ADDIS ABABA UNIVERSITY
COLLEGE OF NATURAL SCIENCE
SCHOOL OF INFORMATION SCIENCE

CYBER HYGIENE PRACTICES AMONGST EMPLOYEES OF ETHIOPIAN COMMERCIAL BANKS

By

Biruk Deferew

March, 2020

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL SCIENCE

SCHOOL OF INFORMATION SCIENCE

CYBER HYGIENE PRACTICES AMONGST EMPLOYEES OF ETHIOPIAN COMMERCIAL BANKS

A Thesis Submitted to the School of Graduate Studies of Addis Ababa University in Partial Fulfillment of the Requirements for the Degree of Master of Science in Information Science

By

Biruk Deferew

March, 2020

CYBER HYGIENE PRACTICES AMONGST EMPLOYEES OF ETHIOPIAN COMMERCIAL BANKS

By

Biruk Deferew

Name and Signature of Members of the Examining Board

	Name	**Signature**	**Date**
Advisor	Rahel Bekele (PhD)	_____	_____
Examiner	_____	_____	_____
Examiner	_____	_____	_____
Chairperson	_____	_____	_____

Declaration

I declared this thesis is my original work and has not been presented in any university.

Biruk Deferew

Signature _____ Date_____

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

Dr. Rahel Bekele (Advisor)

Signature _____ Date_____

Table of content

Acknowledgments

First of all, I would like to say thank you to the almighty God, for all of my life and he gave me the wisdom to accomplish this work. And his beloved mother St. Marry, she was with me yesterday, today and she will be with me forever assisting me in every aspect of my life.

I also would like to say thank you to my advisor Dr. Rahel Bekele from the bottom of my heart that she was guiding me in each and everything of the research, giving me a major and minor corrections and directions without any tiredness.

I also want to say thank you to my ex-wife Sisay, and I want to pass my deepest gratefulness to my beloved family as a whole.

Again I want to say thank you to a lot of people who helped me in this research especially my friends who coordinated, participated in the collection of data such as Yelewtfrie, Henok, Abraham, Zelalem, and others whose names are not mentioned.

Abstract

The ever-expanding cyberspace bring benefits to the financial institutions and there is also threats of attacks through it. Cyber hygiene is like a human being keeping its own personal hygiene not to be exposed by any types of disease, the same is true for cyber hygiene; keeping aside the cyber threats and attacks away. The Ethiopian commercial bank experience insider attacks such as password theft and email phishing attack were observed. Security is a big problem and it needs a big emphasis so that the purpose of the study is to evaluate current cyber hygiene practices of the employees in the Ethiopian commercial banking industry. Quantitative research methodology was used to conduct this research. Among 18 Ethiopian commercial banks three banks (such as Dashen bank, Abay bank, and Commercial bank of Ethiopia) were selected by using stratified sampling and based on the year of core banking automation criteria. The research used convenience sampling method to identify the sample. The primary data collection instrument was self-administered questionnaire which was adapted from related research. SPSS version 20 was used to for data analysis; the research was conducted at the head office and branch level of the selected banks.

Even if the finding shows that there was a gap on computing cyber hygienic practices but there is an observation of a good cyber hygiene practice like that of users didn't stick their password on the office desk, not shared their password and unauthorized person is not allowed to use their computer. Respondents assure that their bank have a clear, specific, formal and understandable ISSP. And its practices of the Ethiopian commercial banks and the respondents' attitude was very good regarding the banks ISSP. The respondents underline that, there was lack of periodic formal cyber hygiene training. The finding of the study shows, the need for regular assessment and follow up so as to provide strategic and adequate training.

Keywords: Cyber, Cyber hygiene, Cyber hygiene practice,

List of Tables

List of Figures

Table of Abbreviations

ATM - Automatic Teller Machine

BBO - Bank Business Officer

BoD - Board of Director

CBE - Commercial Bank of Ethiopia

CORE - Centralized Online Real-time Exchange

CRO - Customer Relation Officer

CSM - Customer Service Manager

CSO - Customer Service Officer

DDoS - Distributed Denial-of-Service

DoS - Denial-of-Service

E-Banking - Electronic banking

IDS - Intrusion Detection System

INSA - Information Network Security Agency

ISP - Information Security Policy

ISSP- Information System Security Policy

JCO - Junior Credit Officer

MIS - Management Information Systems

NBE - National Bank of Ethiopia

Chapter One
Introduction

1.1. Background

The information superhighway has found its way into many homes, schools, businesses, and institutions. Digital technology has revolutionized economic and social interaction. It has transformed the way we do business, the way we educate ourselves, the way we sell and buy products and share data. Internet use is growing, and the methods by which it is accessed are diversified. Side by side cybersecurity is an emerging challenge for the national security of countries across the world as cyber-attacks have become more advanced and frequent over the years (Horne, 2014; Griffiths, 2016).

Ethiopia has also embraced ICT and ICT-based services as key enablers for social and economic development. Various additional efforts to significantly increase internet connection speeds and access are underway. Larger bandwidth makes better internet access, as greater bandwidth can also enable faster and better means of launching cyber-attacks and more openings for criminals to exploit new internet users of mostly in the banking industry (Hailu, 2015).

Countries economy relies on the banking industry, and the contemporary banking business highly dependent on the information system. The dynamic change of information technology, advancement of customer requirement and business competition force banking industry to use the information system to process their financial transactions. Information is an important business asset to all organization (IS017799, 2005: 1); that existed in different forms such as paper and electronic documents, voice recordings and conversations. It is stored in electronic databases, backups, archives, and hard copy files; which can easily be transmitted electronically or by post and even as films and SMSs (short message service), so that the financial information must handle safer than ordinary information. The financial transaction must be secured, and its processing should be very safe and secure from any type of threat (Veiga, 2008).

Accordingly, as with other business assets, the information requires protection to ensure that it is available, confidential and that its integrity is preserved where necessary (ISO17799, 2005: 1). Advancements in IT have exposed organizations to information security threats especially with the widespread use of the internet, electronic handheld devices and wireless technologies (ISO/IEC 17799 (BS 7799-1), 2005).

Threats such as data theft, fraud, fire, viruses, denial of service attacks and even social engineering pose serious risks to the protection of information. These threats, together with careless mistakes and employee ignorance with respect to security controls could lead to severe financial, reputational and other damages to an organization (Veiga, 2008).

According to Africa cybersecurity report (2017), banks were the top risk sector of all lists. This sector mainly faced two main problems such as increasingly being targeted by attackers and those who were attempting to stay ahead of the attackers were pulled back by malicious insiders (Serianu, 2017).

Commercial banks in Ethiopia play big role in economic development through the mobilization of funds from, within and outside the country and channeling such funds to various sectors of the economy. Banks occupy a central place in the payment and settlement system of the country's economy. This industry operates under central bank governing rule, i.e. National Bank of Ethiopia (NBE). Totally there are 18 banks which operate in the country, out of which 16 are private banks and the left are governmental banks (NBE website, 2014).

This research study investigates cyber hygiene practices of Ethiopian commercial banks among employees, so that the stakeholders get ready on the matter of countermeasure to protect their bank from insider threat and information theft of cyber-criminal.

1.2. Statement of the Problem

Nowadays organizations totally or partially depend on IT for better, effective communication and daily operational tasks. Global financial institutions are interconnected with one another. So it is critical to maintain effective information security in banks. Any mishandling of these confidential

financial information assets can cause huge financial loss, and the reputation of the bank would be severely damaged (Woretaw & Lessa, 2012). Maintaining information security requires a support and co-operation from all employees within the organization (Daniel et. al., 2013).

As more and more devices are connected to the Internet every day, it has provided cybercriminals with the opportunities to inflict greater harm to society. The increase in the growth of malware technology combined with the inexperience of new internet users has made threats from malware detrimental to the targeted parties (H1, 2017).

To optimally utilize new technology for producing new digital products, the IT system at banks need to be robust. It should be able to handle when maximizing the volume in a secure manner, providing connectivity to different applications accessing the bank's CORE (Centralized Online Real-time Exchange) banking solution in a secure way and at the same time making sure for the confidentiality of customer information. Recognizing these challenges, the National Bank of Ethiopia has been providing guidance to banks in managing the adoption of technology (Mundra, 2016).

