TECHNICAL VOCATIONAL EDUCATION AND TRAINING INSTITUTE -ADDIS ABABA, ETHIOPIA SCHOOL OF GRADUATE STUDIES FACULTY OF ELECTRICAL ELECTRONICS & INFORMATION AND COMMUNICATION TECHNOLOGY...

Bayu Gezahegn Zewude
Openo Polytechnic college

TECHNICAL VOCATIONAL EDUCATION AND TRAINING INSTITUTE - ADDIS ABABA, ETHIOPIA

SCHOOL OF GRADUATE STUDIES FACULTY OF ELECTRICAL ELECTRONICS & INFORMATION AND COMMUNICATION TECHNOLOGY

ASSESSMENT ON CHALLENGING THREATS OF CYBER SECURITY AND ITS EMERGING TRENDS Development Bank of Ethiopia

By:

BAYU GEZAHEGN ZEWUDE

August, 2020

Addis Ababa, Ethiopia

TECHNICAL VOCATIONAL EDUCATION AND TRAINING INSTITUTE - ADDIS ABABA, ETHIOPIA

SCHOOL OF GRADUATE STUDIES FACULTY OF ELECTRICAL ELECTRONICS & INFORMATION AND COMMUNICATION TECHNOLOGY

ASSESSMENT ON CHALLENGING THREATS OF CYBER SECURITY AND ITS EMERGING TRENDS ON SELECTED ETHIOPIAN BANKING

A Thesis Submitted to School of Graduate Studies of Technical Vocational and Education Training Institute

In Partial Fulfillment of the Requirements for the Award of Master's degree in Information and Communication Technology Management.

By: BAYU GEZAHEGN ZEWUDE

Advisor: Prof. P G V SURESH KUMAR, (PhD)

August, 2020

Addis Ababa, Ethiopia

TECHNICAL VOCATIONAL EDUCATION AND TRAINING INSTITUTE - ADDIS ABABA, ETHIOPIA

SCHOOL OF GRADUATE STUDIES FACULTY OF ELECTRICAL ELECTRONICS & INFORMATION AND COMMUNICATION TECHNOLOGY

ASSESSMENT ON CHALLENGING THREATS OF CYBER SECURITY AND ITS EMERGING TRENDS ON SELECTED ETHIOPIAN BANKING

By: BAYU GEZAHEGN ZEWUDE

Name and signature of members of the examining boards

Prof. P G V SURESH KUMAR, (PhD)	P. G. V. Suresh Kumar	**August 27/2020**
Advisor	**Signature**	**Date**
Dr. Temtim Assefa , (PhD)		**August 30/2020**
Examiner	**Signature**	**Date**
Kasaye Tilahun , MSc		**August 27/2020**
Examiner	**Signature**	**Date**

Declaration

This thesis has not previously been accepted for any degree and is not being concurrently submitted in candidature for degree in any university.

I declare that the thesis is a result of my own study, except where otherwise stated. I have undertaken the study independently with the guidance and support of my research advisor. Other sources are acknowledged by citations giving explicit references. A list of references is appended.

28 08 20

Signature: ____________________

Bayu Gezahegn Zewude

This thesis has been submitted for examination with my approval as a university advisor.

P. G. V. Suresh Kumar

Advisor's Signature: ____________________

Prof. P G V SURESH KUMAR, (PhD)

Dedication

There are people in everyone's lives who make success in both possible and rewarding. This thesis is also dedicated to My lovely mother who passed away when I was a child, to my sister Melkame Gezahegn, and My beloved wife Ararse Tesfa. I'm dedicating this thesis to you because I would have never completed this thesis without your support, prayers and motivation. You have always had faith in me that I could complete a master's degree, I love you and will always be grateful. Thank you for always being there and understanding when I was not. I'll miss you when I leave, but you know where to find me.

Acknowledgements

First and foremost, I would like to thanks the almighty GOD for giving me the ability to do this research study. I would like to thank my research advisor Prof. Suresh Kumar for his suggestion, and guiding throughout my study. His comments and advice have helped me in keeping the right direction for my study.

My special thanks to my sister, Melkame Gezahegn, for giving me the encouragement and support to keep moving forward throughout my career in education and to Bro, Endalkachew Bayu , I am grateful for your help in my maturity as an academician you have prepared me in a good discipline, energetic and motivated person thank you ended. My special thanks also to all research participants, who have given me a time from their busy schedules specially to Ato. Kidus Lelisa, IT service directorate director, Ato. Mekuanent, IT security manager, Ato. Tesfaye Assefie, IT Technician at development bank of Ethiopia and My close friend Nemomsa Befekadu for their kind cooperation and assistance during my study.

It’s also my great pleasure to thank my colleagues Abebe Ayisan, Bilal Abadula and Mohammedamin Teshome for their awesome discussions with splendid humor and for sharing enlightening experiences during this study.

Finally, I want to thank my beloved wife Ararse Tesfa, I don’t have any words to thank you, without your love, patience and support this would not have been possible. Thank you for understanding that the hours spent immersed in this effort were for good purpose, and for giving me the encouragement to keep moving forward.

Bayu Gezahegn

August, 2020

Addis Ababa, Ethiopia

Abstract

Cyber security is basically the process of ensuring the safety of cyberspace from known and unknown threats. The International Telecommunication Union states that cyber security is the collective application of strategies, security measures, plans, threats administration tactics, engagements, training, paramount practices, assurance, and expertise that can be used to guard the information system, organization and related assets.

The motivation of writing this paper was therefore to assess and investigate cyber security challenging threats and its emerging trends in selected banking, specifically in selected bank for this study. The source of information was majorly studies conducted by other scholars related on cyber threats and cyber security challenges published in the various journals. The paper has gone ahead to highlight the major cyber security challenging threats common in the context of selected banking. The paper has also identified some of the commonly used cyber security measures used to handle the identified threats.

Descriptive data analysis techniques are used in SPSS version 23 on the data analysis using questionnaire. The survey indicated that the top-rated cyber security challenges are lack of expertise, inadequate enabling technology and poor leadership style, and absence documented of cyber security policy and standards. The survey also indicated that, job description employee does not include responsibility of cyber security, preparedness of cyber security low on growing emerging trends of cyber security, selected bank is not secured form cyber criminals, processes of implementing new technology documented is not available, the selected bank cannot conduct a cyber security study as financial institution, absence of protective measures to reduce the risk of cyber security.

Moreover, this research indicated that the selected bank is inadequately prepared to detect, prevent, and respond to cyber security threats and breaches. It is not only the technical issues that show a grim picture but the top management are not adequately prepared to prevent and respond to cyber security threats and breaches.

Based on the findings, attempts were made to propose cyber security framework to minimize the challenges faced by the selected bank based on INSA's critical mass cyber security requirement standard version 1.0 and NIST's framework for improving critical infrastructures cyber security version 1.1. Finally, conclusions and recommendations were made based on the findings of the surveys study.

Key words: Cyber security, Cyber threats, cyber security challenge in banking sectors, emerging technology of cyber security.

Table of Contents

List of Tables

List of Figures

LIST OFABBREVIATIONS

CIA - Availability, Integrity, Confidentiality

DBE – Development bank of Ethiopia

EBC - Ethiopian broadcasting corporate

ICT – Information and Communication Technology

IMF – International Monetary Fund

INSA – Information and Network Security Agency

ISACA - Information Systems Audit and Control Association

ISO – International Organization for Standardization

IT – Information Technology

ITSP - Information Technology Service Provider

ITU- International Telecommunication Union

NIST – National Institute for Science and Technology

SPSS - Statistical Package for Social Sciences

UNCTAD - United Nations Conference on Trade and Development

US –United State

CHAPTER ONE

INTRODUCTION

1.1. Background of the Study

Cyber security is one of the main concerns that banks have today. They get more digitized, and they undertake higher risks to be hacked. Huge databases with information about internal operations, customer data and all the sensitive facts may be lost if they do nothing to protect this all. The consequences of a security breach may be not only the loss of reputation but also negative implications for private and commercial customers according to (research in wall street journal, 2019).

Cyber security is a field which focuses on protecting computers, databases, programs and networks from unauthorized access, change or destruction. Cyber security intentions to offer as well as involves the capability to have influence on the actions and rules of cyberspace; this requires adequate knowledge for the stability, limitations and vulnerabilities of ICT, and improving the critical operating factors in cyberspace. In this modern world, this may require innovative, matured participation among developing countries at various levels of development. (Jawad & Shahzad, 2019). However, the analysis of administrative related cyber security issues increased the attention of some researchers but little attention has been paid by researchers regarding to cyber security and national development, mostly within the countries belief, those have to create their nation's security policies. Cyber security is big challenge for many countries including Ethiopia.

Responding to security incidents is becoming increasingly imperative in business environments. According to One-man (2016) study on data breaches reports that 48% of attacks involved malicious activity, 25% were due to negligent human factors, and 27% involved business and information technology process failures. The report indicates that the mean time to identify an incident is, approximately, 201 days and the mean time to contain an incident once discovered is 70 days. The reality is that the effects of a breach can be very destructive to an organization. (Grispos et al. 2017) stated that, destruction can be experienced in the form or ransom ware, system downtime, and intellectual property theft, reducing customer confidence, and facilitating attacks on other organizations.

For an effective cyber security, an organization needs to harmonize its efforts throughout its entire cyber system. Security counter actions help to safeguard the confidentiality, availability, and integrity of cyber systems by preventing asset losses from cyber security attacks as stated by (Franklin, 2011). Effects of cyber security failure leads to the loss of knowledgeable property, direct financial loss from cybercrime, loss of sensitive business information, interruption of operations, extra costs for systems' recovery, stakeholder's loss of on system confidence.

The process of safeguarding cyberspace is the main concern of cyber security. (Tonge, Kasture and Chaudhari, 2013) define cyber security as the activity of protecting information and data systems (networks, computers, databases, data centers and applications) with suitable procedural and technological security actions.

Muckin & Fitch, (2015) stated that the reality of cyberspace in the 21st century is that nothing is secure. The same author says cyber security risk has evolved from a single matter of protecting a computer network from outside intrusion or physical access, to protecting entire nations, its citizens and their most sensitive information. Therefore, cyber security is, the main concern of all nations across the world. Today everybody sends and receive any form of data may be an e-mail or an audio or video just by the tick of a key but did we ever think how securely our data is being transmitted or sent to the other person safely without any leakage of information? The answer lies in cyber security. Today Internet is the rapidly growing IT infrastructure in our every day's life.

Cyber security is, basically, the process of ensuring the safety of cyberspace from identified and unidentified threats. The International Telecommunication Union states that cyber security is the cooperative application of strategies, security actions, plans, threats direction tactics, arrangements, training, paramount practices, and assurance and expertise that can be used to guard the cyber system, organization and related assets. (ITU, 2009).

As Olayemi (2014) stated that cyber security is vital because government, military, commercial, financial, and health administrations gather, process, and store unprecedented amounts of data on computers and other devices. A substantial portion of that data can be sensitive data, whether that is intellectual property, financial data, personal information, or other types of data for which unauthorized access could have negative consequences.

The banking sector in Ethiopia is one of the rapidly growing sectors of the country's economy. This sector is among the leading industries in our country; that is becoming heavily dependent on information technology for its service delivery and other purposes. Banking business competition has stirred the advancement of services enabled by IT which in turn increased the information security risk. (Patrick, 2011).

Modern banking progressively relies on the internet and computer systems to operate their businesses and market exchanges, the threats and security breaches are highly growth in recent years. Insider and outsider attacks have caused worldwide businesses lost trillions of dollars a year.

Ethiopian banking system is one of the most undeveloped compared to the rest of the world. In Ethiopia cash is still the most dominant medium of exchange and electronic-banking is not well known. Proclamation No. 592/2008 does not allow outsiders to own and operate banks in Ethiopia. Hence presently there are no external banks operating in the country. Private commercial banks become the picture of the Ethiopian economy after the historical proclamation of licensing and supervision of banking business Proclamation No. 84/1994 of Ethiopia to undertake commercial banking activities. This proclamation is the basis of private banking in Ethiopia after the revolution.

Bogale (2016) says that computer networks enable financial institutions to operate at high level of efficiency. Private institutions highly depend on information technology for running their daily business. Governments tab in to the internet and computer networks for efficient data processing, storage and dissemination. Bogle (2016) in strengthening this concept that in many organizations, information technology has become crucial in the support, sustainability and growth of the business.

Cyber security breaches remain to grow in both frequency and sophistication for all industries, and the financial sector is mainly vulnerable. According to the report ITSP Magazine, 2018, financial services firms fall victim to cyber security attacks 300 times more frequently than businesses in other industries. Security breaches lead to lost revenue for a banking institution, interruptions in operations and loss of both reputation and customers.

Currently, financial sectors have is no cyber security standards provided and there is no clear guidance regarding what would constitute an acceptable minimum baseline body of cyber security knowledge for end users in the country regarding to managing cyber security risks. It is basically, a blueprint for building a cyber security package to manage risk and decrease vulnerabilities.

The previous US President Obama declared that the *“cyber threat is one of the most serious economic and national security challenges we face as a nation” and that “America's economic prosperity in the twenty-first century will depend on cyber security*” as mentioned in (Hailu, 2015).

Mullane (2017) stated that due to lack of studies in the area of information system security, it is difficult to know the exact statistical figure with respect to financial losses of the incidents.

The growing threat of the malicious insider has agreed to a number of long-term research projects on different sectors of the country. INSA identified several critical infrastructure sectors that require special attention in protecting the cyber space from any possible attacks. Some of them are: banking and finance, information and telecommunications, energy and defense base and related technological infrastructures among the infrastructure that needs special attention. (ENA, 2019).

The availability, integrity, confidentiality (CIA), well-known model for security policy development, used to find problem areas and required solutions for information security according to the scholar (Terry, 2013). Specifically, the bank should be able to ensure the following characteristics of information.

☞ Confidentiality: protecting against unauthorized disclosure and ensuring the authenticity of the data’s source. The property that information is disclosed to unauthorized individuals, entities, or processes

☞ Integrity: preventing unauthorized modification or the property of safe guarding the accuracy and completeness of assets.

☞ Availability: preventing against data delays and denials (removals) and ensuring accessibility to those authorized to do so.

1.2. Statement of the Research Problem

Challenges in banking sectors are numerous and inherently diverse. (G. Nikhita, 2018), said that in today's technical environment, many latest technologies are shifting the face of the mankind. But due to these emerging technologies we are unable to safeguard our private data in a very effective way and hence these days cyber-crimes are increasing day to day. G. Nikhita, (2018), strengthening this idea and said that, in our today's activity more than 60% of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a modern issue. Even the newest technologies like cloud computing, mobile computing, E-commerce, net banking also requests high level of security.

According to ITU, (2009) Ethiopian banking system is still immature compared to the rest of the world concerning with electronic payment, internet banking, telephone banking and online shopping. Such systems are in the early stage. The reason for this evolutionary development is being numerous, the main one that is cited by different scholar is cyber security threats and poor implementation of cyber security mitigation techniques are the main to be mentioned.

The major challenge in cyber security in banking industry is the skill and knowledge gap about the holistic approach of cyber security management, Due to this, most security requirements are derived by the external bodies than the bank's management according to Abiy and Lemma, (2012) studies. Therefore, identifying the cyber security challenging threats in banking sector is actual, immediate and concrete ideas for banking industries as well as for government of Ethiopia.

Literature in the area of cyber security shows that security culture is still in its early stages of development, especially in developing countries like Ethiopia. Thus, the establishment of an organizational cyber security culture is necessary for effective cyber security as cited by (Mohammed, 2009).

The researcher also identified that most of the banks don't conduct any cyber security awareness and training for their staff. The capability and readiness of Ethiopian government organizations to perform audits of cyber security is extremely low (Abiy and Lemma, 2012). According to Patrick, (2011) cyber security risk has evolved from a single matter of protecting a computer network from outside intrusion or physical access, to protect the entire nations and their most sensitive information. Cyber security is, therefore the main concern of developed and developing nations.

The United Nations Conference on Trade and Development (UNCTAD) indicated that developing nations have become staging grounds for attacks by cyber criminals due to the larger prevalence of unprotected systems. (Hailu, 2015). There are several instances of cyber-attacks, in order to combat cyber-attacks, the Ethiopian government enacted legal framework to reduce vulnerabilities.

According to expert of cyber security at INSA Dr. Henok, Ethiopia wants to develop well organized legal framework to challenge the ever-increasing attacks of cyber at the national level, that currently Ethiopia has no organized system to tackle cyber-attack. Another scholar, (Oliviah, 2019) mentioned that cyber security procedures of banking divisions which implement mobile and web to deliver services tend to have a weak security system that why many cyber criminals prefer to target online and mobile banking system. Besides this, Cyber attacker manages to hijack customer and employee’s information detail and use them to penetrate the security system of the bank under cover of the dark web to steal bank data and moneys.

The other study by Accenture in 2018 reviewed 30 major banking systems and found that all them had vulnerabilities reaching from insecure data storage to insecure authentication and code tampering. The report said that, each of them has at least one security risk, although 25% of them had a problematic with high risk of security errors. It means that there were difficulties with the insecure data warehouse, verification and code tampering. Finally found that the financial place is the most vulnerable to attack.

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

As stated by scholars (Reddy and Gander,2014) on their study of cyber security challenges and its emerging trends on modern technologies clearly stated that computer security is a big topic that is becoming more significant because the world is becoming extremely interconnected, with networks being used to carry out critical transactions. They also propose that there is no perfect solution for cyber-crimes, but we should try our level best to minimize and manage them in order to have a safe and secure future in cyber space. Even though this is true, we need to create a model benchmark strategy that can be used as a minimum requirement for cyber security solution as country.

Cyber operators in Africa do not have up-to-date technical security measures like anti-virus packages, and many of the operating systems used are not regularly patched as mentioned in the studies of (Kritznger & Solms, 2012; PWC, 2011). Generally, there is lack of resources to investigate cyber-crime and beef up required instruments to combat cyber security in Africa they said.

Although tremendous amount of effort and money is invested in research in areas of cyber security, Ethiopia is far from safe guarding its cyber space, additionally, many researches have been carried out cyber security in banking, and security strategies in terms of online banking in Ethiopia, but no research addressed challenges faced by cyber security in banking institutions specifically in trying to combat this kind of risk. From further survey of relevant literature, it has been found that there are no published studies specific to Ethiopia on the issues of cyber security challenging threats and its emerging trends in selected banking. Therefore, this study intends to fill these pertinent gaps in literature by assessing cyber security challenging threats and its emerging trends in selected bank of Ethiopia, to have a safe cyber space by identifying factors facilitating these threats, and propose enhanced cyber security framework to minimize the challenging threats of cyber security in banking sectors.

1.3. Research Questions

In this research, challenges faced by cyber security is identified to answer the following research questions. So that, this research answers the following questions.

- What are the current existing challenges of cyber security faced in ensuring safe cyber space at selected bank of Ethiopia?
- Are there adequate cyber security activities such as devising policy, standards, and procedures that govern the overall cyber security related activities at selected bank of Ethiopia?
- What tools are required to minimize cyber security attack at selected bank of Ethiopia?

1.4. Objective of the Research

1.4.1. General objective

The general objective of this research is to assess challenging threats of cyber security and Its emerging trends at selected bank of Ethiopia.

1.4.2. Specific objective

To achieve the above-mentioned general objective the following specific objectives are formulated.

- To assess cyber security challenging threats faced by selected bank of Ethiopia.
- To identify the existing practice of cyber security threats and emerging technology used by the bank.
- To examine employees' attitude towards cyber security policies and standards of bank accordingly.
- To recommend updated cyber security process and propose enhanced cyber security framework to minimize security vulnerabilities of the bank.

1.5. Significance of the Research

This research contributes to existing efforts in cyber security by identifying the challenging threats to selected bank of Ethiopia, in addition from this study the following will help banking sectors in Ethiopia.

- to understand in depth the cyber security challenging threats.
- The study shall serve as a guideline for developing and implementing cyber security framework for Ethiopia banking sectors.
- It enables all banks to have a common cyber security framework in Ethiopia.
- It adds a new way of thinking in the existing body of knowledge.
- It also serves for practitioners and researchers to conduct more comprehensive research in cyber security challenging threats and the emerging trends of technologies in Ethiopian banking sector.

1.6. Scope and Limitation of the Research

The scope of this research is that: due to time and other limitations only development bank will be considered. Other banks are out of the scope of this study. beside it would be more interesting if all banks and other financial sectors were included in the survey and opinion of INSA cyber security expert was incorporated.

During the study of this research the researcher face different challenges among that: difficult to travel place to place to observe the work of cyber security at head office, the absence of internet connection through the country and the current pandemic virus of Covid-19 among the challenges faced during the study. Another challenge is that; collecting data from others bank is difficult because the confidentiality cases they arise, even though student researcher explain the reason why this study is conducted the case of state of emergency are among the challenges faced during this study.

1.7. Motivation of the Research

The motivation to undertake this research is due to different main reasons. It is imperative to understand how cyber security can be effectively managed in banking sectors that can help the government to expand and enhance cyber security management.

With our rapidly evolving digital world and ICT infrastructure, cyber security threats are changing rapidly as well. It’s important for organizations to stay on top of the current best practices to secure their business. Despite this overall understanding, there is frequently an assumption that if security systems and processes are in place, that no further security measures are needed.

A recent report says, global chief executive officers believes investing in cyber security is important for building trust with customers. So far less than half of businesses worldwide are conducting audits of the third parties which handle their collected personal data. In other words, there is a chance an organization collecting personal data is not sure whether this data is being adequately protected.

1.8. Organization of the Thesis

This thesis constitutes five chapters. The first chapter is introduction part that contains, background of the study, statement of the research problem, research questions, objectives, significance of the study and scope as well as limitation of the study.

The second chapter is literature review which provides both conceptual and contextual ground knowledge related to the cyber security, challenging threat of cyber security in banking sectors and the other organizations which are related to the banking sectors. In this chapter cyber security challenging threats at global and national level are discussed, research journals, previous research thesis is reviewed. Moreover, this chapter briefly discusses cyber security research done by different scholars across Ethiopia, the neighboring country and related work, which are related to this study is included.

The third chapter presents the research design and methodology used in this study; sampling taken for the study as well as the ethical consideration taken to account during the study. The fourth chapter is, the data gathered from research participants is analyzed and its discussions on results are presented. Conclusion, recommendations and future area of the research are presented in the last and final chapter of the research that is chapter five.

CHAPTER TWO.

LITERATURE REVIEW AND RELATED WORKS

Introduction

This literature review provides a theoretical framework for cyber security management and a discussion which focuses on the research questions. This chapter starts by examining a definitional difference between information security and cyber security and theories of risk. Based on the theoretical underpinnings, this chapter goes on to outline various types of cyber threats and, more specifically, cyber security challenges against banking sectors.

