion of respondents indicated they use their username and password to obtain access. Others indicated they use a combination of username and password with a randomly

generated number as well as that the IT personnel obtained access for them. The study found that respondents indicated that no device was allowed to be put on the cyber system of their organizations. However, some respondents, said their laptops, phones and tablets respectively were allowed to be put on their corporate or banks cyber system or network. From the study half of the respondents indicated that their longest server downtime was less than one hour.

Majority of the respondents indicated that there was a need to improve the awareness and knowledge level of staff. This would reflect in some of their practices and their adherence to some laid down protocols. About half also said that there was a need to adopt or acquire advance security technologies due to the rapid change in technologies. About 40% of respondents said Employee reward/Disciplinary system had to be reviewed to increase the incentive to be adhere to protocols and disincentive to disregard the protocols for cybersecurity. Some respondents, representing 32% also indicated that senior management needed to be more committed to cybersecurity. 20% also said the capacity of the security department needed to be improved by employing more staff. Lower than 10% also said there was a need to increase the budgetary allocation for cybersecurity since most of these measures bored down to extra expenditure.

5.3 Conclusion

Most respondents who were staff of foreign banks knew there was a cybersecurity policy and were aware of it. But a further probe showed they did not have much information on the policy. Knowledge regarding the standards and framework used was not readily known by most respondents. This therefore calls for education and training regarding the cybersecurity.

Generally, the regulator, Bank of Ghana created the most awareness. Even though this was a good thing, other sources need to be strengthened because they had the means to create awareness and increase the knowledge level in cyber security. It is expected that every staff should have at least gone through a cybersecurity drill in the past year, but about only a half had undergone a drill which is low. This was also the case with reporting exercises of cyber-attacks. This shows a relatively low preparedness for a cyber threat.

Internal Audits was the main means to detect cybersecurity threats followed by formal risk analysis and penetration test. Over half of respondents said they could remotely access the cyber system of the organization. This is however not a good practice to be encouraged. But however, most devices apart from the organization's computers were allowed on the system. This improves security and prevents threats. Downtimes experienced were relatively short but much could be done to minimize it since some had recorded over 12 hours of downtime.

5.4 Recommendation

There should be intensification of improving knowledge and keeping staff update with cyber security issues and systems. This could be achieved through routine training programs, seminars or conferences. Both the bank and the central bank have to make it mandatory for every bank staff to undergo some level of cyber training. Heads of IT departments or those in charge of cyber systems can create inter departmental trainings for staff on basic cyber security procedures.

Drills and exercises in instances of cyber-attacks are an important step towards dealing with a cyber-attack. These exercises ought to be embarked on more regularly and all staff must be

involved so no one is left out. This would relatively improve the level of preparedness for a cyber threat.

Cyber systems need to be audited internally and more frequently to expose loop holes or threats in the systems being used by the banks. This could also be augmented with external audits and risk analysis. This would keep the systems up to date with the improvement and new ways of cyber criminals. There is a need to improve and share cases of cyber-attacks with industry experts to study the cases and provide solutions as well as disseminate it to other institutions.

REFERENCES

Adeyinka, O. (2008), "Internet Attack Methods and Internet Security Technology," *Modeling & Simulation, 2008.AICMS 08. Second Asia International Conference on*, vol., no., pp.77-82, 13-15 May

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, *29*(3), 408-433.

Charles P. Pfleeger, Shari Lawrence Pfleeger (2003) Security in Computing, *Chapter 1; Is There A Security Problem in Computing.*

Chau P. and Lai V., (2003). An empirical investigation of the determinants of user acceptance of internet banking.

Choo, K. K. R. (2011). Cyber threat landscape faced by financial and insurance industry. *Trends and issues in crime and criminal justice*, (408), 1.

Cole, K., Chetty, M., LaRosa, C., Rietta, F., Schmitt, D. K., Goodman, S. E., & Atlanta, G. A. (2008). Cybersecurity in africa: An assessment. *Atlanta, Georgia, Sam Nunn School of International Affairs, Georgia Institute of Technology*.

Cybercrime costs global economy $445 billion a year: report". Reuters. 9 June 2014. Retrieved 17 June 2014.

Drigă, I., & Isac, C. (2014). E-banking services–features, challenges and benefits. *Annals of the University of petroşani, Economics*, *14*(1), 41-50.

Halder, D., Jaishankar, K., & Jaishankar, K. (2012). Cybercrime and the victimization of women: laws, rights and regulations. Hershey, PA: Information Science Reference.

ITU, A Comparative Analysis of Cybersecurity Initiatives Worldwide, in WSIS Thematic Meeting on Cybersecurity. 2005: Geneva

Moore, R. (2005). Cybercrime: Investigating high-technology computer crime. LexisNexis.

National Pensions Regulatory Authority. 28 July 2017. *Approved List of Pension Fund Managers*.http://www.npra.gov.gh/images/pdf/NPRA_PUBLIC_NOTICE_ON_APPROVED_LIST_OF_PENSION_FUND_MANAGERS.pdf

Ofanson E. J. (Ph.D.), Aigbokhaevbolo O. M. (Ph.D.) and Enubulu G. O. (2010). The financial system in Nigeria: An overview of banking sector reforms. *AAU JMS Vol. 1, December*

Richardson, R., & Director, C. S. I. (2008). CSI computer crime and security survey. *Computer security institute*, *1*, 1-30.