Kassa (2017), stated that in Ethiopia by the year 2017, insiders attempted to attack on some financial institutions of the country in collaboration with outsiders. According to one of the Ethiopian commercial bank's report in the year 2018, the bank's management decision committee discussed and decided on the issue of a shared password. The case was an employee shared his password to another employee for the purpose not to halt the bank business transaction process at lunch time, but the other employee used it for the illegal purpose of financial statement fraud. And finally, the committee decided to penalize for the illegal practice of the employee. Moreover, there were email phishing attacks report approved by one of the Ethiopian commercial banks IT security department. The case was one of the bank employees received an email from "Mailbox Account" with "Important Notice" as a subject. The email requests the user to click a link in order to update the email account. The department investigation found out that by using malicious virus, the link redirects to fake company webmail access webpage which requests the user's company email and its password (CBE, 2013; Kassa, 2017).

In addition to the above-stated problems such as insider attacks of password theft, email phishing, and other related cyber hygiene threats, security is a big problem especially in the case of the financial industry. As stated previously, banking industry is the prime target of the insider and outsider attacks, and it needs a high emphasis on this regard. The insider attack is directly related to the good and bad cyber hygiene practices of the employee so that this research needs to be conducted with respect to the employee perspective.

Therefore, this research aims to evaluate current cyber hygiene practices in the Ethiopian commercial banking industry, and assess the cybersecurity awareness level of the employees in the industry, so that the researcher formulated the following research questions for investigation.

1. What is the existing cyber hygiene status of employees in the Ethiopian banking industry?
2. What is the level of cybersecurity awareness among employees?
3. Does information security policy, procedure and guideline are applied in the Ethiopian commercial banks?
4. How can cyber hygiene practice be improved?

1.3. Objective of the study

1.3.1. General Objective

The general objective of the study is to illustrate the cyber hygiene practices between employees of Ethiopian commercial banks.

1.3.2. Specific Objectives

To achieve the general objective, the study has the following specific objectives:

- To understand the Ethiopian commercial banks employee cyber hygiene practices
- To identify whether information security policy, procedure, and a guideline of the bank were implemented
- To evaluate the employees' awareness regarding information security policy, procedure, and a guideline of the bank

- To identify whether regular awareness creation training was conducted
- To identify key gaps that need management and policy intervention so that effective cyber hygiene practice can be established

1.4. Scope and Limitation of the Study

Contemporary Ethiopian commercial bank business used an information system to facilitate their business activities. Therefore this study focuses on the assessment of Ethiopian commercial banks insiders' cybersecurity practice at head office organs and branch level. The study is limited to show how the employees behave to their bank information system, such as practices of the cyber hygiene, ISSP (Information System Security Policy), level of awareness. And to find out how employees behave on the routine tasks to protect their workstation of cyberspace according to what is perceived as correct and acceptable based on their organization ISSP, so that the staff safeguards its financial information, and the study didn't cover the security feature, measures, and other related areas.

This study research is bounded only in the Ethiopian commercial banks transaction related information system users.

1.5. Significance of the Study

The risk that employee behavior poses to the protection of information assets is the vital focus area. The employees should perform their task as per the organizational security policy, procedure and guideline or security rule and regulation of the organization. According to McIIwrath (2006), two to three percent of an organization's annual profit is potentially lost due to information security incidents (Veiga, 2008).

The 2017 African cybersecurity report analyzed over 90% of African organizations were operating below the security poverty line. Significantly exposing themselves to cybersecurity risks and it cost annually for cyber-attack $3.5 billion. The banking sector was the most targeted industry of insider as well as outsider cyber-attack. It is required to identify the cyber hygiene practices of the Ethiopian commercial banks employee (Serianu, 2017). So that decision-makers such as

policymakers, practitioners, and stakeholders of the Ethiopian commercial banks can use this study outcome to develop their cyber hygiene practice of their staff.

1.6. Organization of the Study

This thesis was organized in five chapters; the first chapter introduction contains the background of the study, statement of the problem, research questions, significance of the study, objectives, and the scope and limitation of the study. The second chapter literature review constitutes detail literature review about cyber hygiene and cybersecurity and tried to include related works. Chapter three was all about the methodology that was used to conduct the research; this includes research design, study population, data collection instruments, study variable, sampling design, data analysis and presentation and reliability of the research. Chapter four enclosed arithmetic finding of the study and its discussion. Chapter five finally concluded the study, state the recommendations and final suggestion for future work.

Chapter Two
Literature Review

2.1. Overview

In this chapter, supportive literature to the study has been reviewed. It is presented and used as the base for the researcher to understand the research area of what others had done in considering the cyber hygiene practices and the related research. Accordingly, there are a lot of subsequent subtopics such as cyberspace evolution, tools used to cyber-attack and their actor, cyber hygiene, insider threat, cybersecurity global perspective, information security which are reviewed from different sources such as reports, periodic articles, journal articles, and books. In addition related works are also stated at the end of the chapter.

The emergence of the Internet and the advancement of technology bring infinite benefits to the world. Our lives are exemplified by the digital transformation that is occurring in many aspects and being played out in the virtual world of cyberspace making life easier and digital transformation. The dependency between human life and cyberspace is increasing. The financial sector is one of the most dependent businesses to the cyberspace; at the same time, its vulnerability to harm events also increasing (Jackie, 2018).

According to Hassan (2017), in Nigeria financial sector stood first for the sector that releases the highest number of cybersecurity tenders. Within the country and based on the previous experience the most critical cybersecurity challenges being faced by the local market was budget and lack of awareness.

2.2. Cyberspace Evolution

Cyberspace is a dynamic evolving environment and cyber power is built on quickly shifting environment of cyberspace, which includes not only the internet, but also the legacy telephony infrastructure, cellular phone technologies, and wireless data services. The technologies underlying all of these aspects of cyberspace such as processor speed, bandwidth, functionality,

interconnectedness, and security vulnerabilities have evolved over the decades (Skoudis, 2012; Jackie, 2018).

Skoudis (2012) stated about the evolution of cyberspace and discussed that there are three types of trends:

- Computer and network
- Software
- Social

Computer and network trends enclose the increases in computer and network power, the proliferation of broadband connectivity, the proliferation of wireless connectivity and the transition from Internet Protocol version 4 (IPv4) to IPv6. Although IPv6 deployment has started slowly, it is expected to ramp up; both the Chinese government and the U.S. military has announced IPv4's 32-bit addresses move to 128-bit address space of IPv6 by 2012 to support the modernization of their large networks.

Software trends include an increase in software complexity, enhanced capabilities for search both across local systems and internet-wide, widespread virtualization of operating systems, the convergence of technologies, increased noise in most aspects of cyberspace, and increased vulnerability due to the advancement of computer and network attack and exploit methodologies.

The social trends in the use and development of cyberspace contain worldwide technological development, with different local emphases and the rise in online communities, collaboration, and information-sharing (Skoudis, 2012).

One of the innovations in technology has brought the evolution of methods to deliver financial services. The industry has gone from the widespread use of ATMs in the 1980s to modern point of sale (PoS) terminals in the 1990s, to Internet banking in the 2000s and mobile banking in 2010s. These new and evolving ways of meeting consumer demand, however come with new fraud patterns and evolving risks of cyber-attacks (CSBS, 2014).

2.3. Tools Used to Cyber-Attacks and their Actors

Cybercriminals use a variety of tactics and strategies to attack the cyberspace. Phishing is one of the most common terms associated with cybersecurity. Phishing is a technique aiming to steal private information from users through masquerading as a trustful source (e.g. website). It usually occurs via an email which takes on the appearance of official correspondence from trusted sources like that of a bank or a known entity. The aim is to redirect the user then enter account details or hand over personal data unknowingly (Griffiths, 2016), such as usernames, passwords, credit card details, or personal sensitive information, date of birth and social security number, that can be used to commit identity theft against the individual or gain access to bank systems for theft, disruption, destruction of the information can help the attackers to use it for a criminal purpose. Microsoft Office extensions are the most malicious file extensions used by email hackers, Phishing emails are responsible for about 91% of cyber-attacks, and 92% of malware is delivered via email (Benardo, 2015; Thebestvpn, 2019).

Social engineering is the generic term that label techniques used to gain unauthorized access to information through human communication. DDoS (Distributed Denial of Service) is a type of attack that compromises the availability of data, in the way that the attacker floods the victim (e.g. server) with commands (Bendovschi, 2015). Ransomware is similar to DoS (Denial of Service) as it denies access to services, effectively locking it until a fee is paid. This capability is aimed primarily at customers, albeit recent variants have been shown to target businesses directly (Horne, 2014).