2.1. Overview of Cyber Security

Cyber security has become the heart of modern banking in our world today, and information has come to be the most valuable asset to protect from insiders, outsiders and competitors. The application of information technology has brought about significant changes in the way the institutions in the banking sector process and store data. This sector is now composed to face various developments such as internet banking, mobile banking, e-money, e-cheque, ecommerce etc., as the most modern methods of delivery of services to the customers. However, Customers are very concerned about privacy and identity of theft. Business partners, suppliers, and vendors are seeing security as the top requirement, particularly when providing mutual network and data access. Banks' ability to take advantage of new opportunities often depends on their ability to provide open, accessible, available, and secure network services. Having a good reputation for safeguarding data's and information's will increase market share and profit. Banks are clearly responsible for compromised data in their possession that results in fraud. Therefore, banks have to be responsible for fake activity committed via the internet channel. (As cited in Pellitory, 2017).

2.1.1. What is cyber security?

In this section, definitions of information security and cyber security are discussed. Without a clear definition of key terminologies, further discussions may have limited value as a subject of sustained empirical investigation. The two terms, cyber security and information security are frequently used interchangeably without much distinction (Von Sols & Van Niekerk, 2013; Gout, Raghunathan, & Menon, 2011). However, these are not entirely similar concepts. It is the importance to look into ideas underlying the two concepts in order to measure the views formed around them.

Jung (2018) define cyber security, as protecting information and communication networks, and information from cyber-attacks or cyber threats that occur in the cyberspace or network. This definition emphasized protection from attacks and threats. In the other hand the (ITU, 2009) defined "Cyber security is the collection of tackles, policies, security concepts, security safeguards, guidelines, risk management methods, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets."

Raggad, (2006) define information security, as "the protection of information resources against unauthorized access". It means that only authorized people or ICTs should have access to information resources, such as data, hardware, software, and network. As one of the international standards, (ISO/IEC 27000, 2016) describes information security as the preservation of confidentiality, integrity and availability of information. Integrity, availability, and confidentiality (Known as 'CIA Triad') are depicted as three aspects of information that should be protected to achieve security goals.

2.1.2. Cyber security emerging technology

The extreme development in data volume, the continued increase in computing power, and the need to acclimatize and counter ever-evolving cyber threats has led to the emergence of new technologies (emerging technologies) which provide new tools and techniques to support business needs. Emerging technology such as artificial intelligence, machine learning, blockchain, behavioral biometrics, biometric authentication technologies and emerging cloud services can all be installed to detect and break cyber-attacks and particularly at a speed and scale that wouldn't have been previously possible. (Global Perspectives & Solutions,2019).

This study more strengthening this ideas and mentioned that, successful application of emerging technologies capabilities for cyber defense requires a robust, flexible governance and risk mitigation strategy, including roles and responsibilities, an accounting of emerging technology products, testing and security, enhanced monitoring and anomaly detection, knowledge of sharing platforms and continuous risk identification and mitigation plans. As businesses adopt products that use emerging technology to develop in-house products, a governance framework will manage both the adoption of the new technology as well as its potential risk.

2.1.3. Cyber Threats

Cyber-attack is any type of aggressive movement employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and or personal computer devices by various means of malicious acts usually originating from unidentified source that also steals, alters, or destroys a specified target by hacking into a susceptible system. These can be categorized as either a cyber campaign, cyber terrorism in different situation. Cyber-attacks can range from installing spyware on a computer to attempts to terminate the infrastructure of entire nations. Cyber-attacks have become increasingly sophisticated and dangerous as the Stuxnet worm recently demonstrated as cited in (Gawthorpe, 2017).

The forms of cyber security threats are; Insider Threats, VoIP PBX Fraud, Mobile Money Fraud, Cyber Espionage, Denial of Service attacks, Cyber Crimes, Data Protection, Spam, Cyber Attacks. Every business linked to the internet can expect to fall victim to cyber-crime at some point as criminals expand their ability to steal money directly or to turn stolen data into money. The losses which cost 445 billion dollars yearly are both direct and indirect, with many businesses citing downtime or lost productivity as a costly side-effect of some cyber-criminal activity. The top cyber security threats for 2015, according to European Union Agency for Network and Information Security. include the following: (ENISA,2015)

- Malware;
- Web-based attacks;
- Web application attacks;
- Botnets;
- Denial of service;
- Physical damage/theft/loss and
- Insider abuse

2.1.4. Threat Analysis

Threats can be defined as anything that would contribute to the tampering, destruction or interruption of any service or item of value. The analysis will look at every element of risk that could conceivably happen. These threats can be split into Human and Non-human elements. As shown in table 1 below.

Table 1. Human and non-human threats.

Hackers	Viruses
Theft (electronically and physically)	Fire
Non-technical staff (financial/accounting)	Electrical
Accidental Inadequately trained IT staff	Heat control
Backup operators	Temperature
Technicians, Electricians	Flood

2.1.5. Vulnerability Analysis

The goal of vulnerability analysis is to take what was identified in the gathering of information and test to govern the existing experience, whether current safe guards are adequate in terms of confidentiality, integrity or availability. It will also give an indication as to whether the proposed safe guards will be sufficient.

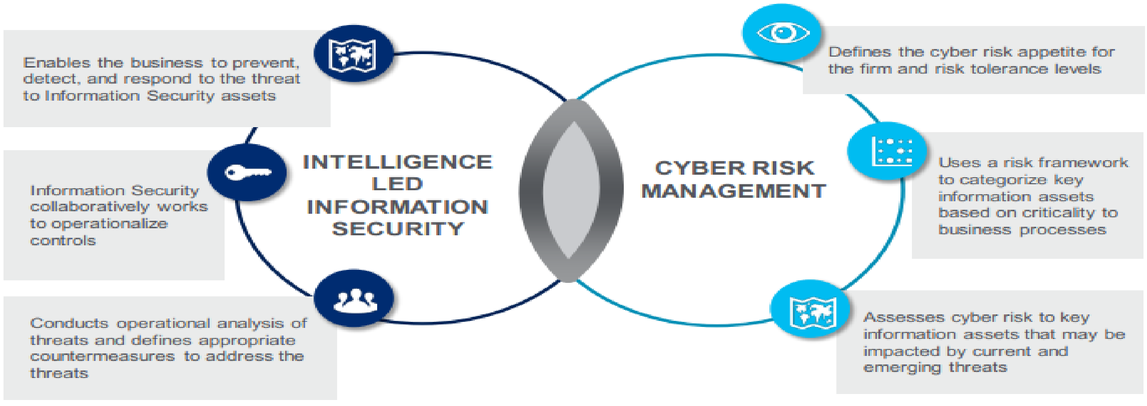
Most organizations are known to be performing vulnerability and network security assessment annually, biannually or quarterly thereby leaving their network vulnerable to intrusion. Vulnerability is defined as inherent weakness in design, configuration, or implementation of systems or network that renders it susceptible to a threat. The growth in number of vulnerabilities and exploits associated with new technology push organizations in conducting a more frequent vulnerability assessment (Rathaus, 2009).

According to Bharat (2005), vulnerability assessment is a systematic examination of a system to identify components that may be at risk of attacks and to determine appropriate procedures that can be implemented to reduce such risks. Vulnerability assessment whether manual or automated is a key component of security strategy and recognized as crucial part of network security.

2.1.6. How is Risk Assessed?

As stated in information security risk management, risk is assessed by finding threats and vulnerabilities, determining the likelihood and the influence for each risk. Unfortunately, risk assessment is a complex accountability, usually based on imperfect information. There are many procedures aimed at allowing risk assessment to be repeatable and give consistent results. (Richard, 2015).

Figure 1. Enhancing defensive posture by assessing cyber risk


Enables the business to prevent, detect, and respond to the threat to Information Security assets
Information Security collaboratively works to operationalize controls
Conducts operational analysis of threats and defines appropriate countermeasures to address the threats
INTELLIGENCE LED INFORMATION SECURITY
CYBER RISK MANAGEMENT
Defines the cyber risk appetite for the firm and risk tolerance levels
Uses a risk framework to categorize key information assets based on criticality to business processes
Assesses cyber risk to key information assets that may be impacted by current and emerging threats

Source: Citi GPS/ Global Perspectives & Solutions,2019

2.1.7. Cyber Security and Threats

The more exhaustive look at one of the common attack steps and its dependence on certain system access pieces, system knowledge and/or attack skills'. In accordance with the occurrence step definition, the exact nature of the preconditioned requirement and the attack result is specified. (Cherdantsevaa, et al., 2016).

Threats can be actions that can cause adverse harm to an asset of an organization. Cyber threats in specific cause harm to software, hardware or data. A common technique for categorizing threats was created by Microsoft called STRIDE according to (Muckin & Fitch, 2019).

- ☞ Spoofing – Impersonating someone
- ☞ Tampering – Modifying the system or its data
- ☞ Repudiation – Disputing who performed a specific action
- ☞ Information Disclosure – Accessing sensitive information without proper authorization.

- ☞ Denial of Service – Avoiding legal users from fully accessing a resource
- ☞ Elevation of Privileges – Gaining privileges without proper authorization

According to Accenture threat report, 2019 entitled “future cyber threats” there are five cyber threats affecting the financial sectors today. We assess how these threats are evolving and how they could create major lasting impacts for both organizations and the global sector at large. (future cyber threats, 2019). The threats featured are:

Credential and identity theft: Breaches of enterprise authorizations and consumer financial data continue to grow in frequency and scale. As the landscape changes, adversaries may use these large data sets in innovative ways, including simultaneous multiparty access and network abuse.

Data theft and manipulation: Financially, politically, and ideologically motivated adversaries have routinely stolen data from financial institutions. Well-resourced adversaries may evolve to incorporate data manipulation for financial gain, destabilizing financial systems and markets.

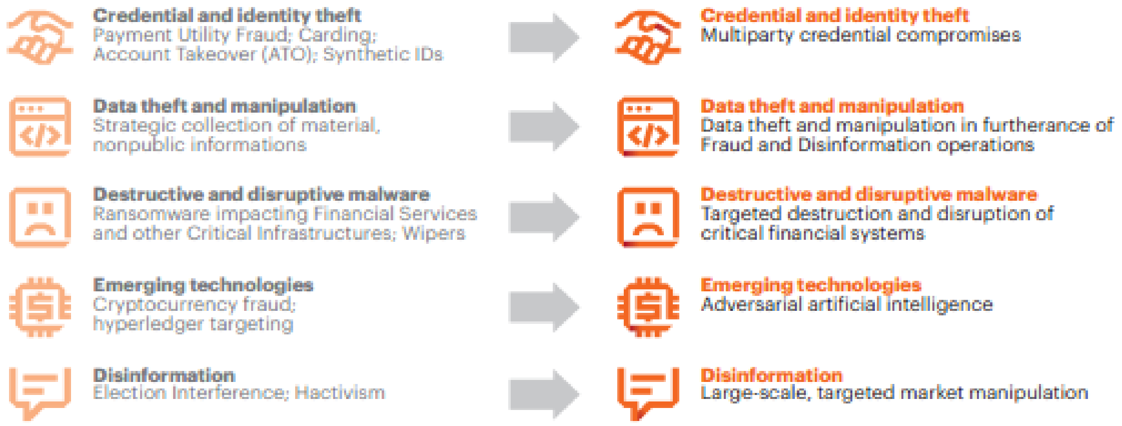
Destructive and disruptive malware: Adversaries are using ransomware attacks against the financial sector at exponential rates. Increased deployment has matched with threat opponents employing destructive malwares, pseudo-ransomwares and defense evasion techniques. Looking ahead, adversaries may deploy wiper malware to conceal their true intentions and stifle the incident response process during financially or politically motivated attacks.

Emerging technologies: Financial services organizations repeatedly discover applications of emerging technologies to deliver faster, extra secure and customer-centric services. Increasingly, as financial services organizations leverage blockchain and artificial intelligence, threat adversaries may seek to exploit these emerging technologies as part of a new wave of malicious campaigns.

Disinformation: Disinformation has played a role in movements of targeting financial institutions and markets since the birth of financial transactions. Combined with the other threats, disinformation may factor more prominently during highly targeted, multistage attacks.

Based on the current research and growing cyber threats, the Accenture security idefense threat intelligence services team highlights the following five threats as key for financial services sector: 1. Credential and identity theft, 2. Data theft and manipulation, 3. Destructive and disruptive malware, 4. Emerging technologies like Blockchain, cryptocurrency and artificial intelligence, and 5. Disinformation are some of the main threats of cyber security mentioned by Accenture.

Figure 2. Current and future state of the threat.


Credential and identity theft
Payment Utility Fraud; Carding; Account Takeover (ATO); Synthetic IDs
Credential and identity theft
Multiparty credential compromises
Data theft and manipulation
Strategic collection of material, nonpublic informations
Data theft and manipulation
Data theft and manipulation in furtherance of Fraud and Disinformation operations
Destructive and disruptive malware
Ransomware impacting Financial Services and other Critical Infrastructures; Wipers
Destructive and disruptive malware
Targeted destruction and disruption of critical financial systems
Emerging technologies
Cryptocurrency fraud; hyperledger targeting
Emerging technologies
Adversarial artificial intelligence
Disinformation
Election Interference; Hactivism
Disinformation
Large-scale, targeted market manipulation

Source: Accenture iDefence threat intelligence.

2.1.8. Cyber security threat sources and origins

Cyber threat sources include disaffected employees, investigative journalists, cybercriminals, extremist organizations, hacktivists, organized crime groups, and foreign intelligence services. (ITU, 2011). Among them, sources that attempt to target SMEs are employees, cybercriminals and organized crime groups. These sources engage in their cybercriminal activities to pursue economic gains or to express their hatred against an employer. Cyber security threats can be grouped into two types depending on origins of threats: internal threats and external threats. (Jang-Jaccard & Nepal,2014).

The previous research on cyber security did not pay much attention to insider threats compared to external threats. Internal threats refer to an intentional misuse of information systems by employees who have authorized access rights. This type of threat is based on the assumption that humans are the weakest link in cyber security management. (Guo, Yuan, Archer, & Connelly, 2011).

Workers are involved in up to 80% of information security incidents (Walton CB & Walton-Mackenzie Limited 2006). It is clear from these statistics that organizations are potentially losing profit as a result of incidents caused by their own employees.

This view is further supported by a survey conducted by price waterhouse coopers (PWC, 2004) which concluded that "human error rather than technology is the root cause of most security breaches". The effectiveness of internal controls designed to protect the integrity, availability and reliability of information and information technology systems depends on the capability and dependability of the people who are implementing and using them (Kruger & Kearney 2019).

2.1.9. Cyber Security Frameworks

Although there are numerous risk models and framework that straight attempt to address the cyber security issue and challenges, National Institute of Standards and Technology released a wide-ranging guidance on a wide range of security issues, and technical, operational and management security controls. The NIST cyber security framework well-defined five fundamental components of cyber security for a protection strategy. (NIST, 2014).

- Identify: Constant cyber threat identification, evaluation, and governance using techniques of management and risk assessment best practice.
- Protect: Structured, solid integrated safety architecture, perimeter network protection, host protection, network protection, device protection and remote connectivity safety.
- Detect: The ability to identify viruses and other cyber annoyances, as well as advanced cyber-attacks like APTs both within the network and within the scheme, and on each recipient.
- Respond: Well established and effective cyber-attack management procedures.
- Recover: Ability to return to normal or degraded operations quickly following an attack– the defense part after the fact, in depth. It is not feasible to avoid or react to certain cyber-attacks. Mostly, APTs and other disastrous assaults are cyber-attacks with an extremely small chance of occurrence and have a strong effect.

2.2. Role of social media in cyber security

As we become extra social in an increasingly connected world, companies must find new ways to defend personal information's. Social media plays a huge role in cyber security and will contribute a lot to personal cyber threats. Global Risks (2013) stated that social media adoption between personnel is skyrocketing and so is the threat of attack. Since social media or social networking sites are almost used by most of them every day it has become a huge platform for the cyber criminals for hacking private information and stealing valuable data. The ability of persons to share information with an audience of millions is at the heart of the particular challenge that social media brings to the current businesses. Global Risks (2013) further strengthening this concept, giving anyone the power to circulate commercially sensitive information, social media also gives the same power to spread false information, which can be just being as destructive. The rapid spread of false information through social media is among the emerging risks.

The greatest and common technology risk or threat to banking and financial institution is phishing attack according (Tarino et al ,2016). The characteristic phishing attack is based on social engineering, a tactic used by computer criminals to trick customers and employees into giving up confidential information like their account user names and passwords. With these credentials, the fraudster can penetrate networks, skim funds, and take over accounts.

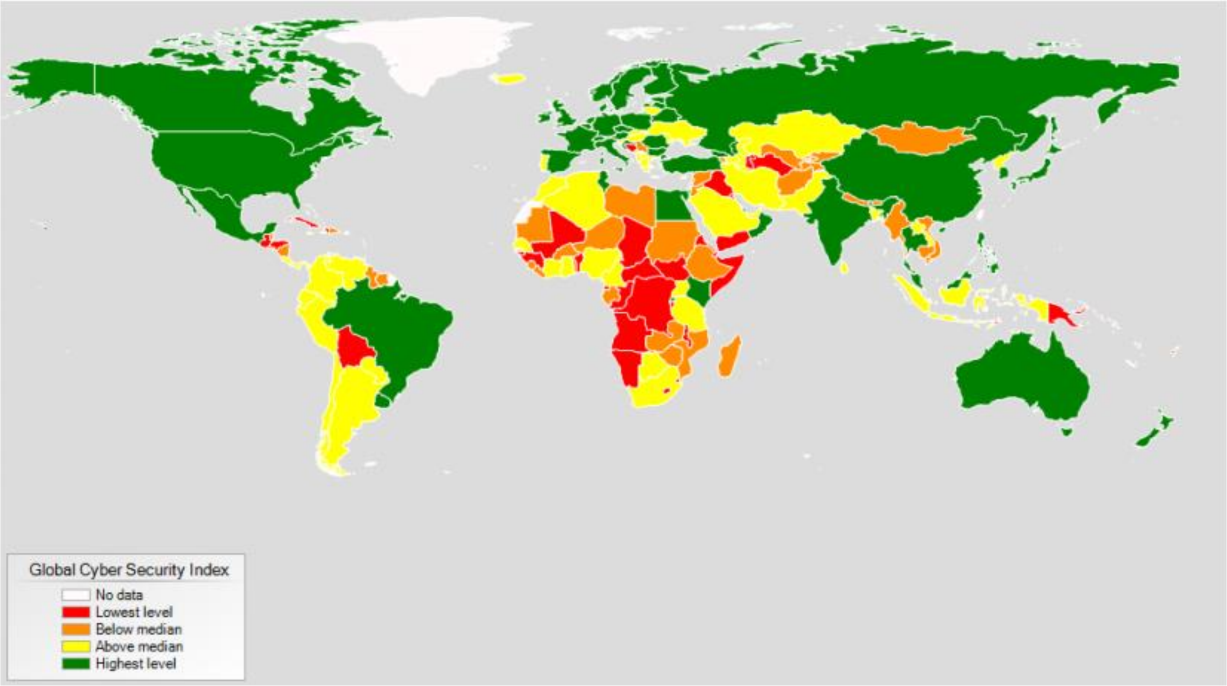
2.3. The role of managers and their leadership in cyber security

A growing body of cyber security studies addressed the role of senior managers. The role of senior management has been examined in relation to various organizational factors. Many studies found that senior management support was a significant factor in fostering cyber security culture within a business. (Knapp, Marshall, Rainer, and Ford (2006) found that top management support had a positive causal impact on both cyber security culture and policy enforcement. Leadership is the ability to influence a group in order to attain a set of goals (Robbins & Judge, 2013). It can be displayed by any member in a group and is not an exclusive province of a few members at the top. (Bass & Riggio, 2006). Even though all administrators are not considered as a leader.

2.4. Countries exposed to cyber risk

The financial area is highly exposed to cyber risk, across all types of the countries according to an agency of the United Nations, called international telecommunication unit that offers a global cybersecurity index for the world. Their catalogue is based on a diversity of factors, including legal, technical and administrative arrangements as well as capacity building and cooperation. (ITU, 2017). The figure below shows the cross-country heterogeneity regarding cyber security.

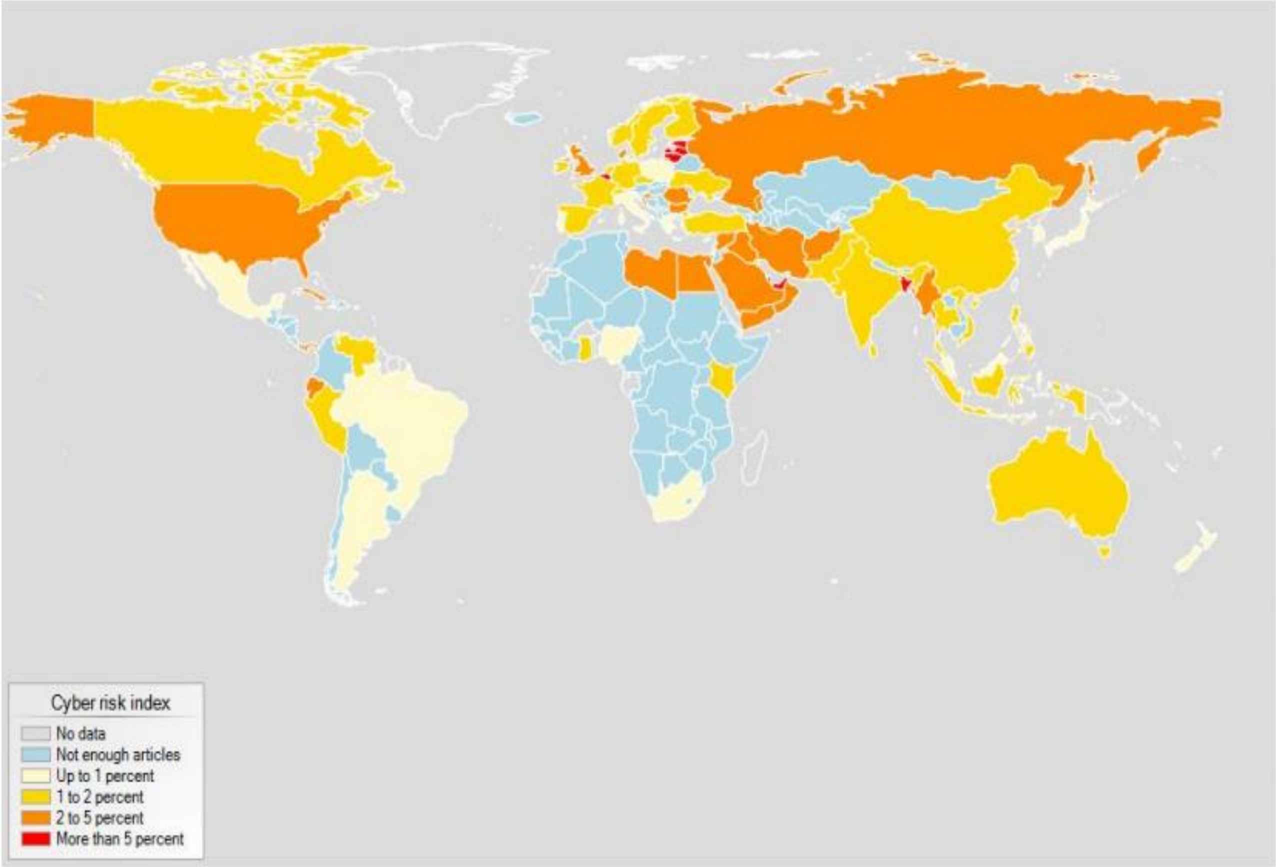
Figure 3. Cross-country heterogeneity regarding cyber security.