Richardson, R., & Director, C. S. I. (2008). CSI computer crime and security survey. *Computer security institute*, *1*, 1-30.

Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Wada F., Longe O. and Danquah (2012), actions speakslouder than words – understanding cybercriminals behaviour using criminological theories. *Journal of internetbanking and commerce*, April, vol. 17, no 1

Wiener, N. (1948). Cybernetics. *Scientific American*, *179*(5), 14-19

Zlatanov, N. Computer Security and Mobile Security Challenges.

APPENDIX 1

QUESTIONNAIRE

UNIVERSITY OF GHANA BUSINESS SCHOOL

MASTER IN BUSINESS ADMINISTRATION - FINANCE

I am a student of the University of Ghana Business School and would like to find about the cyber security awareness and practices of your organization. Your identity/name will not be referred to anywhere in the report. The information you give will be used purely for academic purposes. Please respond to the following questions

1. What is your position in your organization? …….
2. How many years have you been in the banking sector?.....

a. 1-5 years

b. 6-10 years

c. 11-15 years

d. over 15 years

3. How many years have you been in your current organization? …….

a. 1-5 years

b. 6-10 years

c. 11-15 years

d. over 15 years

4.What is your level of knowledge on your bank's cyber security policy?

a. Low

b. Moderate

c. Average

d. High

e. Very High

5.Which of these frameworks and/or standards are you aware of?

- ISO 27001
- NIST
- ISO27032
- PCI-DSS[2]
- FIPS-140

6.Which of the following (policies / procedures) has your organisation documented and approved (multiple answers possible)?

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

7.Who does your information security organisation's executive(s) report to?

- Directors
- Others
- Chief Executive Officer (CEO)
- Reports not available
- Chief Financial Officer (CFO)
- Chief Information Officer (CIO)

8.Does your organisation share information on information security attacks with third parties?

Yes/No/Not applicable

9.How do you highlight information security weaknesses, risks and non-compliance in your organisation (multiple answers possible)?

- Input from peers
- Penetration testing
- Internal audit
- External audit
- Informal risk analysis
- Formal risk analysis
- Input from vendors
- Assessment ofregulatory (non)compliance
- Others
- Not applicable

10.What has raised your awareness of information security attacks (multiple answers possible)?

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

11.What maturity level is your organisation currently at?

- Level 1 -Basic: undocumented, dynamic change, ad hoc, uncontrolled and reactive, individual heroics
- Level 2 -Repeatable: some processes are repeated, perhaps with reliable results, poor discipline process, agreed benchmarks.
- Level 3 -Fixed: a set of defined and documented standard processes, some degree of improvement over time.
- Level 4 -Managed: benchmarking process, effective management control, adaptation without losing quality.
- Level 5 -Optimised: focus is on continuous improvement and innovation.
- Information not available

12. What do you think will help improve your organisation's security levels (multiple answers possible)?

- Senior management commitment
- Larger budgets
- Increased security department staff numbers
- Better employee security awareness
- Employee reward / disciplinary systems
- IT steering committees
- Advanced security technology
- Others

Assessing the practices of cybersecurity risk management in banks

Personnel and responsibilities

13. Who do you contact in case you are hacked or if your computer is infected?

a. CISO b. SA c. Supervisor d. friend

14.How careful are you when you open an attachment in email?

a. I always make sure it is from a person I know and I am expecting the email.

b. As long as I know the person or company that sent me the attachment I open it.

c. There is nothing wrong with opening attachments

Encryption of data (end-to-end)

15.When moving sensitive data from one system to another, what do you do?

a.employ encryption b. use antivirus c. use anti-malware d. just copy to a pendrive

Remote Access authentication and identification

16At which times does your organisation allow remote access connections to systems.

a.all times b. need to access basis c. never d.i don't know

Internet Access and configuration

17.Which devices are you allowed to bring and use on the corporate network?

a. Phone b. Laptop. C. Tablet d. No device

18. Are you aware of a BYOD(Bring your own device) Policy?

a.Yes b. No

Access Control and Authentication

19.Are you able to us your access token(card, biometric, etc) to access all departments?

y/n

20.Which of the following are you able to access on the corporate network using your workstation?

a. Server List

b. Configurations

c. All departmental folders

d. Website folder

Biometric Authentication

21. Does your organisation use a biometric access control system? y/n

22. If yes, is it the only access control mechanism used? y/n

Servers and Work station installation and operation

23.What is the longest server down time your organisation has encountered?

a. 0-1hrs

b. b. 2-5

c. c. 6-12

d. d. 24+

e. e. none

Software Information Security

24. Is penetration testing used for helping or for damaging a system?

A. Damaging

B. Helping

C. I don't know

25.How many authentication steps do you follow to access core applications in your organisation?

a. Username and Password only
b. a randomly generated number
c. username and password and a randomly generated number
d. none -IT signs in for us.

Preparedness

26.Have you been involved in a cybersecurity drill in the past?

Yes/No

27.Which of the following exercises have you been involved in, with your organisation in the past year

a. Spam training
b. Security Incident response process
c. Security Incident Reporting process
d. None of the above

Research

28.Choose all that apply to the objectives of cybersecurity

a. Confidentiality
b. Integrity
c. Availability

d. Non-repudiation

e. Situational awareness