Malware or malicious software is a generic term describing types of malicious software, used by the attacker to compromise the confidentiality, availability, and integrity of data. Most common types of malware are viruses, worms, Trojans, spyware, ransomware, adware, and scare-ware or rogware. The number of groups using destructive malware was increased by 25% in 2018 (Bendovschi, 2015; Thebestvpn, 2019).

2.3.1. Types of Malware

Malware or malicious software is intended to interrupt and damage computers without the users' consent. Malware includes worms, spyware, viruses, and other malicious programs could be classified in several ways in order to differentiate them from one another and giving a better understanding of how they infect. The malware data is detected from four countries such as Malaysia, Indonesia, Brunei, and France. This report was classified the best-known malware types that have been detected in the region which include Trojan, Worms, Backdoor, Downloaders, and Ransomware. The following figure 1 represents the malware types detected in the region between January to June 2017 (H1, 2017).

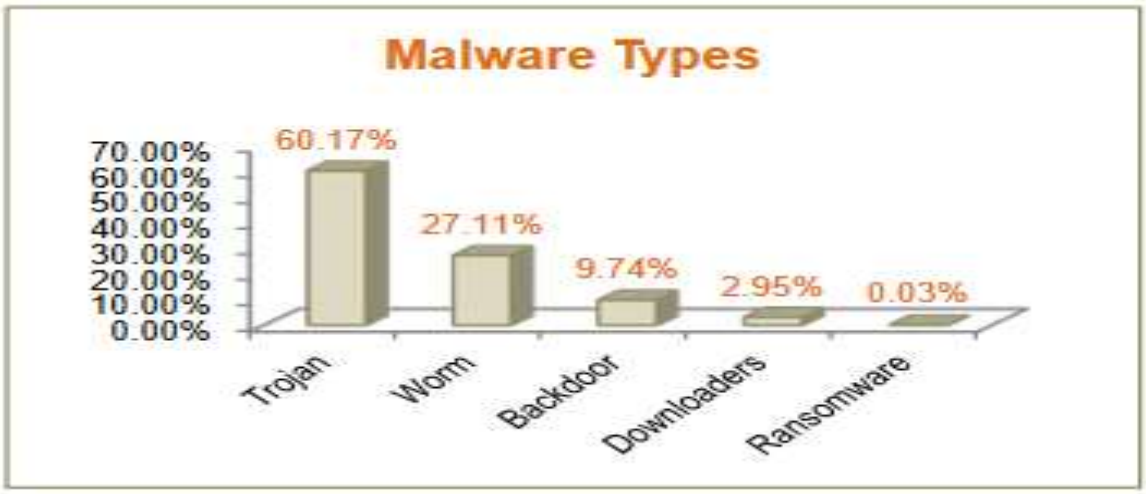

Figure 1: Malware type report 2017 (Source: (H1, 2017))

The first half-year of 2017 was compared with the second half-year of 2016 and presented in the following table 1. The malware types show that in the duration from January to June 2017 the computers, servers, and users were infected primarily by Trojans followed by Worms. The Malware infection detected through Trojan was comparatively higher at 60.17%, 5 times compared to the previous report. In the previous second half-year of 2016, worms are shockingly high at 77.64% compared to the first half-year 2017 which was relatively lower to 27.11%. As per the analysis, malware threats were evolved over time (H1, 2017).

Table 1: Malware type 2016 and 2017 report (Source: (H1, 2017))

Malware types	H2 2016	H1 2017
Trojans	12.04%	60.17%
Worms	77.64%	27.11%
Backdoors	9.03%	9.74%
Downloaders & Droppers	1.26%	2.95%
Ransomware	0.03%	0.03%

Another way of cyber-attack is structured query language (SQL) injection. It is a common way in which websites of organizations attacked. Web applications usually interact with backend databases and when the application receives a request from the user. It fetches the database by generating and executing SQL queries to interact with the relational database. These queries look for the requested data to be displayed in generating HTML pages to the user. In this normal scenario, the user inputs are treated as lexical entities. However, when the user inserts unexpected inputs that are not addressed in the web application's dictionary, the command will lead the webserver to react abnormally. This may cause the web application to display unexpected data which may be classified as confidential. It may be useful for the attacker. This is known as a command injection attack. And such commands could be SQL queries or operating system commands or JavaScript & HTML tags (Ali, 2011; Griffiths, 2016).

2.3.2. Cyber-Attack Actors

Hacktivists: The name derives from "hack" used to describe the use of cyber technology to attack a computer system and the word "activism" which involves bringing social or political change. It is commonly carried by an organization or individual (Griffiths, 2016). Hacktivists are politically and socially motivated individuals use computer systems in order to protest and promote their cause activists. Having increasingly taken to break into computer systems demonstration for political or social causes, hacktivists group use DoS to raise the profile of their campaign and generate publicity, which ultimately erodes customer confidence by disrupting online services (Horne, 2014; Serianu, 2017).

Cyber-criminal: Hostile financial gain and has a high skill level by nature. The main cause of data breaches are malicious or criminal attacks. They are responsible for 48% of all data breaches and 76% of cyber-attacks. They were financially motivated and the global cost of cybercrime is expected to exceed $2 trillion in 2019 (Strauss, 2017; Thebestvpn, 2019).

Corporations: Organizations involved in offensive tactics aim to gain competitive advantage (Strauss, 2017).

Employees (Insiders): Cyber-attacks which emerged due to acts committed by a staff member that is employed by private or governmental Companies, staff, and contractors. Insiders assisting syndicates possesses a significant amount of knowledge that allows them to place effective attacks against assets of their organization (Griffiths, 2016; Strauss, 2017).

Terrorist: Preferred targets of cyber terrorists are mostly critical infrastructures (e.g. public health, energy production, telecommunication), as their failures cause severe malicious impacting in society and government (Strauss, 2017).

Nation-states: Nation-states can have offensive cyber capabilities and could potentially use them against adversary cyberwarfare (Strauss, 2017).

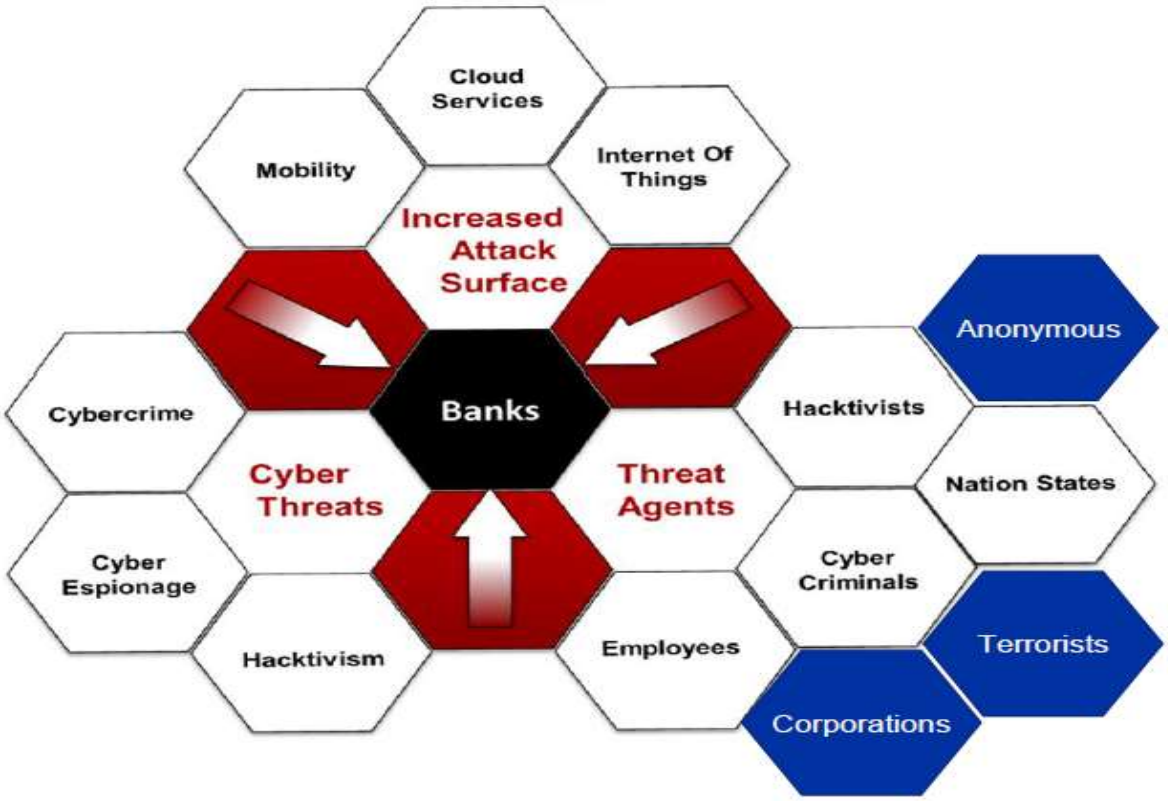

Figure 2: Cyber threat landscape architecture (Source: (CSIR, 2017))

2.4. Cyber Hygiene

Each organization is at risk to be attacked whether it is large or small. Small or midmarket businesses are the focus area of attacks and often serve as a launch pad or conduit for bigger campaigns. Adversaries view small or midmarket businesses as soft targets that have less sophisticated security infrastructure and practices inadequate number of trained personnel to manage and respond to threats. According to cybersecurity research conducted by Cisco (2018), more than half (54%) of all cyber-attacks resulted in financial damage of more than US$500,000, including lost revenue, lost customers, lost opportunities, and out-of-pocket costs. This much amount is enough to put an unprepared small or midmarket business out of operation permanently. While the personnel is trained but it may practice with unhygienic manner to the cyberspace of the organization, the business will no longer sustain (Cisco, 2018; Cisco special report, 2018).