Source: ITU, 2017.

Since there is no quantifiable measure of cyber risk by country for the financial sector, we build an indirect measure using media coverage. An index is figured using the number of articles mentioning to cyber risk by country, divided by the number of articles referring to risk in the financial sectors. This unit said nothing about Ethiopia, since the article written regarding cyber security risk written about Ethiopia is below 25 articles. Hoping that, this study will fill the gap in identifying the cyber risk at selected bank.

Figure 4. Cyber risk index globally.



Sources: Factiva; and author’s calculations.

2.5. Information security

Information is one of a financial institution’s greatest important assets. Protection of information assets is essential to establish and maintain trust between the financial institution and its customers, maintain compliance with the law, and protect the reputation of the institution (Council, F.F.I.E, 2006). Similarly, (Tso, et al., 2013) specified IT systems contain a wealth of private financial information. These data are used as a shared secret between sectors and their information security has become respectively important. (McGlasson, 2007) stated that the most important part of a good organization IT security infrastructure is information security management. In order to protect the information assets and prevent fraud activities, the financial industries should design and implement information security strategies. For this kind of scenarios (McGlasson, 2007) suggested two solutions, the first is establishing information security management framework and the second is organizing information security awareness training program. Security of the information assets is a requirement for all types of organization, whether to protect the business or to meet legal or regulatory requirement as organizations are totally dependent on their IT systems to capture, store, process and distribute organization information (Jones, 2010). For this, information security is and has always been the discipline to alleviate risks impacting on the confidentiality, integrity and availability of a company's IT resources (Von Sols, 2012).

According to Gebrehawariat (2017) a successful organization should have the following multiple layers of security in place for the protection of its operations, this would also include the baking sectors too.

- Physical security – to protect the physical items, objects, or areas of an organization from unauthorized, access and misuse.
- Personal security – to protect the individual or group of individuals who are authorized to access the organization and its operations.
- Operations security – to protect the details of a particular operation or series of activities.
- Communications Security – to defend an organization's communications media, technology, and content.
- Network security – to protect networking components, connections, and contents.
- Information security – to protect the confidentiality, integrity and availability of information assets, while they are in storage, processing, or transmission.

2.6. Security policies, procedures, standards and guidelines.

Security policy outlines, what kind of security controls a company adopts and how they should be implemented, providing a direction and support to cyber security activities. Security policy theorists argue that cyber security policy should be established, implemented, and maintained as research studied by (Hong, Chi, Chao, & Tang, 2003). Creating a policy that reflects both internal and external contexts is just the start of cyber security management. Establishment of policy requires management concern and support toward cyber security. Policy should be formulated first, but implementation of it cannot be over emphasized. It is important for employees, to realize the significance of abiding by the policy. Once security policy is adopted, execution of the policy is in the hands of employees.

As new technologies are introduced, a policy needs to be changed accordingly. It is important to review the policy regularly with the changing business environments (Singh et al., 2013). This is because every new technology has its own security weaknesses along with business benefits.

ISO/IEC 17799 defines a policy as the "overall intention and direction as formally expressed by management". In other words, it is a document describing what management expects of employees in terms of protecting information assets and is usually not technology specific. An example is an information security policy stating that access should be controlled. A procedure provides the detailed steps of a component mentioned in a policy, for instance the process of granting access and distributing passwords. A standard detail the minimum requirements, for instance that a password must be at least 8 characters long and consist of alpha-numeric characters. A guideline is a document that assists management in the implementation of information security.

2.7. Cyber security attacks targeting financial institutions

Financial institutes have been a profitable target for cyber criminals, because of the massive volumes of data and money that can be stolen according to Help Net Security, (2016). As our civilization continues to operate more and more online (mobile banking, online banking, online shopping, the cloud). Cyber criminals have improved potential routes to breach businesses' defenses. Data breaches can have long-lasting harmful effects for any business, regardless of its industry. A 2017 report by the pokémon institute and IBM revealed the average total cost of a data breach in the U.S. reached a record breaking $7.35 million, which is 5% increased, from the previous year according to the report of IBM, (2017). However, when it comes to the financial sector, those costs can be exponentially larger.

2.8. Cyber Security in the world

Global cyber security index / GCI/ (2017) stated that the global community is progressively embracing ICTs as key enabler for social and economic development. It further stated that administrations across the world recognizes that digital transformation has the power to further the prosperity and wellbeing of their citizens. However, these enablers came with the possible threat for social, economic, and political wellbeing for every nation. Due to this (GCI, 2017) affirmed that governments recognize that cyber security must be an integral and inseparable part of technological progress. There are several global cyber security initiatives. Some of these are the Accenture security index, cyber security poverty index, IBM x-force threat intelligence index,

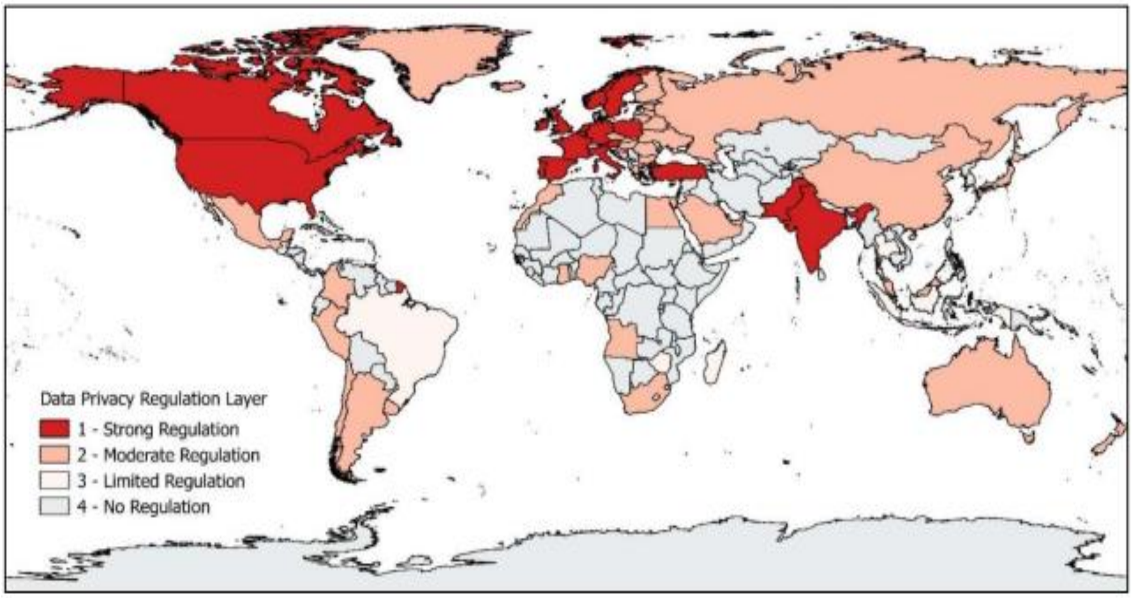
index of cyber security and global cyber security index are the some of the initiative to be mentioned.

2.8.1. Cyber security in Ethiopia.

Ethiopia needs to develop an efficient legal framework to tackle the ever-increasing cyber-attacks at the countrywide level, as stated by an expert on cyber security, Dr. Henok Mulugeta, Ethiopia has no organized system to tackle cyber-attacks. Developed countries which have well systematized technologies are exposed for the global cyber-attacks, due to the complexity of security nature.

Cyber-attacks have augmented from 479,576 to 791 per annum during the past three consecutive years in Ethiopia, which 15% of the attacks during the last nine months of 2018/19 were cyber hacking attempts. About 87.4% of the government institutions have not any recognized legal frameworks to tackle cyber-attacks though some 11.6% are being at their trial level. There is no well-developed and governed legal framework at the national level (ENA, 2019). Henok advised, the country to act quickly in cooperative manner as cyber security desires governance and management from the highest to the lowest level. The country needs a well-organized strategy for five or ten years to manage cyber security attacks otherwise, the influence will be become even worse.

Figure 5. Global Data privacy regulation across the world.



Note: data compile and reviewed from the following sources to create this map: privacy international (2018); Hedrich, et al. (2017)

Source: Cambridge center for Risk Studies.

Blocking financial services be it smart grids or infrastructures, losing public reliability, cyber terrorism, political crisis, economic crisis, national identity, society crisis and sovereignty related attacks. Mentioning to the news agency, head of cyber engineering at information network security agency (INSA), Tigist Hamid said that most of the attacks detected during the concluded Ethiopian fiscal year were web and infrastructural attacks. Causes of cyber-attacks are employees, partners, well organized criminal, cyber terrorists and government and non-government sponsored. Apart from lack of authorized frameworks, lack of awareness on cyber security, lack of well-trained human resources and there is poor cyber security governance at the institutional level (ENA,2019 news).

Head of cyber governance and management at INSA, Temesgen Kitaw said, for his part that considering the legal frameworks which other countries have been developed, Ethiopia has much to do. Stressing the complexity of cyber security which requires massive and well qualified man powers. After having said this, his institution is working in collaboration with the universities such as Addis Ababa and Mekele to manage the cyber security risk. (Source: from Ethiopian News Agency).

2.9. Related Works

There are numerous pragmatic researches across the world in areas of cyber security. In this study recent cyber security challenging treats are discussed.

Baino (2016) conducted a safety risk assessment survey related to networked information systems. The results of the research showed that a large proportion of safety lapses result from system administrators not updating software patches and failing to keep up with innovations in their business. He ascribed this system administrator's ineffectiveness to culture and workload, saying that in most instances system administrators are accountable for taking care of limitless different structures.

Kreicberga (2017) conducted a research on inner risk in tiny and medium sized businesses to data safety countermeasures and human factor. The results for the studies were that official policies that lack of adequate maintenance and consciousness do not affect staff conduct, while informal standards within the organization have the biggest influence on conduct in information security. Countermeasures to technological safety are more efficient and taken seriously if their necessity is described as an advantage to end customers.

Zegers (2016) conducted a survey on social technical views of ICT safety problems, trends and challenges to an ICT safety culture: case of Tanzania's. The research findings showed that cultivating a culture that is vulnerable to ICT safety is not a simple job and it is not a problem that organizations alone can address. Outside organizations, there are considerations that need to be addressed when it comes to ICT safety. For example, when it comes to training and awareness raising for ICT safety, elements such as a country's general education scheme and support structures need to be taken into account, which is similar to our country Ethiopia, we need to open cyber security department at university level since the issue of cyber security is global.

A case study of Kenyan tiny and medium-sized companies in the financial sector was conducted by (Makumbi et al, 2018) in a research entitled “Analysis of Information Technology safety practices”. The study aims were to determine the amount of reliance Kenyan SMEs have on ICT, identify the most common safety threats among Kenyan SMEs, and determine how Kenyan SMEs protect their PCs, data, and networks against information security hazards. The results of the research were that the organizations investigated were aware of the significance of safety of information systems and tried to put in place safety measures based on their dependence.

(Makumbi, 2018) on his thesis awareness ICT safety in selected organizations said that economic fraud appears to feature prominently among the reported events, computer asset loss seemed to be a recurring issue and system user danger was prevalent among the studied organization. The prevalent defense used against hacking is firewalls. The research suggestions were that such organizations should put in place numerous steps including task segregation, physical security controls, and IT asset inventories. The researcher suggested user awareness campaigns to raise awareness about ICT safety.

Njiru (2016) conducted a case study of Kenya’s banking sector on a framework to guide information security measures for banking information systems. The study seeks at identifying prevalent vulnerabilities influencing banking information systems, analyzing current frameworks used to assess safety programs and banking systems projects, identifying gaps in current safety investment frameworks, developing a structure to be used to assess safety programs for the banking industry and validate safety.

The research results showed that individuals are the greatest danger to information systems while clients have quoted lack of adequate communication, lack of skilled labor and security awareness as significant barriers to the efficacy of safety. Fraud, careless or unconscious staff and inner assaults have been quoted as threats that have enhanced the risk exposure of banks. The research found that the most significant thing in transforming information security is management and alignment of individuals, procedures and technology should be taken in to account.

The other empirical research conducted by (Halefom, 2015) with the thesis entitled “The state of Cyber Crime Governance in Ethiopia”. to discover the efforts and initiatives made by the government in fighting cyber-crime from three cyber space governance perspectives. Namely: cyber security related policies and strategies, legislative frameworks, and institutional arrangements.

Based on the empirical data collected and close examination of the legislations and policies, the study recommended on what plans and measures the government can implement in pursuit of safer and secure Ethiopia and built a conceptual framework for the article by citing different related works done by scholars.

Recently, (Tesfaye, 2018), on his research entitled “Cyber Security Auditing Framework for Banking Sector in Ethiopia” after collecting data from different banks and experts, he concluded his study by proposing cyber security auditing framework for the selected banks to be implemented. Even though cyber security is still a very complex field of research, with a lot of unexplored facts in the areas, the researcher proposed framework without comparing the other framework across the world as well as the challenges faced in banking is different.

Tewodros (2018), in his paper of “cyber security practices and challenges at selected critical infrastructures in Ethiopia: towards tailoring cyber security framework” , after collecting data from three critical infrastructures in Ethiopia and interviewing the expert of each critical infrastructures, he indicated that critical infrastructures face challenges: such as of lack of expertise, difficulty in locating the right security alert, inadequate enabling technology and evasion of existing security controls regarding with cyber security in Ethiopian infrastructures by mentioning the same study done across the world and comparing with security pillars across the globe.

Even though those issues are studied in critical infrastructures and financial sectors, the student researchers did not mention the current challenges faced by banking industries and they haven't discussed cyber security challenging treats in their research beside to the neighboring studies. As we mentioned in the above chapter, the literature shows that there is lack of local research that address cyber security challenging treats and its emerging trends in selected banking.

Table 2. Summary of the related work.

No	Name of the Authors and date	Title of the research	Objectives of the research	Findings of the research
1.	Tine Hojsgaard Munk (2015). A Thesis Submitted to the university of Manchester for Doctor of Philosophy in the faculty of Humanities.	Cyber-security in the European Region: Anticipatory Governance and Practices.	The aim of this research is to offer a greater insight in to the different forms of cyber security governance.	The author analyzes anticipatory governance and practices in European region, which are determined by the geographical position and cooperative regionalism considered for their involvement in three European Security institutions- North Atlantic Treaty Organization, The council of Europe, and The European Union.
2.	E Krizinger and SH Von Solms (2012). A research article published at	A Framework for Cyber security in Africa.	The objective of this paper is to propose cyber security framework to assist Africa in increasing	The authors identified four major safety concerns in Africa discussed in recent literature. Based on these four major cyber safety concerns, the

	Journal of Information Assurance & Cybersecurity.		its cybercrime rate especially among home users with no or limited cyber safety knowledge.	authors proposed a framework for cyber security in Africa.
3.	Yeboah-Boateng, Ezer Osei (2013). Thesis Submitted to Aalborg Univesitet Denmark for Doctor of Philosophy.	Cyber security Challenges with SMEs in Developing economies: issues of Confidentiality, Integrity, and Availability (CIA)	To mitigate the impact of cyber security compromises of Confidentiality, Integrity and Availability against their assets in developing economies.	Build a cyber security vulnerability assessment (CSVA) model and enlisting taxonomy of vulnerabilities and threats.
4.	Halefom Hailu (2015). An Empirical Research Article.	The State of Cyber Crime Governance in Ethiopia	Attempt to explore the efforts and initiatives being made by the government in fighting cybercrime from three cyber space governance perspectives: cyber security-related policies and strategies, legislative frameworks, and	Provided recommendations on what plans and measures the government can implement in pursuit of a safer and secure Ethiopia.

			institutional arrangements.	
5.	Aychiluhim Desta and Tibebe Besha (2014). A research article published at HiLCoE Journal of Computer Science and Technology, Vol. 2, No. 2	Internet Banking Security Framework: The case of Ethiopian Banking Industry.	To recommend holistic Multi-layered security that stretches towards client's side security and national financial and security.	The internet banking security framework and its major five security models have been developed and evaluated through expert evaluation method.
6.	Tewodros Getaneh (2018) A Thesis Submitted to the university of Addis Ababa University.	cyber security practices and challenges at selected critical infrastructures in Ethiopia: towards tailoring cyber security framework	To investigates the practices and challenges of cyber security to adapt, modify and tailor a cyber security framework for the selected critical infrastructures in Ethiopia.	critical infrastructures face challenges of lack of in-house expertise, difficulty in locating the right security alert, inadequate enabling technology and evasion of existing security controls.

7.	Tesfaye Asfaw (2018) A Thesis Submitted to the university St. Mary	Cyber Security Auditing Framework (CSAF) For Banking Sector in Ethiopia	proposing a cyber-security auditing framework that enables bank industries to perform effective and efficient cyber security auditing.	Ethiopia banking industries are at low level of readiness and majority of Ethiopia banking industries are lacking procedures.

2.9.1. Research Gap

Based on the above empirical literature review, it is evident that extensive research has been done which are related to the research topic in developed and neighboring countries such as Kenya, Tanzania and the rest of the world. Generally, most of the previous researchers have conducted their studies on the cases like cyber security challenges and solutions through review of existing literature without investigation and assessing the challenges faced by financial sectors. There is no study that have been comprehensively been done concerning cyber security challenging threats and its emerging trends in selected banking, therefore this study has been filled the gap by assessing and investigating the cyber security challenging threats and its emerging trends by distributing questionnaire, in depth interview with security expert of the bank and by reviewing the bank security policy.

2.10. Chapter Summary

Cyber security is a broader concept than information security and computer security. Several threat actors are involved in cyber security breaches. Some of these cyber security breach actors are hackers, hacktivism, criminal groups, state and state affiliated proxies, and malicious inside users. As it has been discussed by different researchers, although a lot of frameworks are capable of what the banks needed, they have their drawbacks and they need to be technologized and make it useful for system protection with the current evolving technologies. After investigating and assessing the researcher’s proposed the framework that could be a very significant input for the current challenges faced by the banking sectors.

CHAPTER THREE.

3. RESEARCH DESIGN AND METHODOLOGY

3.1. Overview

The research targets are to assess and examine challenging threats of cyber security and its emerging trends at selected bank of Ethiopia. The previous chapter extensively reviewed the relevant literature. By doing so, it provided a theoretical and empirical background for the study. This chapter aims to provide an overview of the research approaches used within the cyber security discipline that leads to the selection of proper research methodology for directing the justification of the conceptual framework, and thus answering the research question that the researcher used to analyze the current challenging threats of cyber security at development bank of Ethiopia.

The guide to any research is the research methodology is important. Information and data are research life blood. Methodology for studies is the strategy for obtaining a study response by analyzing primary data. This chapter contains research methodology used for achieving the objectives set for this study. In this section, it is discussed about the research design, sample size, data analysis procedure, tools and techniques, validity and reliability of data.

3.2. Research Design

The research design should be seen as a mixed bag approach that implies choosing from different alternatives and options to ensure that the research purpose and perspective are clarified and achieved. The research problem will determine the methods and procedures: the types of measurement, the sampling, the data collection and the data analysis to be employed for the proposed research (Sigmund et al., 2010:66).

For any research process to be complete, an applicable research design to obtain reliable and valid data has to be described. Hence, the relevant research design for the study that would meet the expectations and requirements of the researcher, as well as the research intentions related to the research problem, research questions and related research aims, is called for. The research design should enable the researcher to justify that the research was undertaken only after careful considerations regarding the enquiry. Based on the scope and complexity of the research problem, the researcher decided on a mixed methods research design to conduct this research.

Since cyber security issues are the complex and interdependent topic of threats, attacks and vulnerabilities, mixed research methods will achieve this goal. Qualitative and quantitative research supports the understanding of the problems or develops the ideas. (Venkatesh & Brown, 2007). Typically, the sample size is tiny and participants are chosen to finish a certain quota. The research begins with literature review by evaluating previous researches conducted by different scholars and experts on cyber security in the banking industry, particularly in our country context.

Williams (2007) stated that, research originates with at least on one question about phenomenon of interest. This research targets to answer five questions as stated in chapter one in specific objectives of the research. He further stated that research questions, help researchers to focus thoughts, manage effort and choose the appropriate approach or perspective from which to make sense of each phenomenon of interest.

Therefore, this research uses both quantitative and qualitative research approaches. Due to this, the research simply uses a mixed research approach. (Williams, 2007) describe that with mixed methods approach to research, researchers incorporate methods of collecting or analyzing data from the quantitative and qualitative research approach in a single research study. Williams further stated that goal for a researcher using the mixed methods approaches to research is to draw the strengths and minimize the weaknesses of the quantitative and qualitative approaches. Both research methods are not only compatible but also complementary.

The research approach that was followed for the purposes of this research was the inductive one. According to this approach, researchers begin with specific observation, which are used to harvest generalized theories and conclusions drawn from the research. The reasons for occupying the inductive approach was that it takes into account the context where research effort is active, while it is also most appropriate for small samples that produce qualitative data. However, the main weakness of the inductive approach is that it produces generalized theories and conclusions based only on a small number of observations, thereby the reliability of research results being under question (Yin, 2014).

Data for qualitative analysis generally result from field work. According to Patton (2002), during fieldwork a researcher spends a significant amount of time in the setting that is being investigated or examined. Generally multimethod in focus, three types of findings often result from the qualitative fieldwork experience; interviews, observations, and documents.

The research design was comprised by the result of the literature review. The study will be conducted using survey questionnaire, and interview as a method of data collection and mixed research method as a research paradigm. Like other research methods, a mixed methods approach has its own challenges. One challenge is that a researcher should be knowledgeable in both qualitative and quantitative methodologies and have more time and resources to complete the research (Singh, 2006).

3.3. Data Source

The intention with this thesis was discovering, assessing, and understanding the challenging threats of cyber security and its emerging trends in Ethiopia banking sectors specifically in selected bank of Ethiopia and proposing appropriate cyber security framework. Therefore, the samples have been selected, questionnaires were distributed and interviews were conducted, which are the characteristics of both quantitative and qualitative research methods. However, the fact that questionnaire is used as a tool for data collection dictates more of quantitative research methods though it is used in both qualitative and quantitative methods.

The research used the mixture of techniques of information collection, both main and secondary sources usually referred to as triangulation. In study triangulation, two or more information sources are referred as combinations. Babbie, (2010) stated that the use of the set of triangulation information increases the accuracy and validity of the collected information. This research collected and analyzed primary and secondary data. The use of triangulation offers a counter-checking for the validity and reliability of the gathered information.