Cyber hygiene is often compared to personal hygiene. Like an individual engages in a certain personal hygiene practices to maintain good health and well-being, cyber hygiene practices can keep data safe and well-protected. This aids in maintaining properly functioning devices by protecting them from attacks, such as malware, which can hinder functionality. Cyber hygiene relates to the practices and precaution users take with the aim of keeping sensitive data organized, safe, and secure from theft and attacks.

Cyber hygiene can be defined as a reference to the practices and steps that users of computers and other devices take to maintain system health and improve online security. These practices are often parts of day to day activities to ensure the safety of identities and other details that could be stolen or corrupted. Much like physical hygiene, cyber hygiene is regularly conducted to ward off natural deterioration and common threats (Brook, 2018).

Symantec Corporation (2019) defines that cyber hygiene is about training ourselves to think proactively about our cybersecurity, as we do with our daily personal hygiene to resist cyber threats and online security issues. Cisco (2018) also defined as it is essentially a set of practices that help manage the most common and pervasive cybersecurity risks faced by organizations today. Real-world breaches and security incidents prove over and over again that most widespread issues still stem from a lack of basic cyber hygiene (Tripwire Inc., 2018).

2.4.1. Cyber Hygiene Benefits

Whenever having a routine of cyber hygiene procedure in the place for the computer hardware or software is beneficial for two distinct reasons; maintenance and security. Maintenance is necessary for computers and software to run at peak efficiency. Files become fragmented whereas programs become outdated, in increasing the risk of vulnerabilities. Routines that include maintenance are likely to spot many of these issues early and prevent serious issues from occurring. A system that is well-maintained is less likely to be vulnerable to cybersecurity risks.

Security is perhaps the most important reason to incorporate a cyber hygiene routine. Hackers, identity thieves, advanced viruses, and intelligent malware are all part of the hostile threat

landscape. While predicting threats can be challenging, preparing and preventing them to become feasible with sound cyber hygiene practices (Brook, 2018).

2.4.2. Common Cyber Hygiene Problems

Enterprises often have multiple elements in need of cyber hygiene. All hardware (computers, phones, and connected devices) and software programs and online applications should be included in a regular ongoing maintenance program. Each of these systems has specific vulnerabilities that can lead to different problems. Some of these problems include the following (Brook, 2018).

- ✓ **Loss of Data**: Hard drives and online cloud storage that isn't backed up or maintained is vulnerable to hack, corruption, and other problems that could result in the loss of information.
- ✓ **Misplaced Data**: Poor cyber hygiene could mean losing data in other ways. The information may not be corrupted or gone for good, but with so many places to store data. Misplacing file is becoming increasingly common place in the modern enterprise.
- ✓ **Security Breach:** There are constant and immediate threats to all enterprise data. Phishing, hackers, malware, spam, viruses, and a variety of other threats exist in the modern threat landscape, which is constantly in a state of flux.
- ✓ **Out of Date Software:** Software applications should be updated regularly, ensuring that the latest security patches and most current versions are in use across the organization for all applications. Out of date software is more vulnerable to attack and malware.
- ✓ **Older Security Software:** Antivirus software and other security software must be updated continuously to keep with the ever-changing threat landscape. Outdated security software that has gone a few months without an update can't protect the enterprise against the latest threats.

2.4.3. Best Practices: A Cyber Hygiene Checklist

While there are numerous threats and multiple vulnerabilities with each piece of the digital puzzle, creating a cyber hygiene routine isn't as difficult as it may seem. A few key practices implemented regularly can dramatically improve the security of any system (Brook, 2018).

2.4.3.1. Document All Current Equipment and Programs

All hardware, software, and online applications will need to be documented. Start by creating a list of these three components (Brook, 2018):

Hardware: Computers, connected devices (i.e. printers, fax machines), and mobile devices (i.e. smartphones, tablets).

Software: All programs, used by everyone on a particular network, that are installed directly onto computers.

Applications: Web apps (i.e. Dropbox, Google Drive) applications on phones, tablets and any other program that isn't directly installed on devices.

2.4.3.2. Analyze the List of Equipment and Programs

After creating a comprehensive list of all cyber facing components can begin to scrutinize that list and find vulnerabilities. Unused equipment should be wiped and disposed of properly. Software and applications that are not current should be updated and all user passwords should be changed. If the programs aren't in regular use, they should be properly uninstalled. Certain software programs and applications should be chosen to be a dedicated choice for certain functions for all users. For instance, if both Google Drive and Dropbox are being used for file storage, one should be deemed primary and the other used as a backup or deleted (Brook, 2018).

2.4.3.3. Create a Common Cyber Hygiene Policy

The newly clarified network of devices and programs will need a common set of practices to maintain cyber hygiene. If there are multiple users, these practices should be documented into a set policy to be followed by all who have access to the network.

Here are a number of typical items that should be included in a cyber hygiene policy (Brook, 2018; Symantec corporation, 2019).

- **Password Changes**: Setting complex, unique and strong password for all of the devices regularly can prevent many malicious activities and protect cybersecurity.
- **Software Updates**: Updating the software or perhaps getting better versions should be a part of the regular hygienic review, update the applications, web browsers, and operating systems regularly to ensure it is working with the latest programs that have eliminated or patched possible glitches. Setting up this feature to update automatically will help and ensure to have the latest protections.
- **Install reputable antivirus and malware software:** The first and maybe the most important step is installing antivirus software. What is it designed to do? Antivirus software is a program or umbrella of programs that scan for and eradicate computer viruses. And other malicious software or malware it's a vital component of overall cyber hygiene in its protection against security breaches, along with other threats.
- **Hardware Updates:** Older computers and smartphones may need to be updated to maintain performance and prevent security issues.
- **Manage New Installs:** Every new install should be done properly and documented to keep an updated inventory of all hardware and software.
- **Limit Users:** Only those who need administrator-level access to programs should have access. Other users should have limited capabilities.
- **Backup Data**: All important data should be backed up to a secondary source offline on an external hard drive, or in the cloud (i.e. hard drive, cloud storage) regularly. This will ensure its safety in the event of a breach, malfunction or it can protect against many types of data loss, especially if hackers gain access to one of the devices.

- **Employ a Cybersecurity Framework**: Businesses may want to review and implement a more advanced system (e.g. the NIST framework) to ensure security.

Once the policy is created, the routine for each item should be set to appropriate timeframes. For instance, changing passwords every 30 days or check for updates at least once per week could be set in place. Doing so, it will ensure the continued cyber hygiene of your entire network of hardware and software.

Developing comprehensive cyber hygiene procedure is a must for today's enterprises. When carried out in conjunction with robust, enterprise-wide security practices, sound cyber hygiene practices aid in maintaining a sound security posture for modern organizations (Brook, 2018; Symantec corporation, 2019).

2.4.4. Cyber Hygiene in Financial Institutions

Financial institutions are organizations that conduct financial transactions such as investments, loans or deposits. There exist various types of financial service firms, including banks, insurance companies, asset management boutiques, credit card companies, consumer finance enterprises, stock brokerages, investment funds, and government-sponsored entities (Parmvir, 2015).

Rajendran (2018) states that the bank should protect, not only its physical asset, but also its information asset. Today's banking is associated with electronic delivery channels like ATMs, Mobile, PoS (Point of Sale) terminals and online modes than with any physical human being. All these electronic delivery channels produce a huge amount of financial information asset. Nowadays, criminals do not rob banks with guns or attack the employees with weapons but they attack with more sophisticated weapons in their arsenal by using a keyboard, mouse, software program and network algorithms. As it is a global phenomenon, the more the banks are prepared to counter the attacks, the more cybercriminals equipped themselves with the latest technology, thus they ensure that the banks always keep running to learn, to equip and to protect their assets.

Due to these highly sensitive financial information assets, financial institutions become a primary target for cyber-attacks; Websense (2015) security labs discussed that financial service firms are

under constant barrage by cybercriminals and on average financial service businesses are attacked 300% more than other institutions.

The targeted intrusion into a bank's systems is often perceived as the greatest threat due to the malicious actor's ability to not only steal data but modify or delete it. By exploiting software, hardware or human vulnerabilities hackers can gain administrative control of networks, if abused, could cause catastrophic consequences. If publicized, network security breaches can affect share prices, cause irreparable reputational damage and impact on the stability of the wider financial market (Horne, 2014).

As the banks moved from branch banking to anywhere 24x7 banking, they were required to expose a segment of their network to the customers accessing their web-based, mobile-based applications like that of internet banking and mobile banking. Cyber adversaries are exploiting the vulnerabilities in the network, servers to commit frauds, data theft and business disruption, etc (Babu, 2018). Some of the common threats faced by the financial institutions mostly banks are Malware, ransom ware, phishing, spear-phishing or whaling, SQL injection attack, cross-site scripting, DoS, social engineering, website defacement, etc. To overcome these threats the banks required to create an internal culture of cyber vigilance. And the most important thing is to make it real so that employees understand that they are part of the equation (Guire, 2017).

2.5. Insider Threat

Historically, information security efforts of financial service firms have centered on defending external borders from intrusion by nefarious outsiders. More recently, security debates have broadened to include trusted employees, contractors, and business partners. Financial service institutions have grown increasingly aware of the changing threat landscape and the debilitating effects of insider attacks on the confidentiality, integrity, and availability of financial data systems. Udeh & Dhillon (2008) argue that external security risks have received considerable attention in the banking industry. However, insider attacks are yet another threat which is exhibiting increasing severity, frequency, and complexity (David, 2011; Mark and Hardy, 2014).

Insider threats are considered to attack which emerged due to an act committed by the staff member who is employed in the specific operation area. These can often be carried out by dissatisfied personnel who disobey to the organization policy and procedure (Griffiths, 2016).

Insiders are defined as current or former employees, contractors, or business partners who had authorized access to an organization's network, system, or data. Having exceeded or used that access, intentionally or unintentionally in a manner adversely affected the confidentiality, integrity, or availability of the organization's network, system, or data (George et. al, 2012).

Known person (insider) can cause severe damage to the system and loss to the organization. The securing of information against insider attacks and proper control on the sharing of information by insiders to unauthorized insiders and outsiders is very important. Moreover, confidential data has to be encrypted even flowing inside the organization and proper locking of internal networks is also necessary (Fernando and Yukawa, 2014).

Financial service firms in particular have been frequent targets of insider attacks. While insider threat awareness levels have increased over the years. Insider threat management practices remain to be better understood. Little is known about the spectrum of measures taken by financial service firms in response to insider attacks (Eggenschwiler et.al., 2016).

An investigation by Cisco (2018) highlights the risk from January to June 2017. They examined data exfiltration trends using machine learning to profile 150,000 users in 34 countries who were using the cloud. Over 1.5 months, researchers found that 0.5% (750) of users made suspicious downloads. Put another way, this means two employees at a 400 person firm would be insider threats. That is 100% too high. Specifically, those users downloaded, in total, more than 3.9 million documents from corporate cloud systems. That's an average of 5,200 documents per user during a 1.5 month or within 45 days period.

Similarly, Schulze (2016) reported that seventy-four percent of organizations feel vulnerable to insider threats, a dramatic seven percentage point increase over the 2015's survey. However, less than half of all organizations (42%) have the appropriate controls in place to prevent an insider attack. Privileged users such as managers with access to sensitive information, pose the biggest

insider threat to organizations (60%). This is followed by contractors and consultants (57%) and regular employees (51%), in the same way, the Africa cybersecurity report (2017) highlighted that insider threats were the top from the list since it comes to high risks among the numerous cases reported by the year 2017. It's clear that the group most implicated was administrators and other privileged users, who were in the best position to carry out a malicious breach, and whose mistakes or negligence could have the most severe effects to the organization. The key contributors to the success of these attacks were inadequate data protection strategies or solutions and a lack of privilege account monitoring. As a result, top insider threats are administrator accounts, privileged users' accounts, and contractors, consultants and temporary workers (Serianu, 2017).

2.5.1. Insider Cybersecurity Behavior

Digital transformation drives efficiency and scale for existing products and services, while making possible new business models that drive growth and profitability. Enterprises are embracing the opportunity by leveraging all digital technology offers but can leave the security of their sensitive data at risk in the rush to deployment.

Thales (2018) report found that the overall adoption of cloud, big data, IoT (Internet of Things), containers, mobile payments and blockchain technologies by enterprises was at record levels to drive this transformation. With some technologies (like big data) reaching 99% adoption, and with 94% planning to use sensitive data within these environments, the scale of adoption makes this problem hyper-critical, as organizations are now using many vendors and environments.

Researchers approved that cyber fraud is being abetted by the staff of organizations working together with hackers who steal password and other important information to help them commit crimes (The East African, 2016).

The 2018 Thales Data threat report quantifies organizations are dealing with massive change as a result of the latest round of digital transformation. As digital transformation inherently drives organizations into a data-driven world, 94% of organizations are using sensitive data in the cloud, big data, IoT, containers or mobile environments; this is creating new attack surfaces and new risks

for data that need to be offset by data security controls. Digital transformation requires new data security approaches organizations need to change how they protect their data.

2.6. Cybersecurity Global Perspective

Globally, the focus has now shifted to cybersecurity, it is no longer an isolated incident affecting one industry or one country. Several cyber-attacks in recent times have been designed to achieve political as well as religious objectives for securing funds for promoting terrorism. This has assumed frightening dimensions as it has an important bearing on financial stability. The importance accorded to the issue can be gauged from the fact that global standard-setting bodies, as well as reputed central banks, have been committing extremely large resources to address this threat (Mundra, 2016).

On the afternoon of Friday 12th May 2017, there were widespread reports of organizations succumbing to the WannaCry classified as ransomware as this malicious code spread quickly like wildfire through the internet around the world. The WannaCry malware attack infected more than 300,000 computers over 150 countries worldwide in less than 24 hours, attacking a total of more than 2 million computers all over the world (Falanx, 2017; Strauss, 2017).

Figure 3: WannaCry worldwide attack map (source: (Serianu, 2017))

Ethiopia Information Network Security Agency (INSA) disclosed that a number of Ethiopian institutions were affected by a global cyber-attack of WannaCry. The nation is one of the 11 African countries targeted by the cyber-attack. The state-run Telecom Company, industries, and hospitals were few among others affected by the computer virus. However, it wasn't revealed the levels of damage caused to the institutions by the cyber-attack, the attack particularly affected institutions that use Windows operating systems and advised on those institutions to update it to avert dangers of cyber threats which are considered to continue. INSA also warned the organizations, not to open email messages sent from an unknown address (Sudan Tribune, 2017).

WannaCry does not only attack businesses, but also automatic teller machines (ATM), point-of-sale terminals, nuclear power plant and hospitals around the globe where it leads to the losses of hundreds of millions of dollars. While a large number of computer security teams were struggling to patch their systems, came to another global attack spreading the ransomware known as NewPetya or NotPetya arrived on June 2017, which behaves similarly to WannaCry (H1, 2017).

Petya infects unpatched Windows devices by exploiting vulnerability in the Server Message Block (SMB) server. This ransomware encrypts the Master File Tree (MFT) tables for the New Technology File System (NTFS) partitions and overrides the Master Boot Record (MBR) of infected Windows computers making the affected machines unusable (H1, 2017).

And yet the ransomware effectiveness was relating to display intimidating messages that will induce a victim not to ask for help. It was done in such a way that a victim was meant to believe the only option they have was to pay the ransom in order to disinfect the system. The authors of Ransomware tend to be instilled fear and panic into their victims causing them to click on a link or pay a ransom. And users system can become infected with malware. Social engineering concepts were also used in some cases to convince a target to succumb to a ransomware attack (Serianu, 2017).