3.3.1. Primary Data

Primary data was collected by using questionnaire. Questionnaires was designed on the basis of specific objective to assess and cyber security challenging threats in selected banking.

i. Questionnaire

For the purpose of collecting information from respondents, scholars defined the questionnaire as a research tool consisting of a series of questions and other prompts, although they are often designed for statistical analysis of the responses. It is a question and declaration timetable for self-administering. Questionnaire method is easy compared to other methods, it is bias-free, less costly and does not exert a great deal of pressure on the respondent, making them more comfortable. Researcher distributed closed ended questionnaires to the chosen participants for this research, according to the information gathered from pilot testing. The method assisted the researcher acquire data from various sample units.

ii. Interview

It is the one of the methods to be used to collect primary data from the respondents. A semi-structured interview is a qualitative method of inquiry that combines a pre-determined set of open questions (questions that prompt discussion) with the chance for the interviewer to explore specific themes or responses further. Structured interviews were conducted to obtain the information on cyber security challenging threats in selected banking.

3.3.2. Secondary Data

Secondary data was collected from numerous sources that include both printed and electronic published and unpublished sources such as mass medias, books, journal articles, seminar, conference proceedings research reports, thesis papers, dissertations and the bank annual report as well as the security policy of the bank are used as secondary data for the study.

3.4. Study Population Size and Sampling Techniques

A study population is the aggregation of elements from which the sample is actually selected. For the current research, the researcher chooses specific experts in the field of study as participants based on their specialized expertise and close involvement in cyber security, as the study population for the qualitative phase of the proposed research. The study population of the qualitative phase comprised of IT directorate staffs in different position under the directorate, employee of the bank who are responsible to use sensitive data, those who are logging into the bank server and top management of the bank are used as part of study.

Among the existing banks the researcher used purposive sampling in order to select development bank of Ethiopia, Sampling is mainly based on ease of access to data and willingness of banks and experts' level of ICT usage to provide relevant information that goes with the research problems.

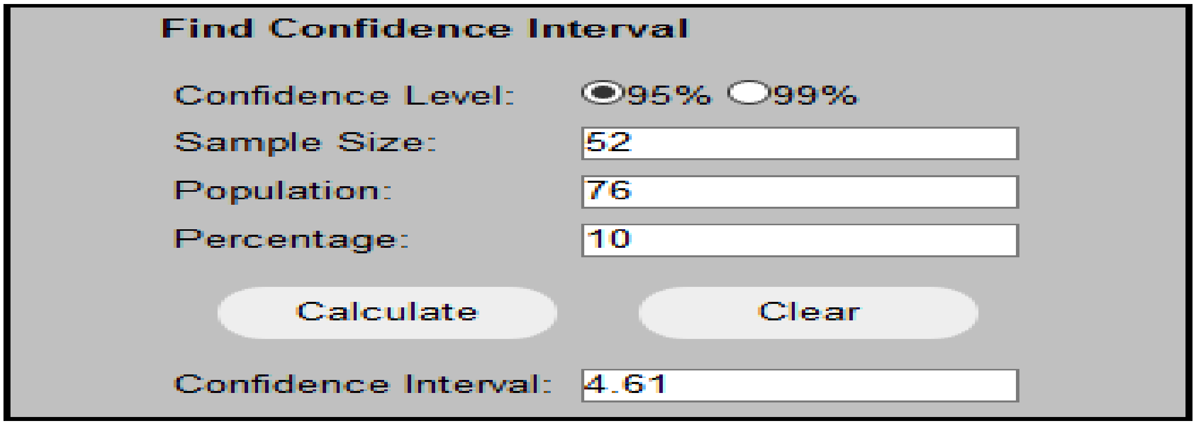
The technique of purposive sampling was used to develop the sample of the research under discussion. According to this method, which belongs to the category of non-probability sampling techniques, sample members are selected on the basis of their knowledge, relationships and expertise regarding a research subject (Freedman et al., 2007).

The selected bank is a specialized state owned development financial institution, which is supervised by the public financial enterprises agency in Ethiopia. The bank has 13 district offices and 110 branches across the nation. Therefore, data sources are obtained from selected bank of Ethiopia (DBE).

3.4.1. Sample size

The actual sample size has been determined from total targeted populations through online calculator (sample size calculator using software - http://www.surveysystem.com/sscalc.htm). With 95% of confidence level, and the sample size is 52. For the simplicity of calculations, the sample size taken by the researcher was 60 bank employees.

Figure 6. Determine sample size



Find Confidence Interval

Confidence Level: ● 95% ○ 99%

Sample Size: 52

Population: 76

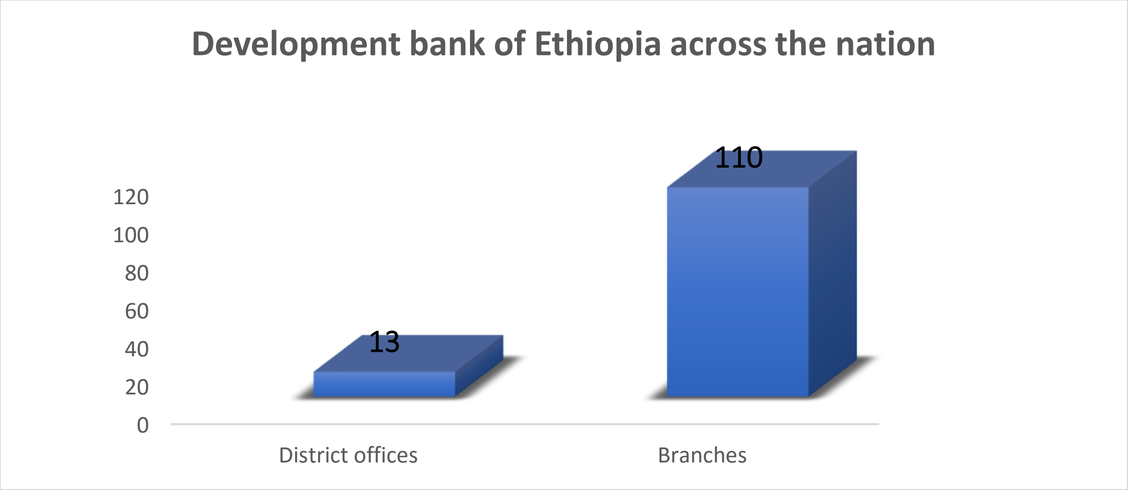
Percentage: 10

Confidence Interval: 4.61

Also sample from each section is selected using purposive sampling a non-probability sampling technique. This involves nothing but purposely selecting individuals from the population based on the researcher's knowledge and judgment.

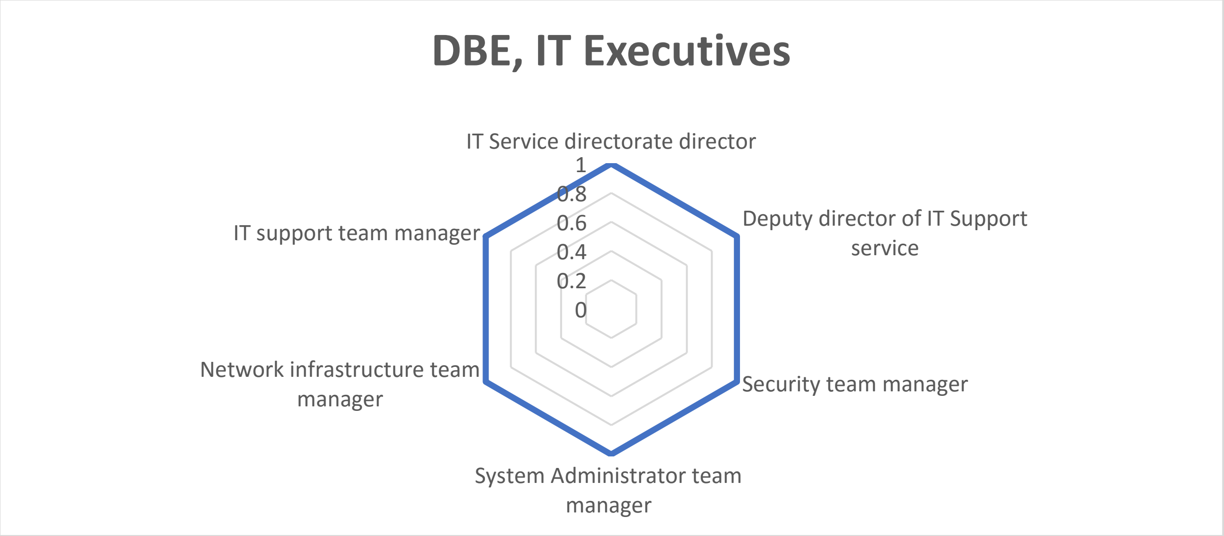
The system will be managed by information technology support directorate but 43.33% of the target population has been taken from district and branches under the district, the rest is from head office. Due to this, the researcher has observed and convinced at least to take 30% (18 employees) of the sampled population size from non-It professional of the bank worker, who are using the T-24 and those who are domain users of the bank server. For the rest of the targeted sampled sizes, the researcher has taken 65% (39 employees) from information technology support directorate and 5% (3 employees) from top management by considering the discussion and interview part.

Figure 7. District and branches of DBE.



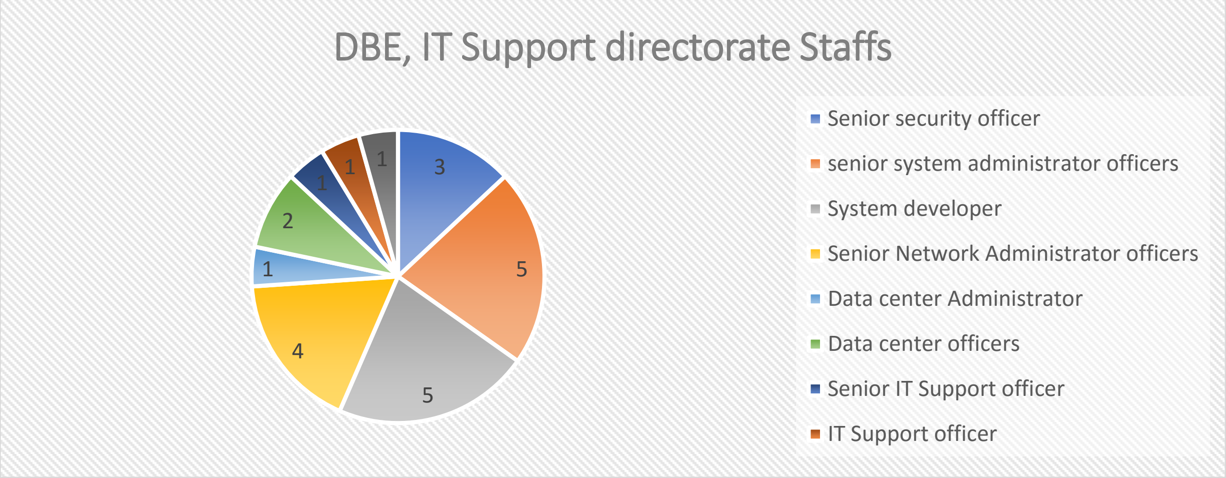
In the current study, the sample members who were selected had special relationship with the situation under investigation, sufficient and relevant work experience in the field of cyber security, IT, active connection in numerous cases of cyber-attacks, and security issues within the bank and they have taken different mitigation techniques regarding to the security issues and they had certificate of security from different networking academy. The participants of this study were 1 director and 2 team managers are interviewed, as shown in the figure below.

Figure 8. List of experts under DBE IT directorate.



Beside this, different officers under IT directorate was participated in questionnaire prepared for IT/ cyber security as professional employee in that departments. Their position was shown as the below figure.

Table 3. Staff numbers under DBE IT directorate.



3.5. Data collection method and instruments.

The quantitative phase was used to assess cyber security challenging threats, policy, procedures in cyber security and emerging used at development bank. This was because there was an obvious lack of situational assessment on banking sectors in Ethiopia. This investigation helped the researcher to identify banking sector challenges which were associated with increasing cyber security treats globally. This quantitative approach explored general cyber security challenging threats for banking and allowing for a statistical balance for this study. The findings produced in this stage laid foundation for the next stage. The qualitative phase addressed unanswered questions from the quantitative phase by interviewing the professionals who are actively participated with situations. This data collection process helped to capture the complexity of the situations surrounding banks.

For the purposes of this research, in depth interviews were used. In depth interviews are personal and structured interviews, whose aim is to identify participant's emotions, feelings, and opinions regarding a particular research subject. The key benefit of personal interviews is that they include personal and direct contact between interviewers and interviewees, as well as remove non-response rates, but interviewers need to have developed the necessary skills to successfully carry an interview (Fisher, 2005, Wilson, 2003). Additionally, structured interviews offer flexibility in terms of the flow of the interview, thereby leaving room for the generation of conclusions that were not initially meant to be derived regarding a research question. However, there is the risk that the interview may deviate from the pre-specified research aims and objectives (Gill & Johnson, 2002).

As far as data collection tools were concerned, the conduction of the research involved the use of structured questionnaire, which was used as an interview guide for the researcher. Some certain questions were prepared, so as for the researcher to guide the interview towards the satisfaction of research objectives, but additional questions were made encountered during the interviews.

For the purpose of data collection, survey questionnaires and interview which are validated by selected expertise were employed together with relevant information that goes with the research study problems. Data were encoded and analyzed by using SPSS and MS-excel, and the findings were discussed and interpreted. Finally, appropriate and updated framework was being proposed, according to the challenges explored in order to minimize the existing cyber security threats.

3.6. Methods of Data Analysis.

This research uses two categories of data analysis techniques; quantitative data analysis and qualitative data analysis techniques. Quantitative data analysis techniques are mainly applied to quantify items from questionnaire data collection instrument. since quantitative research creates meaning through objectivity uncovered in the collected data as explained in research methods wirritten by (Williams, 2007).

Creswell (2003) stated that quantitative research contains the collection of data so that information can be quantified and subjected to statistical treatment in order to support or disprove “alternative knowledge claims”. According to this scholar the findings from quantitative research can be predictive, explanatory and confirming.

The researchers analyze not only numerical data, which is customary for quantitative research, but also narrative data, which is the standard for qualitative research in order to address the research questions defined for a particular research study. As an example, in order to gather a mixture of data, researchers might distribute a survey that contains closed-ended questions to collect the numerical, or quantitative, data and conduct an interview using open-ended questions to collect the narrative, or qualitative data.

After data and information are collected, they are tabulated and presented in the tabular form. After this, different statistical tools are used to analyze those collected data & information to draw the result/conclusion of the research work. The data are collected according to the subject matters. In this research different available literature, journals, reports and data are basis for the study. Then the accumulated literature, reports and data were reviewed and tabulated accordingly with the objectives. The techniques included are statistical tools, tables, bar diagrams, pie Figures, simple average, percentage and others tools as needed to obtain the result. Tools like Microsoft Excel and IBM SPSS Statistics are used for the study.

3.7. Methodological limitations

As it is for every study, this thesis had several challenges that came up during the research work. These are highlighted below.

- ☞ *Sample size*: the sample size is considered not to be too large which could affect the extent to which the findings may be generalized for the whole banks at a country level. and the number of branches included in this study is only two districts among 13 districts.
- ☞ *Time:* the time required to complete the research was very small and this had an influence on the researchers'. The short time did not permit in-depth search for more information's. In some cases, participants may refuse to speak against their banks.

3.8. Research process

Online interview was held with the IT directorate director of the selected bank, security manager and team manager of cyber security, so as to gain acceptance of their participation in the research. More specifically, the researcher came in touch with and asked them to participate in the research after explaining the purpose, nature and the scope of the study. In general terms the respondents were willing to contribute in the research and the interviews were conducted between June and July of 2020. The discussions through online platform because of the world pandemic virus called COVID-19 with the above-mentioned personnel. During the interview and discussion notes were mainly kept, in order to help the researcher to analyze the gathered data and the respondents were free to express their views, they challenging treats they have experienced during the working areas are mentioned. Finally, it should be noted that the conversations flowed smoothly and pleasantly.

3.9. Validity and Reliability of the Data

Because quantitative and qualitative instruments are used in this study, accurate information are highly possible. Besides the additional data collected through questionnaire also help to make data more reliable and valid. Limitations may arise, as it could not represent all the respondent and participants as the limited samples are taken. Since major of the bank IT operations are at head office level. Moreover, the pilot testing on the reliability and validity of the questionnaire and the interview is conducted. For the purpose of collecting reliable data, the researcher designed the questionnaires in a simple, brief and therefore not tedious format, this was done through an elaborate technique involving a series of adjustments under the supervision of the study supervisor to ensure that the fieldwork is carried out using high quality methods of data collections.

3.10. Ethical Consideration

In order to have respondents' genuine responses and to make them free, possible emphasis has been given to the ethical issues. These include the following enough information provided to the participants of the research regarding the objective and nature of study. Participants of the research tell about the confidentiality of their response and there would also be considering of their permission. The review literature acknowledged accordingly. The name of respondents didn't mention in the research. Data collected from the banks was kept confidentially. The following were ensured;

i. The researcher requested approval from the selected bank to obtain the information.

ii. Anonymity was guaranteed to the respondents.

iii. Considerations was applied to information collections, results presentation and interpretation, quotes and references.

3.11. Chapter summary

Quantitative and qualitative research methods investigate and explore the different privileges to knowledge and both methods are intended to address a specific type of research questions. While the quantitative method offers an objective measure of reality, the qualitative method allows the researcher to explore and better understand the complexity of the situations. This paper presented a pure challenging threat founds using quantitative and qualitative research approach.

This research assesses challenging threats of cyber security and its emerging technologies at selected bank in Ethiopia, so that the bank should be protected from any kind of cyber breaches by investigating and observing challenges of cyber security from different perspectives. In order to enhance the reliability and the validity of data collection as much as possible the whole security department / IT staffs, cyber security manager and IT director of the bank is included in the study.

CHAPTER FOUR

4. DATA PRESENTATION, ANALYSIS AND DISCUSSION

4.1. Introduction

This chapter is the outlines of the questionnaire and interviews conducted at the selected bank with the objective of answering the research questions that formed the basis of this research, each research question will be analyzed with the intention of clearly presenting the findings of this research. Data was collected from selected bank of Ethiopia. This study was targeting one selected bank with 60 respondents attaining a 100% response rate of the total response. The interviewees are persons who have worked in various sections within the bank including the, IT directorate director, team managers and cyber security manager and professionals such as cyber security officers, data center officers and network professionals. Finally, the questionnaires were coded individually and input into SPSS and Microsoft excel for analysis. Data was tabulated and presented in the form of frequencies and percentages, in figures, charts and tables.

The chapter is structured on the basis of background information, that is general report of the respondents, the way they responded to each of the variables contained in the questionnaire regarding challenges faced and factors contributing to occurrence of cyber security in Ethiopia banking sector specifically in selected bank for this study.

Data analysis involves putting in order what the researcher has read, seen and heard, in order to make sense of the data, and hence to answer the research questions. It enables a researcher to obtain valuable information from the raw data (Christensen, Johnson & Turner, 2011; Ilya Xi, 2014).

This Chapter is divided into three sections: section one which relates to demographic information of the respondents, section two which focuses on challenging threats faced in selected bank and section three which covers the strategies currently implemented to minimize cyber security risk by banks.

This chapter analyzed and discusses all the research objectives based on the primary data collected from the questionnaires. There was a total of 60 respondents who represented a total of 76 employee from the two selected district and head office of the bank for this research.

4.2. Pilot Testing

A pilot study was conducted with a sample of 15 in order to test the validity and reliability of the questionnaire. Moreover, it helps to ensure whether the instruments are free of ambiguity and irrelevant items. Pilot study is also valuable for controlling bias in data interpretation prior to disseminating the survey to the actual full-scale group. Except one participant, the rest filled the questionnaire, which indicated 93.33% response rate of the pilot study.

Once the questioner was filled, the feedbacks were gathered from the participants. In accordance with the pilot test feedbacks, the questionnaire was amended to improve the clarity of the questions, minimize data interpretation bias and increase the likelihood of success.

4.3. Results and Discussions

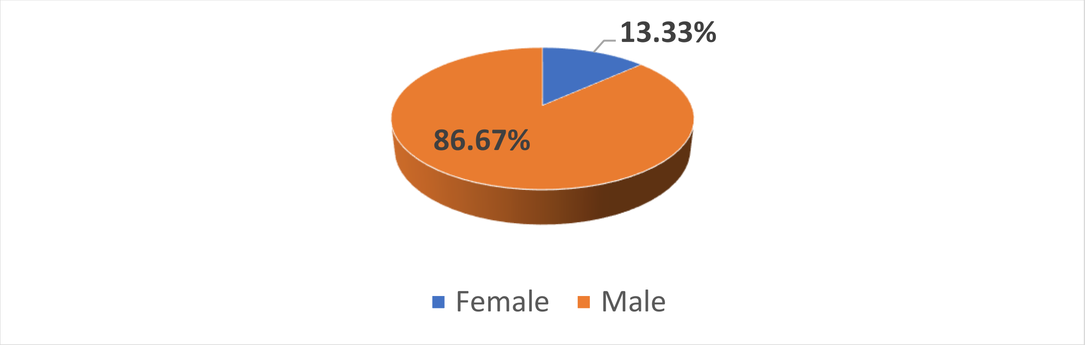
4.3.1. Demography of the respondents.

This portion of the study is concerned with background of the respondents to understand the respondents who participate in filling the questionnaire for this research. Respondents are requested to fill their sex, age and their work experience in the bank.

4.3.1.1. Sex.

Data on sex were collected from 60 respondents, the data was analyzed and the outcomes were as presented as percentages. This shows the gender appropriation in the field of bank administration and there is a huge discrepancy between male and female. 13.33% are females and 86.67% of the respondents are males when summarized.

Figure 9. Sex of the respondents.