According to the East African magazine, African countries lost at least $2 billion in cyber-attacks in the year 2016. Only East Africa, Kenya lonely lost higher than $171 million which is robbed by cybercriminals. Similarly Tanzania followed with $85 million while Ugandan companies lost $35

million (The East African, 2016). Ransomware attack is expected to cost businesses and organizations $11.5 billion in 2019 (Thebestvpn, 2019).

2.6.1. Recent Cyber Incident Reports and it's Economic Impact

According to Cisco (2018), annual cybersecurity report which was combined by survey from different sectors, there were three trends that were in an attempt to weaponry technology to damage government services and infrastructures.

1. **Taking about malware to unprecedented levels of sophistication and impact**

The advent of network-based ransomware crypto worms was eliminating the need for the human element in launching ransomware campaigns. And for some adversaries, the prize wasn't ransom, but the obliteration of systems and data. According to Cisco threat researchers, self-propagating malware was dangerous and has the potential to take down the internet.

2. **Increasing evasion and weaponzing cloud and other technologies**

Actors are embracing encryption to evade detection and adopting techniques that rely on legitimate internet services like Google, Dropbox, and GitHub. The practice makes malware traffic almost impossible to identify. Many attackers are now launching multiple campaigns from a single domain and reusing infrastructure resources, such as registrant email addresses, autonomous system numbers (ASNs), and name servers to get the best return on their investments.

3. **Exploiting undefended gaps in security for IoT and cloud services**

Unpatched and unmonitored IoT devices and cloud environments are giving attackers opportunities to infiltrate networks. IoT botnets are growing and becoming automated for advanced distributed denial-of-service (DDoS) attacks. And organizations are susceptible to attack seem unmotivated to fix the problem in a timely manner. Worse yet, such groups probably have more vulnerable IoT devices than they realize (Cisco, 2018).

Cyber incidents were increasingly shifting towards targeting financial institutions instead of end-users. In August 2, 2016, Bitfinex, a Hong Kong exchange for the trading of digital currencies, announced that some of its customer accounts were hacked and bitcoins were stolen. The value of the stolen bitcoins had been reported to be approximately US$65 million or more. As a consequence, the value of bitcoins came down and the trust of the digital currency shaken.

At the beginning of the year 2016, Bangladesh Bank was the target and an attempt was made to be stolen US$1 billion and ultimately the attackers could successfully get away with US$81 million. By the same year 2016 in India, a similar attempt was made on a commercial bank by generating fraudulent payment instructions on the Nostro accounts and transmitting them over the SWIFT messaging system. Though monetary loss could be prevented with proactive follow up with the concerned paying or intermediary banks, the incident has reinforced the fact that the various stakeholders had not learned the lessons yet (Mundra, 2016).

WannaCry earned more than US$143,000 through bitcoin payments at the point the wallets were cashed out. Cisco threat researchers estimate that roughly 312 ransom payments were made. Unfortunately, WannaCry did not track encrypted damage to the payments made by affecting users. So the number of users who received decryption keys after making a payment was unknown (Cisco, 2018).

2.7. Information Security

Information security refers to protecting or safeguarding any kind of sensitive information and information systems from unauthorized access, disclosure, modification, disruption and destruction (ISO/IEC 27001:2009, 2009). For most organizations information is a critical resource to be secured. If sensitive information falls into wrong hands then the respective organization may face a great deal. According to KragBrotby (2009), a major focus of information security had been the protection of the IT systems that process and store the vast majority of information, rather than the information itself.

According to Paul (2004), information security provides the management processes, technology and assurance to allow business management to ensure business transactions can be trusted and

ensured IT services are usable and can appropriately resist and recover from failures due to error deliberate attacks or disaster and ensure critical confidential information withheld from those who should not have access to it (COBIT, 2004).

Information security is concerned with implementing adequate controls to protect information assets. These controls must be aligned with the organization's security objectives and should minimize the risks to which the organization is exposed (ISO/IEC 17799 (BS 7799-1), 2005). Controls cover a wide spectrum of technology such as firewalls, processes, change management, and human elements such as information security induction training (Veiga, 2008).

Information intended for internal use only is usually meant to be seen by employees, contractors, and service providers, but not by the general public. Companies may have confidential information, such as researches and development plans, manufacturing processes, strategic corporate information, product roadmaps, process descriptions, customer lists, and contact information, financial forecasts. And earnings announcements, which are intended for internal use needs know basis. Loss or theft of confidential information could violate the privacy of individuals, reduce the company's competitive advantage, or cause damage to the company. This type of information is available to external audiences only for business-related purposes and only after entering a nondisclosure agreement or equivalent obligation of confidentiality (Ousley, 2013).

Cybersecurity depends on an employee's attitude. According to the Oxford English Dictionary (2019) attitude is defined as a feeling or opinion about something or someone, or a way of behaving. Martins and Eloff (2006) underlined that, the behavior of employees and their interaction with computer systems have a significant impact on the security of information. Training or coaching can play a big role to make sure that employees understand security is very important.

On the other hand, in order to aware employee concerning the essentiality and necessity of organizational security, coaching is important to know the threat and vulnerable areas. This can benefit both the employee and the organization as it is a good idea, and applies pleasantly by the staff members, whereas, as per the Oxford English Dictionary (2019) definition good idea is

defined as a wise suggestion. Necessary is defined as the need to be done or essential to the practice, beneficiary defined as derives advantage from something. And pleasant defined as a person or their manner.

Straub and Welke (1998) mention to the importance of raising security awareness through education and training programs, in order to progress toward the development of information systems security through risk analysis, countermeasures, and security implementation, training programs spread through sensitive business areas which utilize information security such as financial industry.

The Symantec report (2012) acknowledges that the financial industry has a superior level of technical controls but emphasizes that any effective treatment of risks must take a holistic (systems) approach since an increasing number of attacks are aimed at people both employees and customers. Unfortunately, most researches have focused on technology. And more work is required on the socio-technical aspects of information security. A bank which fails to protect its information systems not only loses its competitive advantage and repute but also threatens its existence (Hagen et.al., 2008; Von Solms et. al., 2011).

Historically, a bank's primary security concern centered on protecting physical data assets such as posted ledger cards, promissory notes, and critical documents in the vault as well as securing the perimeter of the bank premises. In today's banking environment, business functions and technologies are increasingly interconnected, requiring financial institutions to secure a greater number of access points. Raytheon (2015) concludes that a cyber-crisis at one or more banks could result in financial catastrophe, not only to customers and banks but to a country's financial system as a whole (Benardo, 2015; Websense, 2015).

Information security and data protection have become important concerns and challenges facing the banking industry and users since the banking industry have very sensitive data. Information security researchers have recently emphasized that management's attention is required to secure information resources to design effective security policies and to enhance users' security awareness to comply with information security policies (Siponen, 2007).

Ula et al. (2011) identified the following threats: physical destruction of premises and systems by natural disasters; unintentional damage due to human error, abuse of system and sensitive information by employees or agents of the bank, systematic collection of sensitive information by foreign intelligence services; and external attacks which compromise confidentiality, integrity and availability of information.

Even big banks that generally do a better job of security are found to be victims of security breaches (Woretaw & Lessa, 2012). Ultimately, the success of a bank can depend on its ability to manage its information security and provide secure services. And it is hardly surprising, therefore, that 80% of leaders in the financial services sector cite cyber risks as a top concern (Ula et. al., 2011; Travelers, 2015).

The threats that banks face are amplified by customers' expectations. Customers want to interact easily, yet securely with their bank in real-time through an increasing range of mobile services. The expansion of these services increased the attack surface and consequent security threats, the number, and complexity of attacks. And the resultant losses are increasing rapidly. Many losses are not caused by a lack of technology or faulty technology rather by users of technology and faulty human behavior. A security breach resulted from malicious behavior by an employee incurring a cost of $7 billion (Udeh & Dhillon, 2008; Woretaw & Lessa, 2012).

In 2015, Kaspersky revealed cyber attackers targeted up to 100 banks, e-payment systems, and other financial institutions in around 30 countries stealing $1bn within two years. Online banking fraud increased from £40.9 million to £60.4 million in the UK in 2014, a 48% rise and another major contributor was the recent increase in telephone-based deception crimes (FFA, 2015).

2.7.1. Organizational Information Security Culture

There are many ways of building, changing and maintaining the organizational culture. These are processes and methods to apply when it wants to build and manage culture. Every organization is unique and comes with its own culture and subcultures. Researchers agree that establishing and socializing organizational culture and norms is essential for employees' adaptation to attempt that

reinforce controls using informal communication and security awareness among social agents (Funkhouser & Ritti, 2014; Roer, 2015).

According to the Oxford English Dictionary (2019), culture is the ideas, customs and social behaviors of a particular people or group and security is the state of being free from danger or threat. Combining these two definitions we can get that security culture is the ideas, customs and social behaviors of a particular people or group that helps them be free from threat and danger.

Culture is not one thing only; it is the accumulation of many groups of people. The sales department, the accounting department, the IT department, the developers, the builders, testers and so on (Roer, 2015). Each of these departments has its own more or less distinct culture ideas, customs and social behaviors that belong to that particular department. Together, these subcultures form the company culture (Martins and Eloff, 2006).

Shamal and Ivan (2009) define security culture as a combination of tangible factors and intangible factors within both an organization's culture and its subcultures. Intangible factors are invisible assumptions, norms, and values of a culture's participants. Tangible factors are visible artifacts of a culture or subculture. These artifacts are represented by technical controls, procedural controls or socio-technical measures. Technical controls represent the mechanisms controlling security. These include passwords and digital certificates. Procedural controls are organizational policies and procedures reflecting the presence of security. These include security policies, instructions for using technical controls, and guidelines for secure data handling. Socio-technical measures augment both technical and procedural controls and are designed to increase the potency of intangible factors. Examples of these measures include security awareness programs and guidelines for ethical conduct.

Security culture is a set of customs shared by a community whose members may be targeted by government design to minimize risk. Having a security culture in place has a great contribution to create a safe environment for everyone in trouble to work out towards safety measures. Culture is unconscious, instinctive and effortless; once the safest possible behavior has become habitual for everyone in the team and; can spend less time and energy the need for it. Security equipment and

policy is a tool but security culture is a key to solve security problems. Employees' information security attitude can set an organization security culture. Building security culture requires a lot more than just information security competence. Technology and policies are a part of security culture, like people and competence (Roer, 2015).

Similarly, Veiga (2008) defined information security as the attitudes, assumptions, beliefs, values, and knowledge that employees or stakeholders use to interact with the organizational systems and procedures at any point in time. The interaction results in acceptable or unacceptable behavior (i.e. incidents) evident in artifacts and creations that become part of the way things are done in an organization to protect its information assets. This information security culture changes over time.

Martins and Eloff (2006) define information security culture as the assumption about acceptable information security behavior and it can be regarded as a set of information security characteristics such as confidentiality, integrity, and availability of information. The systematic review of Karlsson et al. (2015) summarized the consensus definition as a shared pattern of values, mental models and activities that are traded among an organization's employees overtime, affecting information security.

According to Information Security Forum (2000); information security culture refers to the shared values ('what is important') and beliefs (about 'how things work') that people in the organization have about information security. It interacts with the organization's systems and procedures to influence behavior ('the way we do things around here').

Hirschheim & Newman (1991) stated that many authors describe security culture as a mentally perceived concept, such as security awareness or obedient behavior, but we believe that definition fails to explain a larger picture. Like other writers on security culture, we take inspiration from Schein (2012) and his layered model of organizational culture, but we also consider the work of those who consider culture as an ordered system of symbols where meaning is based on individual participants, rather than the organization as a whole.

Awareness alone is insufficient to create a positive security culture (one where each member is helping each other to do the right thing. According to ISACA (2010), the most effective changes

in the perception of information security tend to happen when a board-level senior manager assumes responsibility for security and reshapes the organizational culture (ISACA, 2011).

Martins and Eloff (2002) stated that an information security culture emerges from the assumption about what characteristics and behaviors are encouraged to be acceptable, and it results in the manner people behave with regard to information security in the organization (Veiga, 2008).

Veiga (2008) stated that a person's perceptions of an issue can change from year to year as he/she is exposed to situations and gains life experience. In the same way, employees who have worked in an organization for a long period could be more positive about the protection of information assets and perceive it in a different manner, compared to employees who have worked for the organization for less than a year.

2.7.2. Organizational Asset

The ISO17799 (2005) defines an asset as anything that adds value to the organization. This would include information, for example contracts, training material and strategies; software such as system software and utilities; physical assets such as computer equipment; services like communication services and other utilities such as power and lighting; people with their skills and experiences, and lastly, intangible assets such as the image and reputation of the organization. For the purpose of defining an information security culture, the focus is on information, people and intangible assets.

2.7.3. Information System Security Policy (ISSP)

During the last decade, banks started to implement preventive controls such as information security policies (ISP), which introduce a binding standard concerning IS behaviors among all users, to reduce IS-related loss incidents (Bauer S. et. al., 2017)

Information security involves technology, processes, and people. Roer (2015) stated information security policy created based on how people used the technology; the policy was initiated by technology. The process of developing an effective information security policy is straight forward

which is shaped by threats to an information system. The information systems security policy defines the objectives of the information system of an organization and outlines a strategy to achieve these stated objectives (Tessem & Skaraas, 2005; SANS, 2009).

Information systems security policy (ISSP) supports appropriate behavior among employees by providing clear instruction of responsibilities to follow terms and conditions of such policies and it should be distributed to every employee, whenever accomplishing their day to day task all employees should be the same page of understanding on the organization policy, procedure and guideline (Siponen, 2007).

Rajendran (2018) states that the alignment of technology and its law or policy hugely impact the security of the bank, and how the same technology can be used, misused or abused to make the activity absolutely lawful or unlawful.

Information security policy forms the foundation of the information security program. All the initiatives on the IT front will draw support from this policy and will also extend their support. The security procedures will have to be integrated with the existing and/or future procedures for managing information assets. The banks will issue guidelines, whenever necessary, to add the technology specifics to the procedures.

The security policy framework is necessary to establish, implement, operate, monitor, review, maintain and improve security and related risks at the bank. Figure 4 shows components of the ISSP framework that were suggested by United Bank of India (2015).

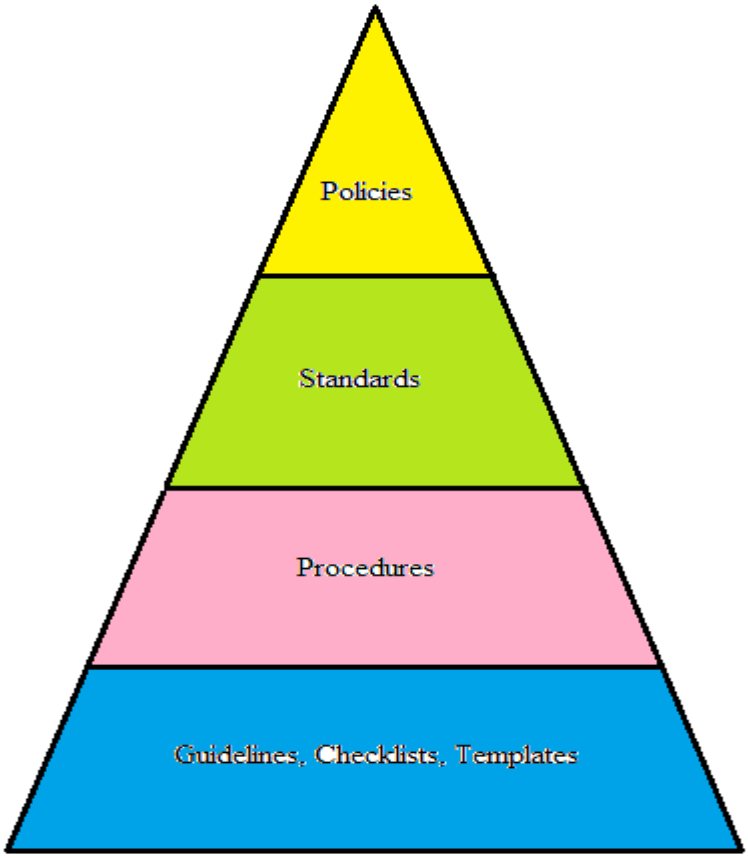

Figure 4: Security policy framework (Source: *(Union Bank of India, 2015)*)

Policies

Policies shall include a commitment from senior management of the organization to meet various compliance, regulatory requirements, the objective, goals, and principles of the bank. It is a high-level statement of requirements which aims to provide management direction and support for information security, including laws and regulations. It supports appropriate behavior among employees by providing clear instruction of responsibilities to follow terms and conditions.