4.3.1.2. Age of the respondents

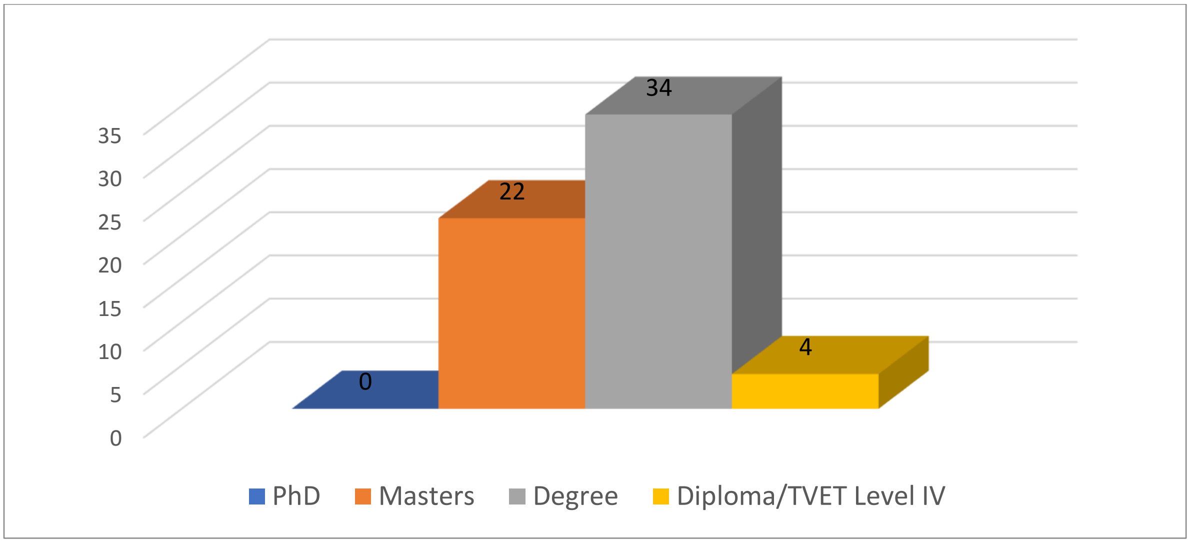
When we see the respondents by age range 29.4% participants are categorized in age range between 20 - 30 years, 47.1% in the age range of 30 – 40 years while 23.5% of the respondents are categorized in age range above 40 years. This shows that most of the respondents are below the age range of 40 years.

4.3.1.3. Education background of respondents

The questionnaire contains four demographic items specifically educational status (Diploma, / Level IV, Degree, MSc and PhD). From the total respondents of the selected bank, 23.33% of the respondents are master's degree holder, 71.67.% are degree holder while 5% of the respondents are Diploma or TVET graduates respectively.

These rates contribute significant share to the validity of the response and the level of security enforced. However, it is not only the educational status but also the security certification and experience within the bank contributes to mitigate cyber security challenges faced at the selected bank.

Figure 10. Educational Status of the respondents.

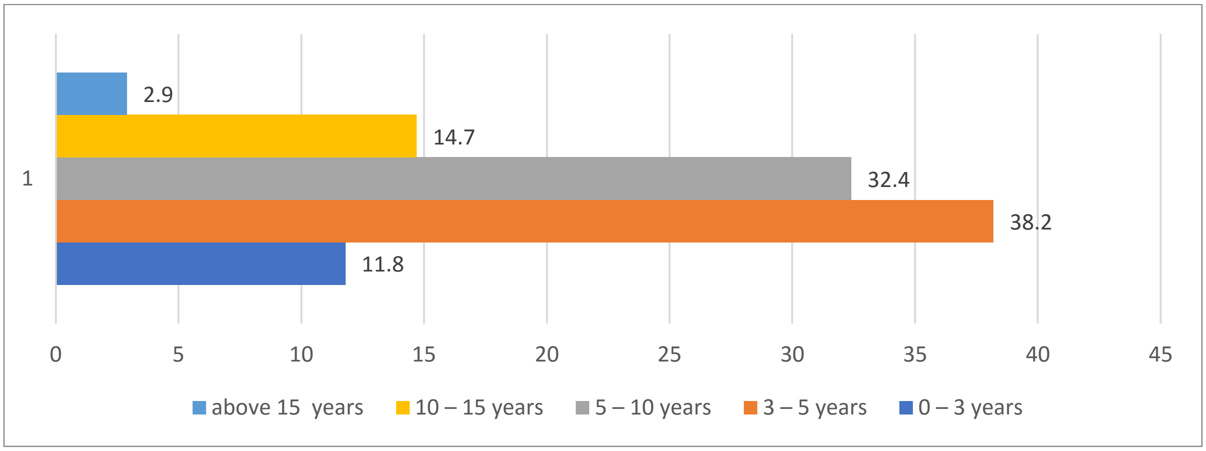


Source: Field Data 2020.

4.3.1.4. Work experience of the respondents.

The job experience of the respondents is included in the questionnaire since it can show how familiar the respondents are with their work operation and how experienced they are with different systems. When we see the respondents work experience in the bank 38.2% of the respondents experience is under 0-3 years, 32. 4% of the respondents are between 5-10 years of work experience and only 14.7% are between 10-15 years of work experience, 11.8% above 3 years while the rest 2.9% of the respondents have work experience greater than 15 years. The study work experience indicated as follows in figure 11 below.

Figure 11. Experience of the respondents.



Source: Field Data 2020.

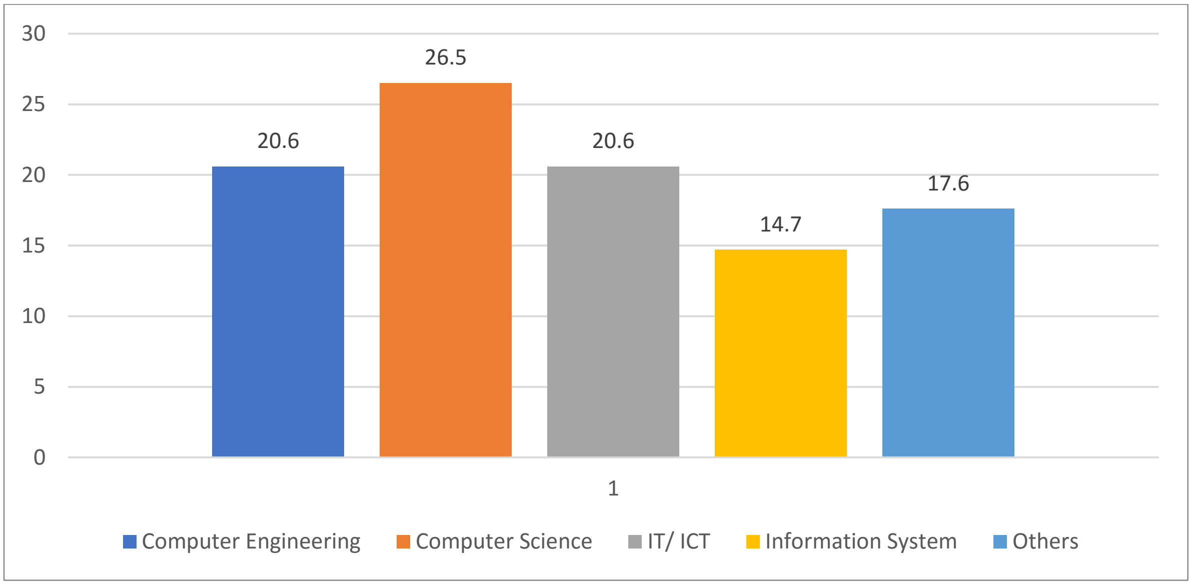
4.3.1.5. Position of the IT respondents

The respondent's position is important for this survey since some of the questioner prepared were technical and administrative questions. The study indicated that 41.2% IT officers, 14.7% cyber security experts and IT Auditors, 11.8% system administrator and others position which are not mentioned in the questioner while 5.9% are IT managerial position including IT directorate director.

4.3.1.6. Profession of IT respondents

The study sought to find out respondents' field of study this makes study more valuable since professionals of the selected bank were from different stream of education. This study indicated that 26.5% computer science field, 20.6% computer engineering and IT/ICT fields, 14.7% information system while 17.6% are other field of study. These rates contribute significant share to the validity of the response and the level of security enforced. As indicated in the figure 12 below.

Figure 12. Profession of the respondents.



Source: Field Data 2020.

4.4. Cyber security challenges at selected bank.

Primary data result of analysis and interpretation is the statements in the questioner were grouped under different parameter on the literature review done in chapter two and the number of participants for each response in the questioner under the dimension were counted to make up the average result for their respective dimension.

In order to obtain the participants with favorable attitude, the strongly agree and agree responses were grouped together. The strongly disagree and disagree responses were grouped together to constitute respondents with unfavorable attitude.

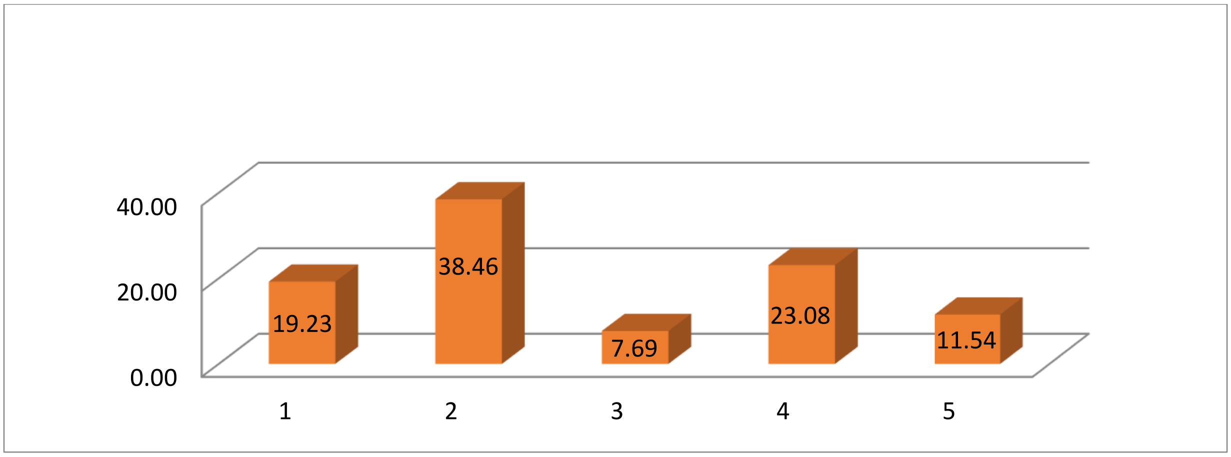
Note 1: Strongly Agree; 2: Disagree; 3: undecided; 4: Agree; 5: Strongly Disagree.

All respondents explained the challenges associated with cyber security faced in their bank. Challenges faced in in selected bank were analyzed as follows

4.4.1. Importance of choosing a strong password.

The bank employee with non IT professionals were asked the importance of choosing strong password, since they were login to the bank system, agree responses were 19.23%, disagree response is 38.46%, while 7.69% of the respondents says strongly agree and 23.08% were said strongly disagree the rest respondents 11.54% says undecided. This is an indication that, they have gap of skill and knowledge regarding with credentials password and the importance of password is not clearly understood by the employees.

Figure 13. Importance of strong password.



Source: Field Data 2020.

4.4.2. Risk of cyber-attacks and implementation of safeguarding techniques

The same employee was asked how the implementation of safeguarding techniques useful for risk of cyber-attacks, the result indicated that 50% responded that implementation of safeguarding techniques is required for the selected bank and 23.08% responded that undecided to the question while 7.6% disagree to the question. This result indicated that, half the respondents were strongly agree to the importance of implementing safeguarding techniques is essential to financial institutions like a bank. This leads into conclusion, that constantly the importance of implementing risk techniques for vulnerabilities have not been in place.

4.4.3. Funds to promote countermeasures against cyber-attacks

Allocating adequate funds to promote countermeasures against cyber-attacks is important for one organization and bank to minimize cyber-attacks especially in banking sector. The benefit is beyond that, since the financial sectors are the first choice to be hacked by cyber attackers. Question prepared for the respondents of bank employee are, how adequate budget their banks allocate to minimize cyber security risk, since 8% respondents were decision makers and in managerial positions. The result of the study indicated that, the selected bank cannot allocate enough budget for cyber security.

4.4.4. Role of senior management in developing cyber security policy.

Senior management and IT professional play vital roles in developing and preparing cyber security policy by consulting concerned bodies and professional in the area of cyber security. The participant of the bank asked whether the bank management play important role in developing cyber security policies in their respective bank and their responses indicated that 53.5% responded that they agreed to the questions and 31.5% strongly agreed that role senior management is important in developing cyber security policy in banking sector, while 15% disagreed to the question.

4.4.5. Software solutions to protect against cyber-attacks

Every organization should have used a risk assessment framework. Risk assessment framework is a system for prioritizing and sharing information about the security risks posed to any organization using information technology as a business process backbone. The information should be presented in a way that both non-technical and technical personnel can understand.

The study sought to find out whether the banks staffs and professionals agree that software's are solutions to protect cyber-attacks. The study result indicated that 46.7% of the respondent agree that software as solution to protect cyber-attacks, 28% of the respondents disagree to the questions, while 19.5% of the study indicated that strongly disagree and the rest 5.8% of the respondent undecided to the questions.

4.4.6. Employees responsibility in preventing against cyber-attacks

The employees in bank have their own responsibility in preventing cyber security attacks, so that selected bank was asked whether their employees are responsible to prevent cyber-attacks, and the study indicated that: 30.7% agree, and 19.2% strongly agree, which mean that, they are responsible to prevent cyber-attacks. Even though it is not included in their job description. While 23.08% disagree and 15.3% strongly disagree, which the respondent are not accountable to prevent cyber-attacks, while the rest 11.54% undecided to the question.

4.4.7. Importance of keeping their passwords secret.

The study sought to find out whether the banks employee know the importance of keeping their password secret. Keeping password secretly and using strong password is very essentials in financial institutions like bank, employees assigned in bank work cannot share their own login password to each other, even though some time they are using the same computers. The results showed that 76.77% responded agree, while 23.08% disagree.

4.4.8. Job description responsibility for cyber security.

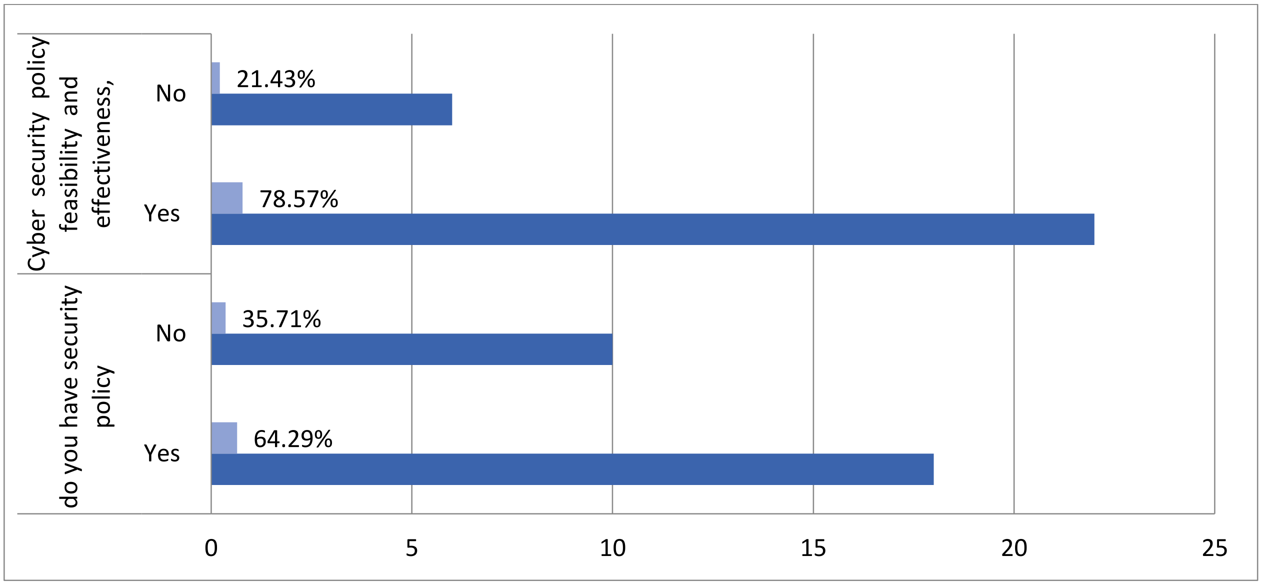
One's employee is employed in the financial institutions like a bank, the bank should have a to be included a responsibility of cyber security in their job description. The study sought to find out whether cyber security responsibility is included with the job description on the selected banks, and the result shows 71% of the respondents opinioned that disagree while 28.92% of the respondents opinioned that undecided to the questions, this showed that their job description doesn't included cyber security responsibility, except the cyber security professional under the IT directorate.

4.4.9. Cyber security policy and standard in banking

The organization's security policy is the set of laws, rules and practices that regulate how an organization manager protects and distributes resources to achieve specified security objectives. (Muniru, 2011). These laws, rules, and practices must identify criteria for individual's authority, and many specify conditions under which individuals are permitted to exercise their authority. To be expressive, these laws, rules, and practices must provide individuals measurable ability to determine whether their actions violate or comply with the policy (Hessetbech, 2011).

The selected banks were asked whether they have cyber security policies document & procedures, its implementation status, standards, and feasibility and effectiveness of the policy for cyber security. The study sought to find out how important cyber security policy standard and its feasibility and effectiveness were useful to protect cyber-attacks and the sampled bank opinioned that 21.43% of the respondents says cyber security policy standard were not important while 78.57% of the respondents opinioned that important to the bank.

Figure 14. Cyber security policy.



Source: Field Data 2020.

As shown in the figure 14 above, the findings from the survey shows that 21.43% of the surveyed banks don't have documented cyber security policy document while the rest 64.29% possesses the document which they cascaded and adopted from the national and international cyber security policy by consulting INSA. Cyber security policy feasibility and effectiveness of the survey shows that 21.43% effective and 78.57% feasible according to the respondents of the study.

4.5. Cyber security threat detecting preparedness of the bank.

Due to the importance of detecting cyber security threats for financial institution like banks, collecting data about the challenges and identifying the cyber security threats to take appropriate measures are very important for banks. Accordingly, this survey research targets to identify cyber security challenges faced at selected bank on five cyber security threats namely,

- Insider attacks
- Social media attackers
- E-mail attackers
- Cyber-criminals
- External attacks

The respondents are asked to rate the above challenges of cyber security in a lickert scale from 1 to 5 as 1: Inadequately Prepared, 2: Somewhat inadequately Prepared, 3: Somewhat secured, 4: Secured and 5: Highly Secured.

4.5.1. Insider attacks

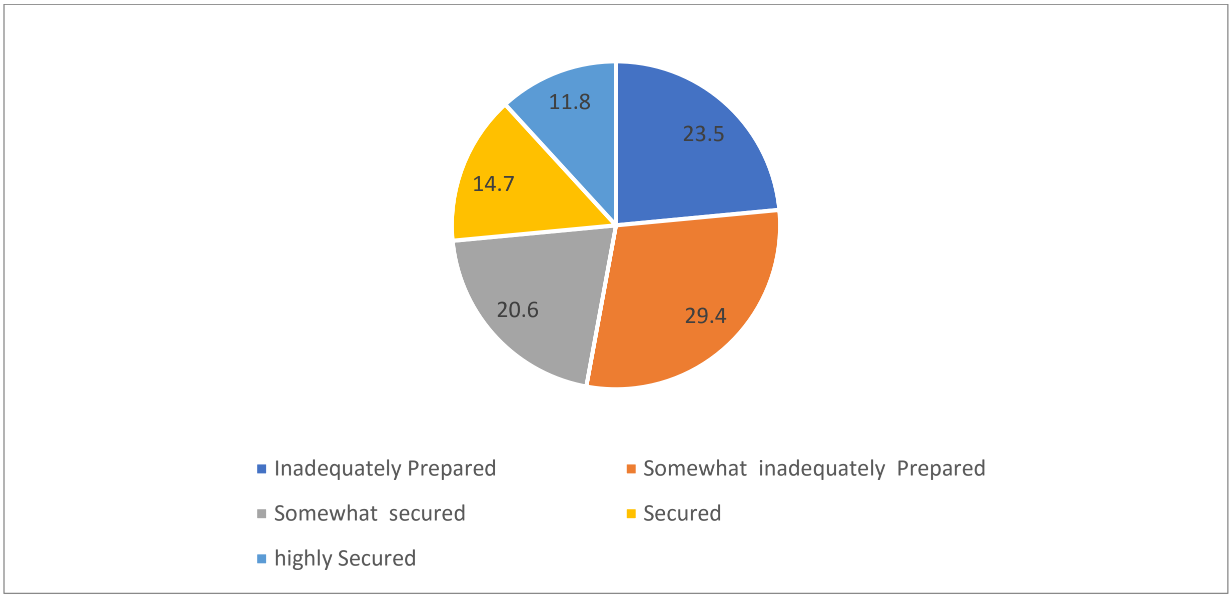
Likert	Number of Employees	Percentage
Somewhat inadequately Prepared	1	2.9
Somewhat secured	9	26.5
Secured	12	35.3
highly Secured	12	35.3
Total	34	100.0

Table 4. Insider attacks result

To determine extent of the insider attacks that banks in Ethiopia are faced, data collected from selected bank were analyzed using frequency distribution and percentage. As indicated in table above. This section sought to capture different answers on cyber security threats preparedness by the selected bank of Ethiopia. Prevention of any cyber security breach is the ultimate goal of any financial institutions. According to NIST (2017) prevent refers to developing and implementing the appropriate safeguards to ensure delivery of financial institutions. However complete prevention of cyber security threats is nearly impossible in these days. But banks capability to prevent cyber security threats should be increased which saves money and bank reputation. Therefore, the bank should have higher capability to prevent cyber security threats. The questioner was answered by five lickert and five cyber security threats questions.

However, the survey of the insider attacks indicated that 70.6% highly secured and which the bank is not exposed of the insider's attacks, 26.5% responded that somewhat secured. The second cyber security preparedness questions indicated that 29.4% somewhat inadequately prepared from social media attackers, while 20.6% of the respondents says somewhat secured, this indicated that the selected bank was not that much prepared to be secured from social media attackers. Figure 15 below shows the result of the study.

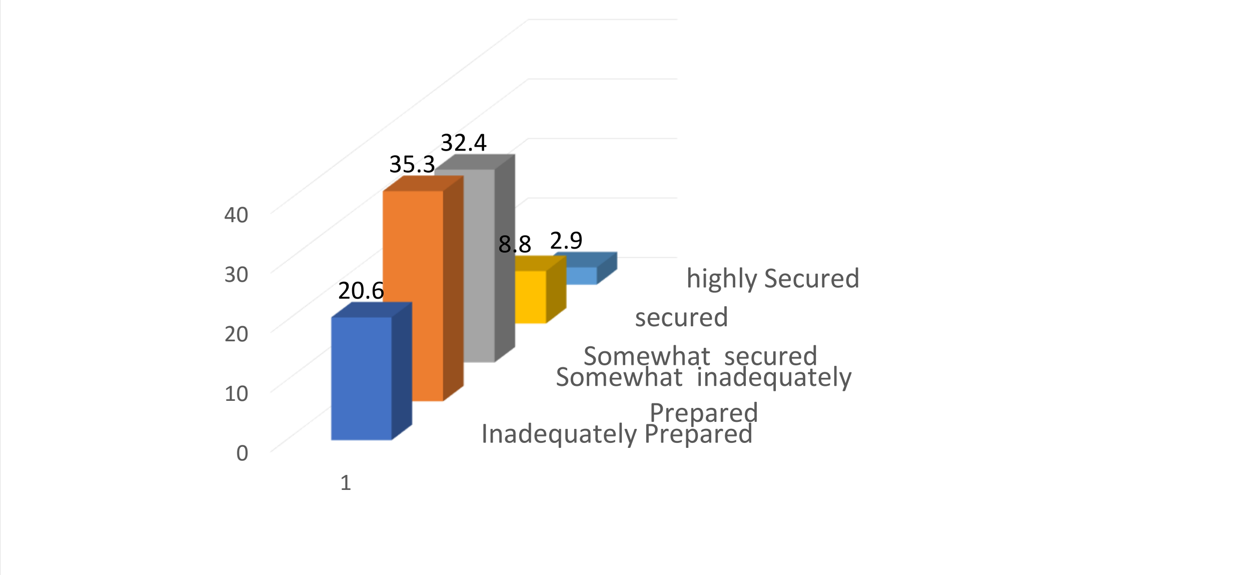
Figure 15. Social media attacks.



The third cyber security preparedness questions indicated that, 41% of the respondent said that their respective bank is secured, to prevent attacks from via emails, while 20.6% of the respondents said somewhat secured. The survey sought that the selected bank was secured to be hacked by email attackers.

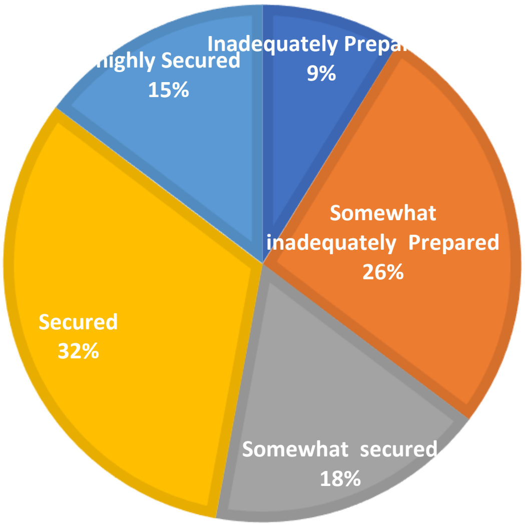
The fourth and the main cyber security challenges faced in banking industry is that cybercriminal as stated in the chapter two of the study literature review. The study indicated that the selected bank is not secured form cyber criminals, the evidence shows 35.3% respondents responded that their bank was somewhat inadequately prepared and 32.4% responded that their bank is secured. This indicated that the selected bank work on this type challenges in order to prevent the bank from cyber criminals. The study result is summarized as below figure 16.

Figure 16. Cyber-criminals.



The last and the reverse question of insider attacks, indicated that their bank are 32% secured form external attackers, even though 26.5% of the respondents said that somewhat inadequately prepared, this shows that there is an internal attack from the internal staff even if they are willing to mention through interview too.

Figure 17. External attacks.



4.6. Cyber Security Policy and Standards of the bank

The objective of this study were to assess and investigate cyber security challenging threats and its emerging trends in banking sectors specifically at selected bank for this study as mentioned in chapter one of this study. Respondents gave their views and opinions on the cyber security threats faced in selected bank.

The "Yes", "No", "I don't know" options were used to identify the practiced taken by the selected bank of information technology directorate and encoding the questionnaire for analysis. The three options are used to indicate the selected bank cyber security policy practices , whether fully practiced, rarely, completely not practiced. The following table clarifies the options.

Options Clarification	
Options	**Meaning**
Yes	The bank is performed or practiced it fully
No	The bank is completely not practiced it
I don't know	Does not have the information in the bank

Majority of the respondents demanded that cyber security policy has been put in place to address cyber threats. cyber security policy is a formal set of rules by which those people who are given access to company technology and information assets must abide. The cyber security policy describes the technology and information assets that organization must protect and identifies many of the threats to those assets (Geer Dan, 2016).

4.6.1. Technological barrier to information/cyber security policy.

Security policy is important to bank as organization to protect cyber-attacks. The study indicated that the cyber security policy considered as a barrier to technological opportunities responded by the yes, no and I don't know response from the respondents of the bank showed that; 35.2% Yes response, 62.7% No response while 2.9% of the respondents responded that I don't know response, this indicated that cyber security policy is not barrier to emerging technology of the bank.

4.6.2. Cyber security policy document.

Security Policy is a set of guidelines established to safeguard the network from attacks, both from inside and outside a bank. A cyber security policy must be developed which reflects bank's objectives, management support and commitment, and core values gives to technological advancements. The organization’s security policy is the set of laws, rules and practices that regulate how an organization manager protects and distributes resources to achieve specified security objectives (Muniru, 2011).

The study sought to find out how often the banks had a cyber security policy as a way of regulating cybercrime and the selected banks were asked whether they have cyber security policies document, its implementation status in their bank. The selected bank has a cyber security team which is located under IT directorate director; it is not yet in department level; it is just a team located under directorate lead by cyber security team manager. The cyber security team has 3 senior officers under the team, and each members of the team are not assigned to a specific role, they are all working in cyber security domain. The study indicated that 75.5% of the respondents responded that they have no documented cyber security policy since they are very few in numbers and not at department level while the rest 23.5% of the respondents said they have no ideas of cyber security policy. To confirm this, the interview were conducted with IT directorate and cyber security team leader and they said that:

> *“We are working on cyber security policy and others policy considered to the department as directorate with national bank of Ethiopia, since we are monitored under national bank as well as we are consulting INSA to have a best cyber security policy document by referring the international policy of cyber security”.*

4.7. System Development and Maintenance

4.7.1. Processes to implement new technologies in the bank.

New technology is important for banking sector, since our world technology is emerging, the financial institutions should have to update themselves to attract the customer and minimize the time with effective and efficient way.

The result of the processes to implement new technologies in selected bank indicated 41.8% there is no processes of implementing new technology, while 23.5% responded there is a process taken. 35.2% of the respondents they don’t know whether the bank implement new technologies.

4.7.2. Culture of conducting cyber security study

For one organization conducting cyber security study and assessment is important before implementing and developing new technologies, the study sought that the selected bank was asked whether they have a culture of conducting cyber security requirement study before systems development and test its security related issue in the selected bank. The result of the study is indicated that 26.4% of the respondents said that their bank conducts a cyber security study while 44.1% of the respondents responded that the bank cannot conduct cyber security study, this showed that the selected bank cannot conduct a cyber security study as institution. The interview confirmed the same result of the questioner.

"As a bank we have no yet conduct a cyber security study but we have participated in government and non-government as well as international study of cyber security. As the institution the national bank study cyber security with the collaboration of INSA as regulatory body"

4.7.3. Protective measures to reduce risk

Like other study, the study sought that the selected bank was asked whether they have implemented protective measures to reduce risk when implementing new technologies in the bank And the study indicated that, 55.8% of the respondents responded that No response, which means that the selected bank needed to implement protective measures to reduce the risk of cyber security while 38.2% of the respondents responded that Yes response and the rest of the respondents have no ideas of the question which is 5.8% say I don't know.

4.8. Top cyber security challenges of the bank

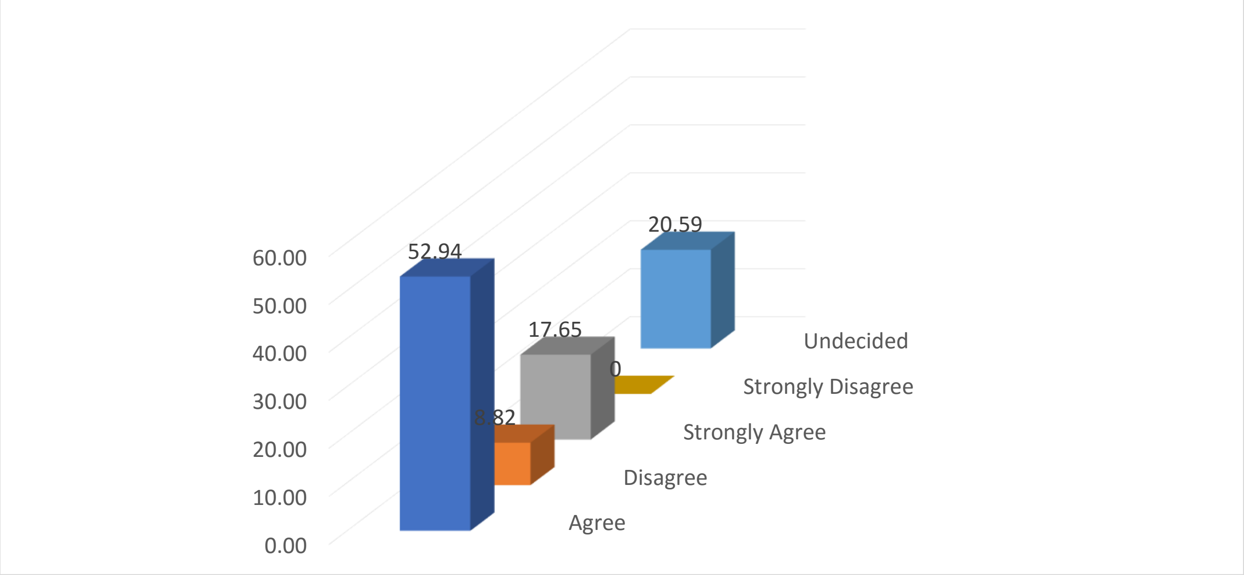
All respondents explained the challenges associated with cyber security faced in their bank. The data is collected from the respondents on the above security threats using Lickert scale that is; 1: Strongly Disagree, 2: Disagree, 3: Undecided 4: Agree and 5: Strongly Agree. and the challenges were analyzed as follows;

4.8.1. Lack of professional expertise

The lacks of professional expertise to ensure cyber security at financial institutions is most important issue in banks, to confirms this as, the study of Kritzinger and Solms conformed that and they said "the availability of specialist training in telecommunications is currently extremely limited on the continent of Africa" as cited in (Kritzinger and Solms,2012).

The survey indicated that the selected bank has a lack of professional expertise with 52.9% response from the questioner, without internal or external expertise, is ridiculous to minimize cyber security risk. This survey shows that lack of professional expertise is the top-rated challenge at the selected Ethiopian bank, this figure below indicated the response of the respondents.

Figure 18. Lack of professional expertise.



Moreover, the interview with IT directorate and security team manager confirmed this as:

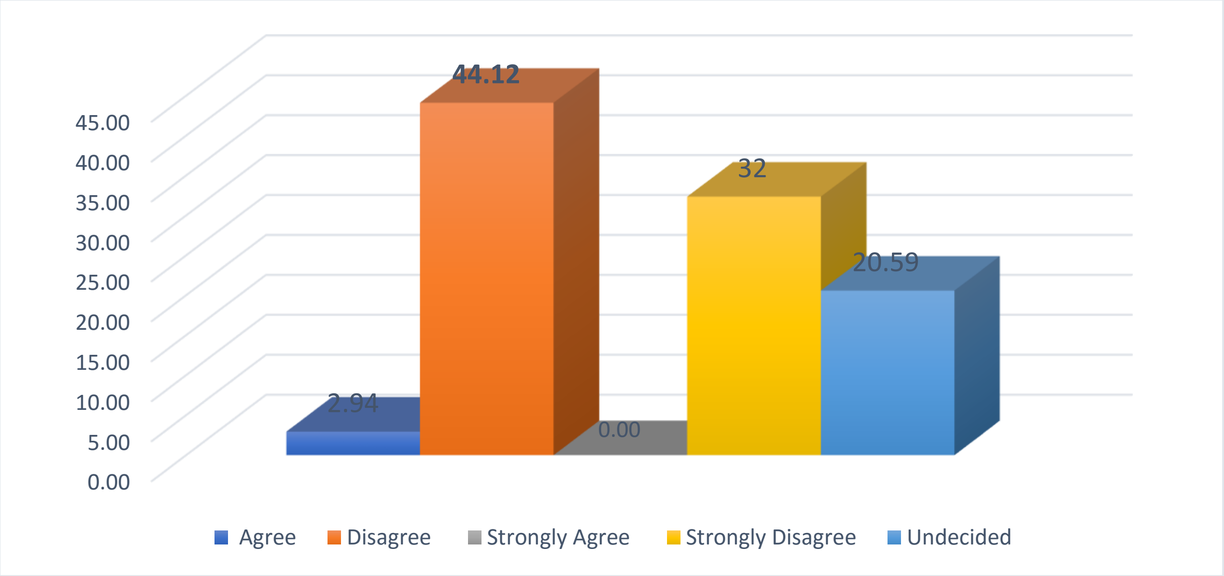
> "*We comprise numerous challenges to secure cyber space. From these challenges lack of qualified experts and acquiring proper technology are the most remarkable. furthermore, absence of qualified experts are the major challenges of cyber security we had as bank, since cyber security field is not available here in our public and private higher institutions, we employed competent staff in other department like computer science and information technology the we provide short term training to our staff accordingly.*"

4.8.2. Loss of sensitive or confidential data.

The second rated security challenges indicated by the respondents are loss of sensitive or confidential data to have a secure cyber space it is highly required to equip with technical aspects of cyber safety like up-to-date anti-virus packages and regularly patched operating systems. It is not only the case of Ethiopia, However, the African continent faced this challenge as well. In describing this Kritzinger and Solms (2012) in their study entitled "*A Framework for Cyber Security in Africa*".

The study sought to find out if the selected bank loss sensitive data and information by cyber-security attackers. And 44.1% of the respondents stated that they had not lost confidential data; 32 % stated that they loss confidential data, while 20.5% stated that they undecided. This an indication that the selected bank loss confidential information into some extent.

Figure 19. Loss of sensitive or confidential data.



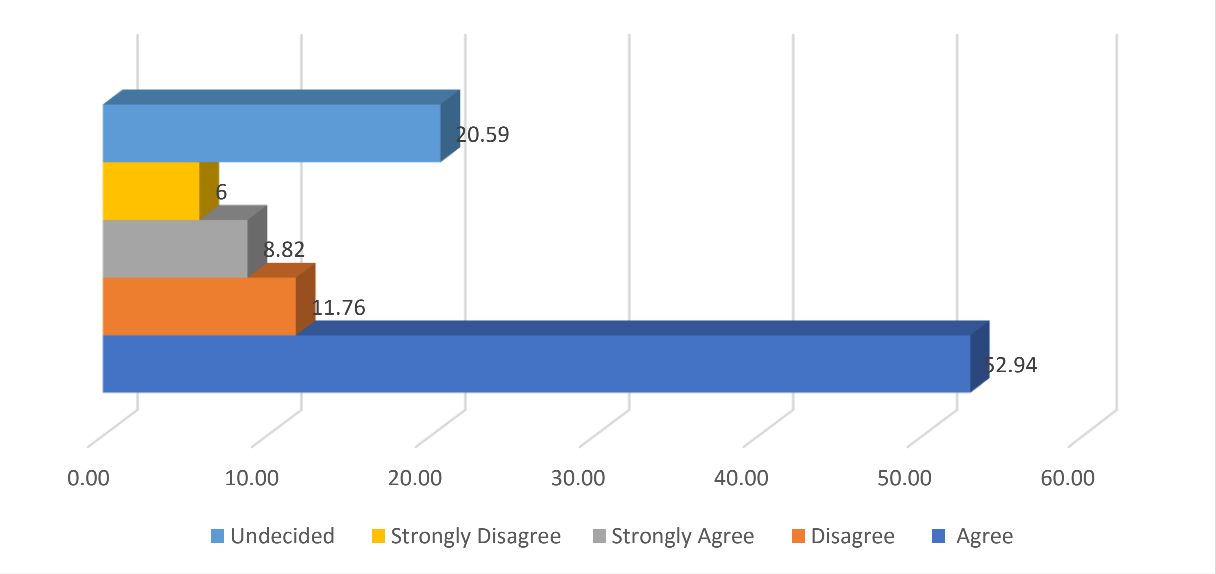
The interview with IT directorate and security team manager were different from the questioner participants:

> *"As a financial institutions we face different challenges like others but we need to protect our data and customer information from cyber-criminal, till now we did not loose any data by cyber criminals for this matter we have using different techniques in our data center for this matter never mention what kinds of application and mitigation techniques we are using for the sake confidentiality".*

4.8.3. Poor leadership

The study sought to find out if the decision makers and the bank leaders at banking sectors are led their respective employee properly regarding to cyber security to have save cyber space, 52.9% of the respondents indicated that they have poor leadership while 6% of the respondents indicated that they have good leadership. Figure 20 below tabulates the respondent's views.

Figure 20. Poor Leadership.



The interview conducted indicated that;

> *"The leadership style to minimize a cyber risk is going smoothly since we have cyber security department under the directorate and the professionals under the team are disciplined, sometimes they raise a training and we have given a training twice a year and the security team manager was trained in south Africa for three months sponsored by the bank".*

4.8.4. Inadequate enabling technology

Cyber users in Africa do not have up-to-date technical security measures like anti-virus packages, and many of the operating systems used are not regularly patched, since they are not using licensed operation system and utility software as well. The study also sought to assess from the selected banks whether the adequate enabling technology guidelines were sufficient to protect cyber security attacks and provide a good banking service.

The study indicated that 29.4% agree and 26.4% strongly agree response which indicated that there is inadequacy of enabling technology in selected bank, while 32.3% undecided response from the respondents. The interview conducted with the directorate and team manager indicated that challenges of appropriate enabling cyber security technology as:

> *"We are using a licensed antivirus package. nevertheless, this is not a case all the time. We have also a problem in using properly patched operating system like western country*

> *abroad. This makes our system exposed of cyber security attacks not only this the other application we are using for sake of protective is trial version".*

4.8.5. Insufficient funding

The study sought to find out whether the bank allocate sufficient budget for the response of the cyber security attacks, since financial institutions at the top to be hacked by cyber criminals, the survey indicated that 35.2% of the respondent agreed that the selected bank has not allocate enough budget for the sake of cyber security, while 17.6% of the respondent agreed that the bank allocate enough budget for this work, 20.5% of the respondent opinion is that undecided which, they have no idea about the budget while 23.5% of the respondent said that strongly agree to the case. However, the interview conducted stated that:

> *"The annual budget allocated specifically for our directorate is insufficient for obtaining the knowledges and technologies we need for cyber security compared to the work load, technology needed and for capacity building for our employee. This one of our challenges we faced as bank".*

4.9. Security attack the bank has experienced over the last 5 years.

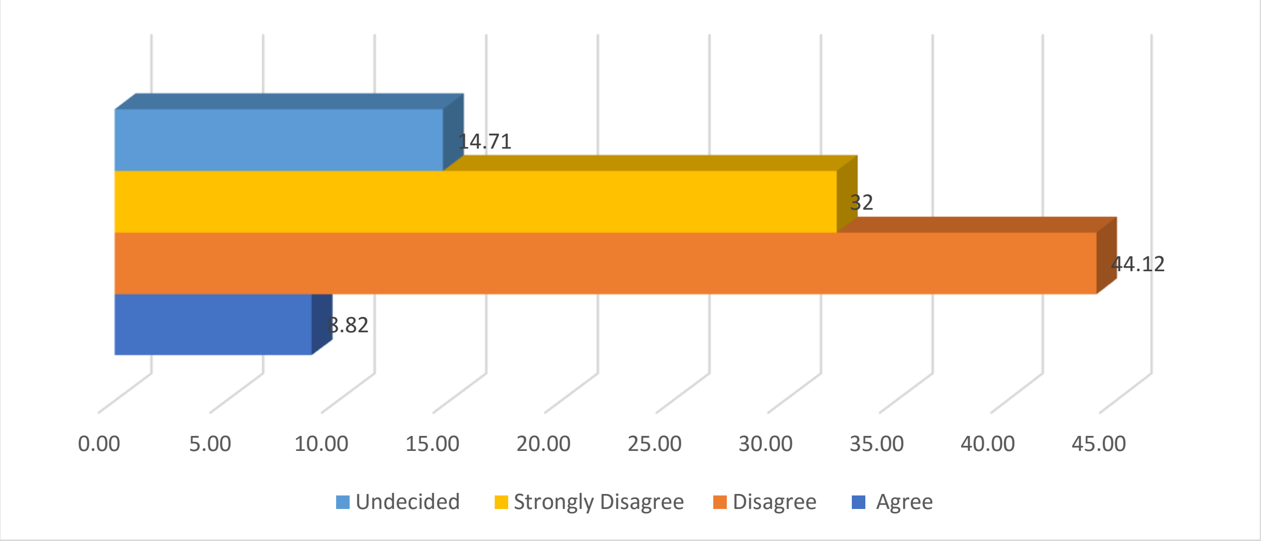
The study sought to find out whether the recent past cyber-attacks had been on the increase, the survey has been collected by five different variables as listed below:

4.9.1. Web-based and Web application attacks

Researcher discovered that fake offers on the internet to share security credentials as cyber threat highly contribute into cybercrimes. This act is called phishing. Phishing is a method that hackers use to steal personal information, like credit card details or login credentials. The hacker duplicates an existing login page from an online service. This fake website contains code that sends all personal data you submit directly to the hacker (https://medium.com/phishing). To get you to this fake website, hackers send a convincing email to you. In this email, you will be asked to log in to the given system. The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate web servers they've compromised. But data-stealing attacks, many of which get the attention of media, are also a big threat. Now, we need a greater emphasis on protecting web servers and web applications. Web servers are especially the best platform for these cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions in order not to fall as a prey for these crimes. 63% claimed that cyber security threats faced by financial institutions is an attack that resulted in online banking and transferring money through different platforms.

The web based and web application attacks of the bank indicated that 32% of the respondents opinioned that they strongly disagreed that they are not experienced such kind of attacks over the past five, 23.5% of the respondents opinioned that they agreed that in the recent past cyber-attacks had been occurred in the selected bank and 44.1% of the respondents opinioned that they disagreed that in the past cyber-attacks had been on the increase. Figure 21 below shows in a tabular format of the opinion's respondents.

Figure 21. Web-based and Web application attacks.



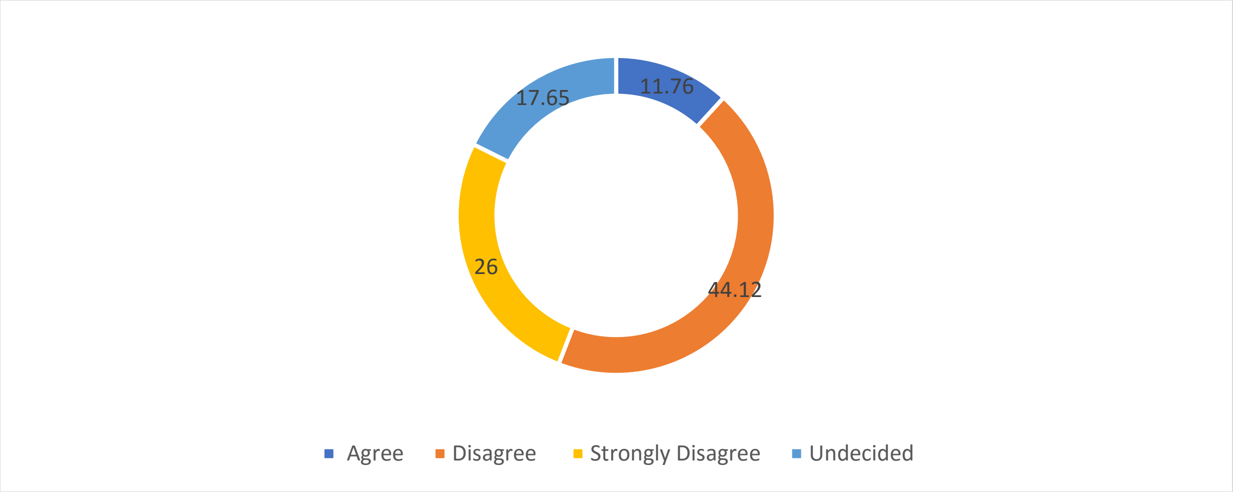
4.9.2. Malware attack

The other variable of the study is malware attack, this attack in selected bank indicated that 55.8% of the respondent strongly disagreed and 21% disagreed that they are not experienced malware attacks since the selected bank is using licensed antivirus as indicated in the above, while 8.8% of the respondent view is strongly agreed and 5.8% of the respondents are undecided to the question, which they are not seen such kind of attacks during their work experience in selected bank.

4.9.3. Information Disclosure and Denial of service attack

Information is vital for one organization especially for the financial intuitions like bank information crucial since they are recoding the customer information for sake business. The study sought to find out whether the selected bank experienced information disclosure and denial of service whenever they provide service to their customer and the survey questionnaire indicated that 44.1% strongly disagree to the question that their bank information is secured and the service delivered by the bank is not denied by cyber-attacks, while 17.6% of the respondent agreed to the questions. The below Figure 22 indicated the views of respondent.

Figure 22. Information Disclosure and Denial of service attack



4.9.4. Network security, data and information of the bank.

The research sought to find out whether banks network security and information/ data of the bank attacked by cyber criminals and the study indicated that 50% of the respondent disagreed and 26% of the respondent strongly disagree to the question, which mean that they are not yet attacked by cyber criminals, while the rest 23.5% of the respondent undecided to the question, this indicated that have no ideas of the question or they don't want say attacked since they lost their potential customers for this matter.

4.9.5. A Virus attack of the bank

The study sought to find out whether the selected bank was attacked by a virus, which a type of cyber-attacks. The study indicated that 35.2% of the respondent strongly agreed and 38.2% of the respondent agreed that they are attacked by virus. While 17.6% of the respondent disagree that virus attack is not a type of cyber criminals and the rest 2.9% undecided to the question, so that according to the survey a virus attacks of the bank is not the type of cyber-attacks.

4.10. Summary and Discussion of the findings

The first research question of this study is to identify the challenges of ensuring safe cyber space at selected bank, the survey research which is a case study of one purposive selected noncommercial bank in Ethiopia to identify the major challenging treats of cyber security and its emerging trends. The Ethiopian government in recognizing the inadequacy of the former penal law issued a proclamation on Telecom Fraud Offence with Proclamation No. 716/2012. Furthermore, there are two policy issues which are related with ensuring safe cyber space. These are national spatial information technology policy and the national information and communication technology policy and strategy.

This study indicated that selected bank faced challenges of lack of expertise, inadequate enabling technology and insufficient budget and resource. Cyber security requires professional trained expertise. The report of (GOA, 2007) entitled in "Cybersecurity for Critical Infrastructure Protection" states that technologies do not work in isolation. Cyber security solutions make use of people, process, and technology. Cyber security technology must work within an overall security process and trained personnel, even though the study were done for critical infrastructures the same is true for financial institution like bank. In Ethiopia as we have mentioned in statements of problem in chapter two, one problem of cyber security is: well-trained man power since the field of study not available in our higher institutions. Therefore, financial institutions in Ethiopia should develop a strategy to recruit, develop and retain professional expertise in the area of cyber security. The other main component for cyber security is the emerging technology since we are very far away from the recent technologies.

Additionally, this study identified that there was a poor leadership of cyber security at the selected bank. Cyber security requires excellent leadership style and adequate amount of budget, while the selected bank would not allocate enough budget according to the survey questioner and interview. Even though, the profession of cyber security at selected bank, spending more time on work cyber security as observed before the distribution of questioner.

Moreover, the results showed that the selected bank for this study has the absence training provided and certification cyber security department is not enough, in addition lack of support from the top managing bodies of the banks, poor awareness on cyber security issues with the staff of the bank, lack of guiding and controlling means so as to enhance security related problems, work overlap in

IT department, absence of a predefined security requirement identification methodology or model, less attention and less controlling mechanism for managing traffic that come from untrusted sources and medium level of access control using passwords and less skill in managing personal password from the staff of the banks, loose of confidential data are the finding to be mentioned by this study.

The other and the main finding of this study is that cyber security threats detecting preparedness of the bank should be improved, since the banking and financial industries are the first choice of cyber attackers, the management of the bank not lead in the proper and good way this indicated that there is a poor leadership style in managing cyber security, internal attacks from the staffs, inadequacy of enabling technology in selected bank are some to be mentioned among the main finding of the study.

Although banking institutions have taken important steps to rise cyber security efforts in recent years, banks and other financial services companies will continue to be challenged by the rapidity of technological dynamic change and the increasing sophisticated nature of threats. While institutions are aware that the threat landscape is constantly evolving, they may find it difficult to keep up with the latest developments and competitive pressure to integrate new technologies into the bank system. Although institutions seem more willing than in the past to share information regarding threats and attacks, many remain hesitant to reveal perceived or actual security weaknesses to competitor.

The second research question of this thesis is to identify the implementation of cyber security activities such as devising policy, standards, and procedures that govern cyber security activities at selected bank of Ethiopia. The study of the selected bank indicated that the top cyber security challenges of the bank is that they haven’t documented cyber security policy in place that includes what are considered to be the key pillars of security: Written information security policy, security awareness education and employee training, risk management of cyber-risk, inclusive of identification of key risks and trends, information security audits and incident monitoring and reporting. this study indicated that there was the absence of a printed and recognized cyber security policy, guideline, procedure, and standards in the bank, no legal and documented cyber security policy, employee’s awareness to cyber security is very low.

As per data gathered from the bank employee through questioner and interview, there has no written and formal cyber security policy, guideline, procedure, and standards so far, the implementation of safeguarding techniques for cyber security is very low, the role of senior managers to cyber security is low, employees responsibility in preventing against cyber-attacks and the strategic plan in protecting cyber-attacks needs to be improved since cyber security is not only the responsibility of cyber security professionals.

As a result, all statements in the questioner aimed at assessing the cyber security challenges faced and its emerging trends in selected bank for this study, the policy, guideline, procedure, and standards ignored. The absence of such a written and formal document in the bank shows that the selected bank taken seriously the issues of cyber security. ISO 17799 defines a policy as the "overall intention and direction as formally expressed by management". In other words, it is a document detailing what management expects of employees in terms of protecting information assets.

Furthermore, policy is the underpinning of the other cyber security mechanisms. Policy has a number of functions including setting standards and ensuring a minimum level of uniformity in implementation of cyber security reducing mechanisms; providing a framework for action and for dealing with potentially sensitive security issues; and promoting the transparency and accountability among departments and employees. Without cyber security policy, the appropriate direction for the other information security components such as the level of risk posed and the resultant level of protection required cannot be effectively provided. It is based on these risk definition and level of protection required that the organization can determine the organizational structure and resource to be committed for cyber security (Von Solms, 2000).

Without security policy, the appropriate direction for the supplementary cyber security mechanisms such as the level of risk posed and the resultant level of defense required cannot be effectively provided. It is based on these risk definition and level of protection required that the organization can determine the organizational structure and resource to be committed for cyber security. Without a cyber security policy, security practices its is difficult to protect cyber-attacks.

Effective security policies would help to define the users right and responsibility in relation to information within the organization and help users to understand acceptable and responsible behavior in information resources. The existence of well printed and documented cyber security policy also helps senior managers to control and monitor employee behavior in relation to information resources. (Von Solms, 2000).

For instance, cyber security policy stating that access should be controlled. A procedure provides the detailed steps of a component mentioned in a policy, for instance the process of granting access of T-24, other loan registering application and distributing passwords. A standard detail the minimum requirements, for instance that a password must be at least 8 characters long and consist of alpha-numeric characters. A guideline is a document that assists management in the implementation of cyber security at financial sectors since they are more targeted to be hacked by cyber criminals. Therefore, without cyber security policies and guidelines to direct, control and monitor, employees could not well interact with information assets in ways to minimize risk. In time, such potentially harmful conduct could inappropriately give rise a culture neglect the policy of cyber security at selected bank.

The selected bank need to evaluate their information security compliance level and they should have a mechanism to ensure that the practice of employees is compliant with the information security policy particularly because a significant number of information security breaches result from employee's failure to comply with security policies. As a result, policy enforcement is necessary and essential for the protection of information assets in an organization (Vroom & Von Solms, 2004).

Specifically 34.5% of respondents strongly agree and 59.3% of respondents agree that employees should be monitored on their compliance to information security policies and procedures such as measuring the use of email, monitoring which sites visited and what software is installed on computers and 32.4% of respondents strongly agree and 60% of respondents agree that action should be taken against anyone who violated restrictions on sites to be visited, usage of email, and software to be installed on computers.

Monitoring of employee behavior could include monitoring the installation of unauthorized software, the use of strong passwords or Internet sites visited. Technology monitoring could relate to capacity and network traffic monitoring. Information security auditing is necessary to ensure that the policies, processes, procedures and controls are in line with the objectives, goals and vision of the organization (Vroom & Von Solms, 2004). As such the high positive attitude of employees towards security program management activities will lay fertile ground for the bank in its overall effectiveness of information security protection endeavors.

Moreover statements employed to measure ethical attitude of employees reveal that 40% of respondents strongly agree and 55.17% of respondents agree that it is important to regard the work they do as part of the intellectual property of the bank; and 31% of respondents strongly agree and 50% of respondents agree that e-mail and internet access are for bank purposes and not for personal use they said. The result shows that respondents are more inclined to ethical values and rules which is very conducive for favorable information security culture to thrive.

The third and final research questions of the study is tools required to minimize cyber security attack at the bank. The literature review, questionnaire and interview findings and the researcher's findings and experience shows that there is no local cyber security auditing framework that aid in development and implementation of cyber security framework to secure data in banking industry in Ethiopia, beside the research done by St. Mary university entitled "cyber security Auditing framework for Ethiopian banking industry " by Tesfaye Asfaw in 2018.

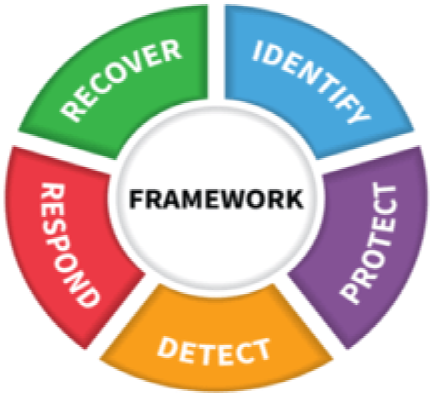
The result of this study indicated that, the selected bank cannot used any tools to protect the cyber security attacks. Therefore, based on insights gained from the analysis of literature on various international frameworks such as ISO/IEC27k series, Control Objectives for Information Technology (COBIT), IMF research papers, data analysis of interviews and questionnaire findings, and the student researcher exposure findings from different sources, the tools required to minimize cyber security attack at the financial institutions and critical infrastructures. Ethiopian banks have different goals, strategies, organizational cultures and structures. Consequently, the ideal management system and the way to accomplish things will differ among the other country's bank. Thus, this study proposed cyber security framework to minimize cyber security challenges at selected bank to control cyber security and used for management techniques.

IMF working paper entitled "Cyber risk for the financial sector: A framework for quantitative assessment" by Antoine Bouveret said that cyber-attacks can impact firms through the three main aspects of information security: confidentiality, integrity and availability. Confidentiality issues arise when private information within a firm is disclosed to third parties as in the case of data breaches. Integrity issues relate to misuse of the systems, as is the case for fraud.

The objective of the tools mainly focuses on supporting the achievement and understanding of three cyber security objectives across banks:

- ☞ Confidentiality,
- ☞ Integrity and
- ☞ Availability of information.

Finally, student researcher proposed ISO/IEC27k and Control Objectives for Information Technology, COBIT framework as the tools required to minimize cyber security attacks. Although there are several risk models and framework that directly attempt to address the cyber security issue and challenges, NIST released a comprehensive guidance on a wide range of security issues, and technical, operational and management security controls. The NIST cyber security framework defined by international cyber security framework standard define core five components of cyber security for a defense strategy (National Institute of Standards and Technology, 2014). This defense strategy helps the selected bank to minimize cyber security risk and aligning the strategy as context of the bank it is recommended too. The core five components of cyber security are: identify, protect, detect, respond, and recover. (NIST, 2014).



Source: NIST, 2014

CHAPTER FIVE

5. CONCLUSION AND RECOMMENDATIONS

This chapter presents conclusion and recommendations based on the analysis and findings of the research at selected bank. This portion also lists recommendations for future research.

5.1. Conclusions

This research used both quantitative survey and purposefully selected interviews are conducted to collect data. The quantitative survey is conducted by using questionnaire which was adapted and modified from International Telecommunication Union /ITU/, Global cyber security Index 2017 questionnaire and the research done entitled in "Cyber security practices and challenges at selected critical infrastructures in Ethiopia: Towards tailoring cyber security framework" by Tewodros Getaneh at Addis Ababa university.

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

- One of the major conclusions of this study is that the overall cyber security culture of the bank is not conducive for the protection of information assets and minimization of cyber-attacks. There is no appropriate foundation for defining how cyber security should be managed in the bank. The risk identification process and documentation as well as control mechanisms are unsystematic.

- The bank does not have a cyber security policy and guideline that systematically coordinates the cyber security activities in the bank as a financial institution, between departments, and individual employees. Cyber security activities, and information assets of the bank are not effectively organized and directed towards the information technology purpose and achievement of the bank business goals and objectives. Consequently, the absence security policy, standard and guideline implementation in the bank is a critical area of improvement.

Generally, the overall finding indicated in chapter four of cyber security challenges are a serious security threats, costing millions of birr in lost revenue of Ethiopian banking industry and the selected bank for the this research, even during this research Ethiopian broadcasting corporate/EBC/ covers the news of cyber security done in Ethiopian as well as the world since the attention given to cyber security protecting are low by the financial sectors. The findings from the research have shown that the management of cyber security threats in the context of the selected banks needs to be seriously looked at. The critical information assets management of the bank shows that they are vulnerable to attack.

5.2. Recommendations

From the results of this study finding there are several proposed improvements that can be undertaken to improve cyber security in the selected bank. Banking institutions need to invest in appropriate ICT security structures: example the use of new generation firewall which has capability of intrusion prevention, advanced malware protection and URL filtering. Therefore, there is need to have cyber security policies and develop a framework that to ensure that the bank follow the international and national security framework. There is also need to share cyber intrusion and penetration between the banking industry to provide a forum to enable the industry, to manage the cyber-crime threats and to improve their current systems and policies.

Financial institutions in Ethiopia are facing increasing cyber threats. This trend underscores the importance of strengthening cybersecurity measures. This means that, the selected bank must increase investment in cyber security technologies, provide cyber security related training to employees and hire proper professionals expertise to the IT directorate of the bank. It is also important to create cyber security awareness among employees to create an awareness to the non IT staffs.

Policy makers in the banking sectors should focus on increasing bank staff and public awareness of cyber security practices and strengthening regulatory and enforcement capabilities in cyber security areas. Regulations requiring strong cyber security measures in banking sectors need to be introduced and revised. Initiatives also need to focus on enhancing law enforcement capacities to increase certainty of punishment for those engaged in cybercrime activities.

The bank should implement a comprehensive and adequate set of cyber security components that aid in addressing threats on the technical, process and people levels based on identified cyber security risks and the appropriate controls that are necessary to mitigate the identified risks. The bank should adapt and implement international standards such as the Information Security Forum (ISF 2008), the Control Objectives for Information Technology (COBIT 2014), the Information Systems Audit and Control Association (ISACA 2008) and ISO/IEC 17799 (2017) to implement and manage cyber and information security components.

Executive management of the bank should organize information technology and security department at a higher possible level in the bank and seriously take cyber security agenda as an important performance measurement and should commit enough resources for the operation of cyber security in the bank. The bank should have to invest appropriate budget funding to the department to minimize cyber risk as a financial institution and arrange the program and find the local and international training to the staff of IT directorate as profession and fill the attitude and knowledge gab of the employees as whole.

Finally it is recommended to improve security weakness find by the finding of the study and the researcher recommends that the bank should include the role cyber security in employees job description and give awareness creation training to the staff who are directly access confidential information to be hacked by the cyber-criminal and develop the strategic plan for cyber security as bank and based on that, conduct the cyber security survey annually and provide the long- and short-term training of cyber security to the staff and certify them in international standard since cyber security is the worldwide issues.

5.3. Suggestions for Further Research

Before concluding, we suggest several potentially fruitful avenues for future research. Prior research has noted that cybercrimes targeting developing economies such as those in Africa exhibit a heavy concentration in specific financial sectors. In future conceptual and empirical work scholars need to compare and contrast financial sectors facing high profile of cyberattacks. The area of future research might be to examine institutional determinants of cyber-crime related legal and regulatory frameworks in banking sectors.

Due to the dynamic nature of the ICT and the cyber security challenge and the ever dynamic and innovation of ICT products in the banking industry to meet the customers need and to be a competitive edge. There is need to further study and to determine the changes and the dynamic nature of cyber-crime that becomes sophisticated with every transaction innovation and incorporating the opinion of INSA and cyber security professionals in our country with this study is recommended for future study. Another area of possible future research is to apply the methodology or develop a prototypical that helps to identify and combat cyber security challenges within the bank and used to analyze the dynamic nature of the cyber security threats problem.

Refencences

Abeselom Negussie(2015). Practices, Challenges and Prospects of Information Security in Ethiopian Banking Industry, School of Information Science , Addis Ababa University, Addis Ababa, Ethiopia.

Abiy Woretaw; Lemma Lessa. (2012). Information security Culture in the Banking sector in Ethiopia. in proceedings of the 5th ICT Ethiopia Conference. A.A. Retrieved from http://www.ictet.org/downloads/Inf_L5ww9o_1X7b.pdf.

Aychiluhim Desisa & Tebebe Besha (2014).Internet Banking Security Framework: The case of Ethiopian Banking Industry,HiLCoE Journal of Computer Science and Technology, Vol. 2, No. 2.

Babbie, E. (2002), "Survey Research Methods", Woodsworth: Belmont

Bahabtu Amare (2015). Assessment of Insider Threat in Ethiopian Banking Industry, School of Information Science , Addis Ababa University, Addis Ababa, Ethiopia.

Baino T. (2016) Evaluation of Security Risks Associated with Networked Information Systems. Melbourne: Royal Melbourne Institute of Technology University.

Bharat J. (2005) Intrusion Prevention and Vulnerability Assessment, Masters in/Technology Thesis.

Cherdantsevaa, Y. et al., 2016. A review of cyber security risk assessment methods for SCADA systems. elsevier, Volume 56, pp. 1-27.

Council, F.F.I.E. (2006, July). Information Security IT Examination Handbook. FFIE.

Creswell, J. (2003). Research design: Qualitative, quantitative and mixed methods approaches (2nd ed.).

Daniel Gebrehawariat (2017). Assessment of the Effectiveness of Card Banking Security in Ethiopian Financial Sector, School of Information Science , Addis Ababa University, Addis Ababa, Ethiopia.

ENISA. ENISA threat landscape 2015. European Union Agency for Network and Information Security; 2016 . Available from: https://www.enisa.europa.eu/publications/etl2015.

Franklin D. Kramer, An Integrated Governmental Strategy for Progress, IOSR – JCE pp. 136-150, (2011),http://www.jstor.org/stable/43133822.

Fritzvold, E. (2017). Cyber Security in Organizations. 1–178. Retrieved from https://brage.bibsys.no/xmlui/bitstream/handle/11250/2460083/Fritzvold_Einar.pdf?sequence=1&isAllowed=y

Gawthorpe, D. A. J. (2017). Cyber threats and cybercrime – a disruption of human security? 1(April), 1 46. https://doi.org/10.1109/UCC.2011.36

Grispos,G., Bradley,G.W,Storer,T.,"Security Incident Response Criteria: A practitioner's perspective." Hove.C.&Tarens.M(2013).Information Security Incident Management: An

Empirical Study of Current Practice.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. Journal of Management Information Systems, 28(2), 203-236.Hoe,

Halefom Hailu(2015). The State of Cyber Crime Governance in Ethiopia, Addis Ababa, Information Science, Addis Ababa University, and Addis Ababa, Ethiopia.

Hong, K., Chi, Y., Chao, L., R., Tang, J. (2003). An integrated system theory of information security management Information Management & Computer Security, 11(5), 243-248.

ITU. "Understanding Cybercrime" A Guide for Developing Country. Geneva: International Telecommunication Union (ITU).2009.

Johnson, R. B. & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. Educational Researcher, 33(7), 14-26.

Jung, J. (2018). A Study of Cyber Security Management within South Korean Businesses – An examination of risk and cybercrime involving industrial security. (July), 355. https://doi.org/https://researchportal.port.ac.uk/portal/files/12936107/Thesis_final_submission_Jeyong_Jung.pdf

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: management's effect on culture and policy. Information Management & Computer Security, 14(1), 24-36.

Kreicberga G. (2017) Internal Threat to Information Security-Countermeasures and human factor within SME. Kiruna: Lulea University of Technology.

Kruger, H. A., & Kearney, W. D. (2019). A prototype for assessing information security awareness. (June 2006). https://doi.org/10.1016/j.cose.2006.02.008

Makumbi et al (2018) An Analysis of Information Technology (IT) Security Practices: A Case Study of Kenyan Small and Medium Enterprises (SMEs) in the Financial Sector. Nairobi: University of Nairobi.

McGlasson, L. (2007, October 26). Tjx update: Breach worse than reported. Bank Info Security.

Mengistu Bogale Ayele (2016). Auditing IT and IT Governance in Ethiopia, School of Information Science, Addis Ababa University, and Addis Ababa, Ethiopia.

Mohammed, A., & Karen, N. Proceedings of the 7th Australian Information Security Management Conference: A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context. 2009.

Muckin, M., & Fitch, S. C. (2015). A Threat-Driven Approach to Cyber Security.

NIST. Framework for improving critical infrastructure cyber security, version 1.On-line available:http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214_nal.pdf, February 12, 2014.

Öğüt, H., Raghunathan, S., & Menon, N. (2011). Cyber Security Risk Management: Public Policy

Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. Risk Analysis, 31(3), 497-512.

Olayemi,J. O.(2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. International Journal of Sociology and Anthropology, 6(3), 116-125. doi:10.5897/IJSA2013.0510

Patrick, D. G. (2011). Managing Information Security Risk: Organization, Mission, and Information System View. U.S. Special Publication.

PWC (2011), Cybercrime: protecting against the growing threat. Global Economic Crime Survey, www.pwc.com/crimesurvey.

Rathaus N. (2009) Vulnerability assessment white paper: Automating Vulnerability Assessment, www.SecuriTeam.com

Raggad, B. G., & D, P. (2006). The Simple Information Security Audit Process : SISAP. Journal of Computer Science, 6(6), 189–198.

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information security management (ISM) practices: Lessons from select cases from India and Germany. Global Journal of Flexible Systems Management, 14(4), 225–239.

Reddy, G. N., & Reddy, G. J. U. (n.d.). A study of Cyber security challenges and its emergning trends on latest technologies.

Tagert, A. C. (2010). Cybersecurity Challenges in Developing Nations. PhD Thesis, 158. Retrieved from repository.cmu.edu/cgi/viewcontent.cgi?article=1021&context=dissertations

Tarino et al (2016) An Approach to Enhance ICT Infrastructures' Security Through Legal, Regulatory Influence. In J. E. HS Venter (Ed.), ISSA 2005 New Knowledge Today Conference. Sandton, South Africa.

Tesfaye Asfaw(2018). Cyber Security Auditing Framework (CSAF) for Banking Sector in Ethiopia. School of Graduate Studies, St. Mary's University, Addis Ababa, Ethiopia.

Tewodros Getaneh(2018). Cyber Security Practices and Challenges at Selected Critical Infrastructures in Ethiopia, School of Information Science , Addis Ababa University, Addis Ababa, Ethiopia.

The World Street Journal. 2016 . Swift reports summer cyber attacks on three banks. [cited 2016 Oct 9]. Available from: http://www.wsj.com/articles/swift-reports-summer-cyber-attacks-on-three-banks-1474924036.

Tonge, Kasture and Chaudhari(2013). Cybersecuirty Challenges for Society – Literature Review,

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. Computers & Security, 29(4), 476-486.

Venkatesh, V., & Brown, S. A. (2013). Guidelines for conducting mixed methods Research In Informations Systems. MIS Quarterly, X(X), 1–34.

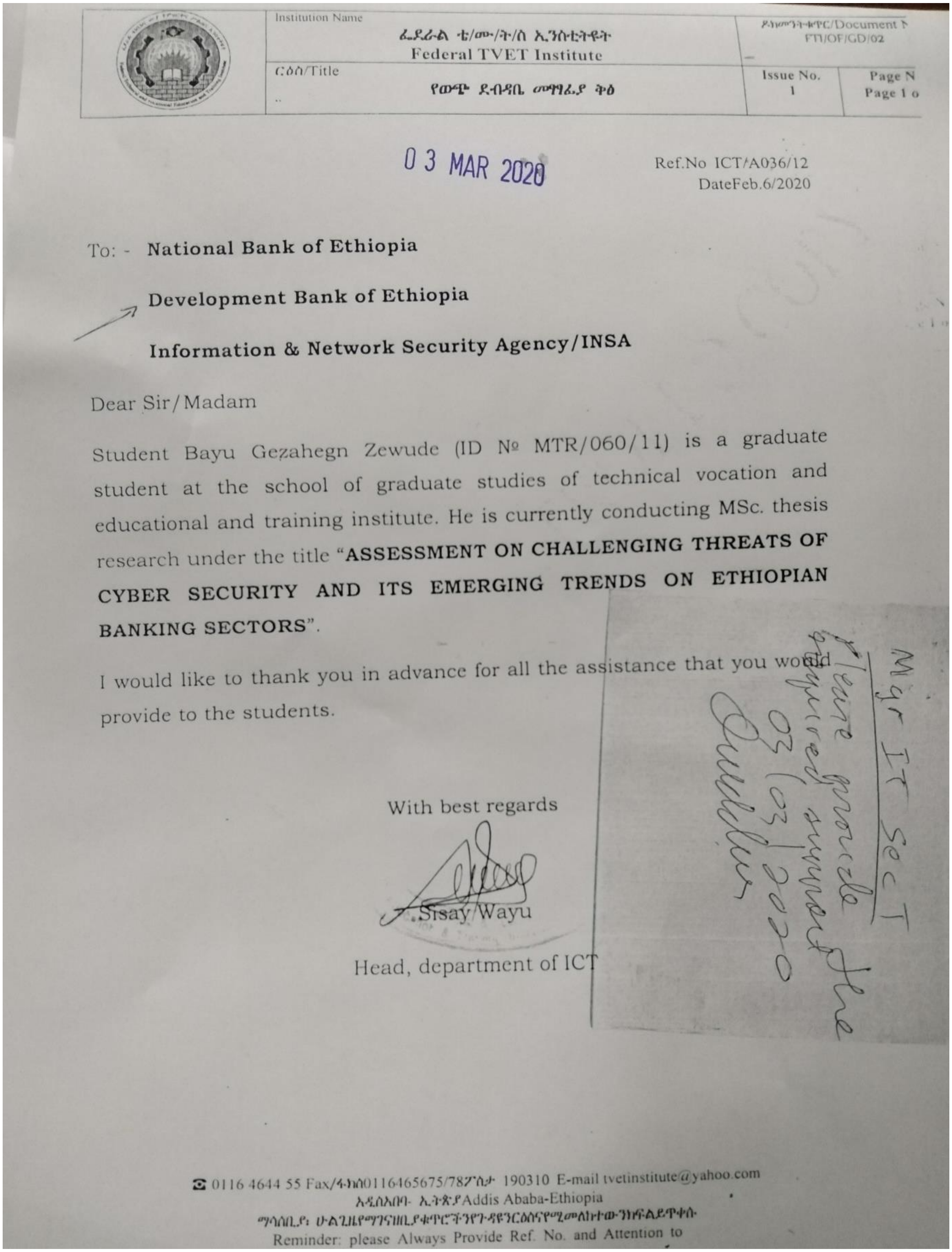
Walton CB,R. and Walton-Mackenzie Limited. 2006. Balancing the insider and outsider threat. Computer Fraud and Security,2006(11):8-11. Whitman,

Williams, C. (2007). Research Methods. 5(3), 65–72.

Woodside, A. G., & Wilson, E. J. (2003). Case study research for theory-building Journal of Business & Industrial Marketing Article information : (March 2016). https://doi.org/10.1108/08858620310492374

Zegers, N. (2016) A Methodolgy for Improving Information Security Incident Identification and Response. Rotteram: Erasmus Universiteit Rotterdam.

Annex 1. Letter to collect data



	Institution Name ፌደራል ቴ/ሙ/ት/ስ ኢንስቲትዩት Federal TVET Institute	ዶክመንት ቁጥር/Document N FTI/OF/GD/02	
	ርዕስ/Title የወጭ ደብዳቤ መፃፊያ ቅፅ	Issue No. 1	Page N Page 1 o

0 3 MAR 2020

Ref.No ICT/A036/12
DateFeb.6/2020

To: - **National Bank of Ethiopia**

Development Bank of Ethiopia

Information & Network Security Agency/INSA

Dear Sir/Madam

Student Bayu Gezahegn Zewude (ID № MTR/060/11) is a graduate student at the school of graduate studies of technical vocation and educational and training institute. He is currently conducting MSc. thesis research under the title “**ASSESSMENT ON CHALLENGING THREATS OF CYBER SECURITY AND ITS EMERGING TRENDS ON ETHIOPIAN BANKING SECTORS**”.

I would like to thank you in advance for all the assistance that you would provide to the students.

Mgr IT Sect
Please provide
required support the
03/03/2020

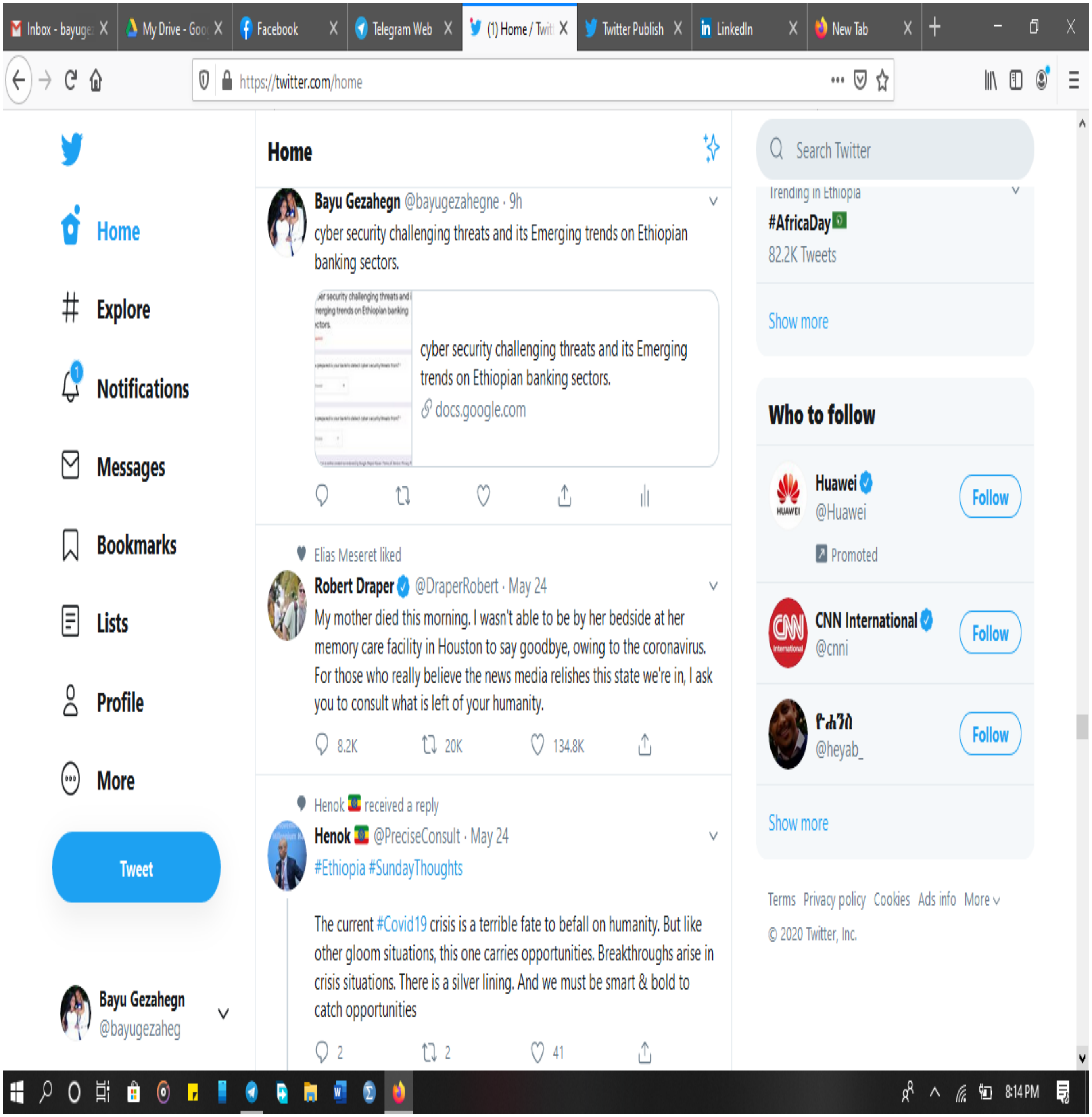
With best regards

Sisay Wayu

Head, department of ICT

☎ 0116 4644 55 Fax/ፋክስ0116465675/78ፖስታ 190310 E-mail tvetinstitute@yahoo.com
አዲስአበባ- ኢትዮጵያAddis Ababa-Ethiopia
ማሳሰቢያ፡ ሁልጊዜየማገናዘቢያቁጥርችንየጉዳዩንርዕስናየሚመለከተውንክፍልይጥቀሱ
Reminder: please Always Provide Ref. No. and Attention to

Annex 2. Online published questioner through twitter.



Bayu Gezahegn @bayugezahegne · 9h

cyber security challenging threats and its Emerging trends on Ethiopian banking sectors.

cyber security challenging threats and its Emerging trends on Ethiopian banking sectors.

docs.google.com

Elias Meseret liked

Robert Draper @DraperRobert · May 24

My mother died this morning. I wasn't able to be by her bedside at her memory care facility in Houston to say goodbye, owing to the coronavirus. For those who really believe the news media relishes this state we're in, I ask you to consult what is left of your humanity.

8.2K 20K 134.8K

Henok received a reply

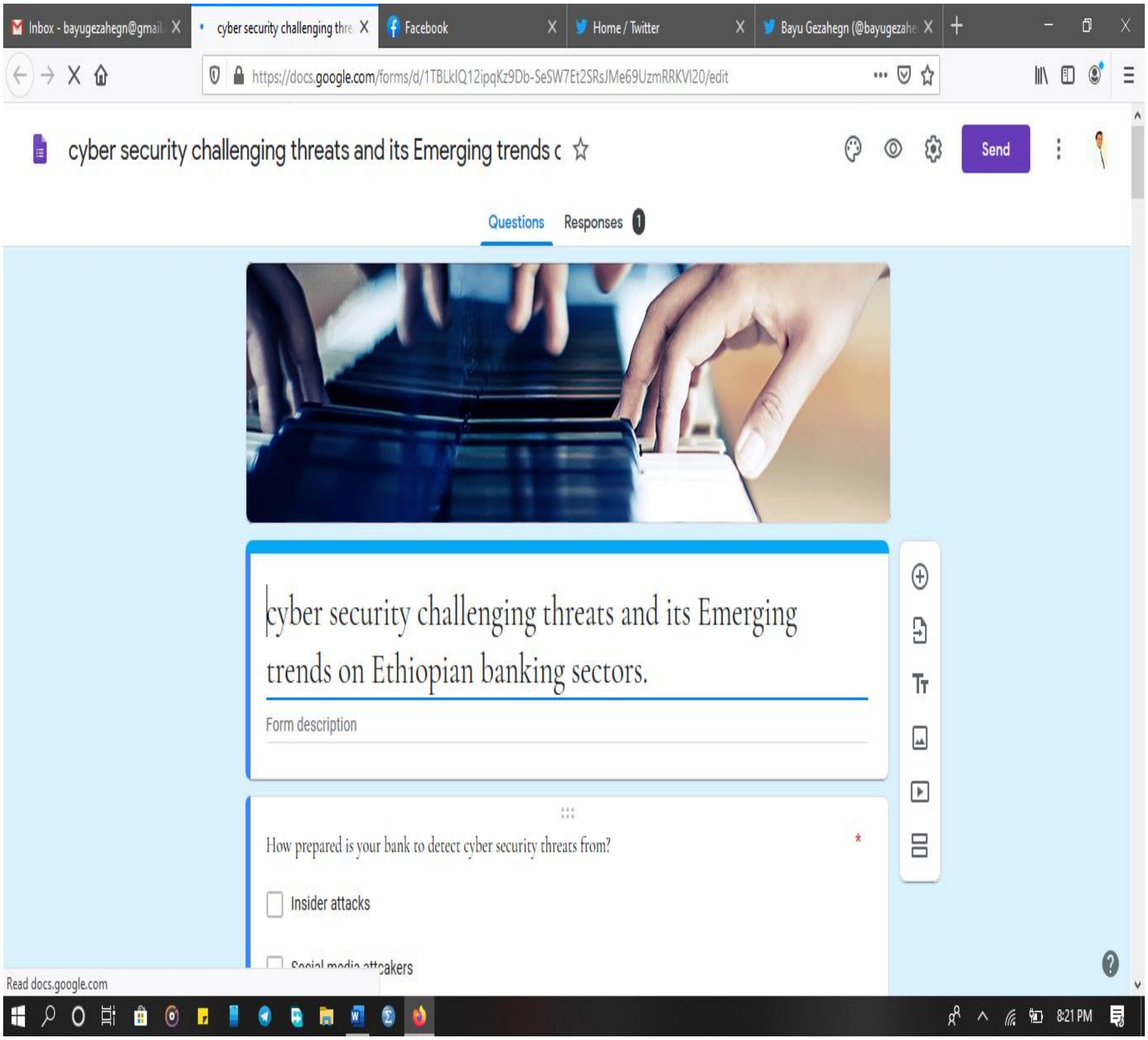
Henok @PreciseConsult · May 24

#Ethiopia #SundayThoughts

The current #Covid19 crisis is a terrible fate to befall on humanity. But like other gloom situations, this one carries opportunities. Breakthroughs arise in crisis situations. There is a silver lining. And we must be smart & bold to catch opportunities

2 2 41

Annex 3. Online published through google doc.


Inbox - bayugezahegn@gmail.
cyber security challenging thre
Facebook
Home / Twitter
Bayu Gezahegn (@bayugezahe
https://docs.google.com/forms/d/1TBLkIQ12ipqKz9Db-SeSW7Et2SRsJMe69UzmRRKVI20/edit
cyber security challenging threats and its Emerging trends c
Send
Questions
Responses 1
Form description
Read docs.google.com
8:21 PM

cyber security challenging threats and its Emerging trends on Ethiopian banking sectors.

How prepared is your bank to detect cyber security threats from? *

□ Insider attacks

□ Social media attcakers

Appendix 1. Research Questionnaire for IT Professionals

TECHNICAL VOCATIONAL EDUCATION AND TRAINING INSTITUTE, ADDIS ABABA - ETHIOPIA

SCHOOL OF GRADUATE STUDIES

FACULTY OF ELECTRICAL ELECTRONICS

and

INFORMATION & COMMUNICATION TECHNOLOGY

Dear respondent,

First of all, I would like to thank you in advance for devoting your valuable time to fill the questionnaire. This questionnaire is prepared *to assess and challenging threats of cyber security and its emerging trends on selected banking in Ethiopia* and *exploit as an input develop enhanced cyber security framework*.

The study is done as part of partial fulfillment *of Master of Science in Information Communication Technology Management*. Your data is expected to contribute for the success of the study tremendously. This research is believed to produce results that can improve the protection of cyber security in selected banking. Your honest responses to each questions and statement are extremely valuable to the outcome of this research. The questionnaire survey will take approximately 25 minutes to complete and the results of the survey will be used for the purpose of academic research only. Hence, all responses will be kept in strict confidentiality.

Your dedication is most valued and appreciated and I would like to take this opportunity to thank you in advance for your kind participation, genuine and on time response to the questionnaire.

If you have any enquires, you may contact me via the address stated below.

Thank you again!

Bayu Gezahegn

E-mail: bayugezahegn@gmail.com

Mobile: +251-912-381-666

Thank you so much for your cooperation in advance.

General Instruction:

Please put tick sign (√) in the square bracket for each item.

Part 1: PROFILE OF RESPONDENTS

1. Sex: □ Male □ Female
2. Marital status: □ Single □ Married □ Others
3. Age: □ 20-30 □ 30-40 □ above 40
4. Educational Level: □ Diploma (Level IV)

   □ First Degree □ Masters □ PhD
5. Your Profession:

   □ Computer Science □ Computer Engineering

   □ IT / ICT □ Information System

   □ Cyber Security □ Others
6. Position: ____
7. Work Experience: □ 0 – 3 years □ 3 – 5 years

   □ 5 – 10 years □ 10 – 15 years

   □ above 15 years

Part 2: The following questions are intended to assess and explore cyber security challenges and its emerging trends in DBE for ***IT and cyber security professionals***.

	Inadequately Prepared ***(1)***	***Somewhat inadequately Prepared*** ***(2)***	***Somewhat secured*** ***(3)***	***Secured*** ***(4)***	***highly Secured*** ***(5)***
How prepared is your bank to detect cyber security threats from?					
1) Insider attacks					
2) Social media attackers					
3) E-mail attackers					
4) Cyber-criminals					
5) External attacks					

	Yes ***(1)***	***No*** ***(2)***	***I don't Know*** ***(3)***
Cyber Security Policy and Standards			
1) Is your bank information/cyber security policy often considered as a barrier to technological opportunities?			
2) Do you have Cyber Security policy document to ensure the security of your bank cyber system?			
3) Is the cyber security policy feasibility and effectiveness, as well as the cyber security team's efficacy, regularly reviewed by an independent body?			
System Development and Maintenance			

4) When implementing new technologies, do you assess their potential impact on the established cyber security policy?			
5) Are the processes to implement new technologies documented in your bank?			
6) Is there a culture of conducting cyber security requirement study before systems development and test its security related issue in your bank?			
7) Are there protective measures to reduce risk when implementing new technologies?			

	Strongly Disagree (1)	***Disagree (2)***	***Undecided (3)***	***Agree (4)***	***Strongly Agree (5)***
How do your rate your bank top cyber security challenges?					
1) Lack of professional expertise					
2) Loss of sensitive or confidential data.					
3) Poor leadership					
4) Inadequate enabling technology					
5) Insufficient funding					
What type of security threats attack your banks has experienced over the last 5 years?					
1) Attack via E-mail					
2) Attacks via social media					
3) Insider attacks					
4) Hackers attack					
5) Web-based attacks and Web application attacks					
6) Malware attack					
7) Information Disclosure and Denial of service attack					

8) A cyberattack is a perceived threat to network security, data and information.					
9) A Virus attack is a type of a cyber-attack.					
10) Cyber-attackers focus on targets such as networks, servers and routers.					
11) In our bank, government practices and guidelines has helped us in safeguarding against cyberattacks.					
12) Our bank has implemented an effective anti-virus software program to safeguard against cyberattacks.					
13) Our bank has implemented an effective up-to-date software patching procedure to safeguard against cyberattacks.					
14) The bank uses emerging technologies to minimize cyber risk					

Appendix 2. Research Questionnaire for non IT Professionals

The following questions are intended to assess and explore cyber security challenges and its emerging trends in DBE for **non-IT *and cyber security staff of the bank employees.***

	Strongly Disagree *(1)*	***Disagree*** *(2)*	***Undecided*** *(3)*	***Agree*** *(4)*	***Strongly Agree*** *(5)*
Cyber security challenging threats knowledge and skill in your banks.					
1. Our employees' written job description include responsibility for cyber security.					
2. I understand the importance of choosing a strong password					
3. Our bank understands the risk of cyberattacks and the importance of implementing safeguarding techniques.					
4. Our bank has invested adequate funds to promote countermeasures against cyberattacks.					
5. All employees in our bank are aware of the strategic plan implemented to protect against cyberattacks					
6. Senior management has an important role in developing cyber security policies for our bank.					

7. Cybersecurity generally should be the responsibility of the IT department.					
8. Our bank has implemented software solutions to protect against cyberattacks.					
9. All employees who join our bank must go through a cybersecurity awareness training.					
10. Employees in our bank understand their responsibility in preventing against cyberattacks					
11. Our employees know the importance of keeping their passwords secret.					
12. Our employees understand the importance of not connecting their personal devices (smartphones etc.) on bank network systems.					