Standards

Standards shall be introduced as an applicable base on the information security policies to establish the baseline or the benchmark for the technical or operational procedures against which the compliance could be measured uniformly. Standards specifies how to configure devices, how to

install and configure software, and how to use computer systems and other organizational assets, to be compliant with the intentions of the policy

Procedures

Procedures derived to meet the objectives of the policies stated in the information security policy. Procedures shall describe what to do, who is responsible and how to execute the step-by-step instructions to perform various tasks in accordance with policies and standard and the corresponding work product of each activity.

Guideline, Templates, and Checklists

Guidelines are suggestions, not rules for carrying out the activities stated in the procedures and advised about how to achieve the goals of the security policy. They are important communication tool to let people know how to follow the policy guidance, it conveys best practices for using technology systems or behaving according to management's preferences. Templates shall be used to document the execution of the activities. Checklists are triggers to ensure that the activities in the procedures are effectively carried out (Veiga, 2008; Ousley, 2013; Union Bank of India, 2015; Alqahtani, 2017).

2.7.4. Ethiopian Cybercrime Rule

Ethiopia introduced the first set of cybercrime rules with the enactment of the criminal code in 2004. The Code criminalizes a set of three cybercrimes namely hacking, dissemination of malware and denial of service attacks (DoS). Several cybercrimes have been perpetrated against the Ethiopian cyberspace since the enactment of the computer crimes rules, but there were only a few reported court cases (Ethiopia, 2004; k. Yilma, 2014).

In 2013, Ethiopia’s cyber command INSA released a draft comprehensive cybercrime legislation that not only extended the range of outlawed cybercrimes but also introduced crucial evidentiary and procedural rules for the investigation and prosecution of cybercrimes. By 2016, after three years of hiatus and new drafting (or redrafting) the second version of the rule had been adopted.

The newly enacted cybercrime law had some changes to the initial versions of the law. It seems to have sacrificed precision for the sake of ensuring clarity by framing provisions in an excessively detailed manner (Ethiopian Ministry of Justice, 2016).

2.7.5. Security Awareness Program

Organizations implement firewalls, comprehensive cybersecurity defense systems, and sophisticated IT protocols to keep themselves safe from online threats. Without an embedded culture of cybersecurity awareness and enforcement, all of those fancy and expensive systems aren't going to do much better. The human aspect of cybersecurity plays a vital role. Researchers have also commented on the fact that most humans is the weakest chain part of the cybersecurity (L. Hadlington, 2018; FraudWatch International, 2019).

Similarly, employees are the first and primary line of defense against online crime. Setup security awareness program helps to change bahavior and nurture a security culture which can strenghth the human element of security risk. Identify specific types of users role who need to have training, in addition to receive required training, may require a special version of training, delivery method, or specific topics.

Once the user privilage role is identified then after the specific training topic which should be related to the organizational culture and role. Focus on a small number of topics and behaviors that represent the greatest risk to the organization. The training included training topics such as security policy, data classification, acceptable use policy, phishing, social engineering, Ransomware, password management,online security, incident management and how to report it.

If users are not willing or are not motivated to change behaviors, the training program will fail. The first step is to engage the audience. The engagment can be in two ways these are, organiational and personal.

Company culture should be considered whenever the engament is in organizational context, or develop a plan and approach in conjunction with senior management and corporate communications that reflects a top down, full support of the security awareness program initiatives

and goals. Work directly with senior leadership & corporate communications to identify opportunities to strengthen the support for security awareness and secure behaviors and habits.

Personal engagement emphasizing that people have lives outside of work and are also subjected to the same types of risks is a great way to engage users. The intent will be to empower users with the ability to make smart, security-driven decisions in their personal lives that nurture secure habits; along with the tools and resources to maintain secure behaviors at work. Giving them ways to protect their family is always big win.

The training conducted annually or semiannually, or using other schedule could be used depending on the business security impact or prioritizing the organization business plan. Parallel to the training, awareness initiatives supportive strategy to develop the security culture of the organization like security ambassador group of volunteer employee, newsletters within every week or month. Metrics are one of the evaluation mechanisms to the awareness program of the training strategy, simulation is one of the metrics to measure the program (FraudWatch International, 2019; Habitu8, 2019).

2.8. Related Works

Griffiths (2016) carried out a study on "Cyber Security as an Emerging Challenge to South African National Security" at South Africa Pretoria University. Qualitative research approach with exploratory study and used two combined research method; the first one was desk research, the primary source includes policy documents such as national development plan, speech by government ministers, the defense review, and cybersecurity bill; the second method was an analytical and descriptive research approach which explore most publicly destructive cyber-attacks that had taken place globally and also explore most public cyber-attacks that had targeted South African directly. The finding was the country produced cyber policy framework to guide the creation of more focused legislation but there remains a lack of engagement and discourse on the importance of cybersecurity to national security.

The 2030 national development plan fails to articulate any clear strategy with regard to cybersecurity that shows that the country didn't prioritize the cybersecurity. This is because of the

fact that, the government underestimated the impact of cyber-attack to the country. There was a definite need for the capacity building with the public domain particularly focus on technical skills such as cyber forensics, cryptography, information security, and other cyber-related disciplines. One of the challenges facing the country was lack of proper cyber investigations take place because the South African Police Service (SAPS) don't have the necessary skills and it needs to be supported by training. The same is true in the military and state intelligence. Another problem facing the country was lack of information sharing with regard to cyber-attacks. The government needs to proactively engage with companies like banks and financial institutions. The country should also develop cyber-security partnerships outside of the border to strengthen the country's cybersecurity position.

The researcher concluded that the country faced numerous cyber-attacks in the past and may continue in the future. The country lacks urgency and prioritization to the cyber-security which can affect the national security.

Woretaw and Lessa (2012) conduct their research on the title "Information Security Culture in the Banking Sector in Ethiopia". The research objective was to identify the key gap and establish effective information security culture and fill its gap regarding researching in Ethiopia banking sector. A questionnaire survey research method was employed to assess the information security culture and auditing process used to find out its level in the banking sector in Ethiopia. Primary data were collected from the headquarters of 11 banks; 4 governmental and 7 private. IT or IS departments were the main participants of the survey. A non-probability convenience snowball sampling technique is used to collect data from all the banks. Their finding dimensional frequency analysis shows holistic and strategic work that was needed to promote information security culture in the banking sector in Ethiopia. They concluded that unsatisfactory security awareness existed in the banking sector, the security level of governance was a critical area of improvement, a space to enhance the trust between managers and employees that can promote change in security culture; and the findings advocate the need for effective information security awareness, trust environment, and communication to promote sustainable change in information security culture which enables proper information security governance and implementation that complies with local and international standards.

Woretaw and Lessa (2012) recommended that banks should invest in the effective information security communication methods such as training employees with information security measures and prepared information security awareness programs. International information security governance standards ISO27002 and information security management standards ISO27001 should be implemented. And factors that influence information security culture and practices were organizational cultures, top management support, information security risk analysis, information security policy, information security management standardization, information security awareness, and training programs information security compliance.

Ayalew (2016) conducted a study on the title "Assessment of Information Security Culture in the Banking Industry: The Case Study of Development Bank of Ethiopia". As the title indicates the research takes place at Development Bank of Ethiopia of all employees who used the T-24 Core banking system and the research used quantitative research method. Assessment instrument questionnaire was adopted from previous studies to assess the information security. A stratified sampling technique was used to select respondents. The result shows that there was a positive aspect about the information security culture in the bank in which the bank can scale up its effort for a more conducive information security culture for the protection of its information assets; on the other hand, a huge gap with respect to information security culture in the Bank was found. The major finding of the study was lack of a written and formal information security policy, guideline and procedure. The conclusion was the overall information security culture of the bank was not conducive for the protection of information assets. The bank's security management was weak and not trusted; and the researcher recommended that the bank should implement a comprehensive and adequate set of information security components. It should compile and implement a formal well-defined information security policy and its derivatives, executive management of the bank should organize information security department at a higher possible level in the organization, continuous information security culture development parallel with change in the business environment should be carried out in the bank.

Jowi & Abade (2016) conduct their study on 43 Kenyan banks with the title "Evaluation of Information Security Risk Assessment for Internet Banking among Commercial Banks in Kenya". All 43 banks were selected for the target population and the study targeted four major departments

namely; security department, operation department, audit department, and risk management department. Quantitative analysis approach was used for the primary data source. They used questionnaires; it was coded using the Statistical Package for Social Sciences (SPSS version 20) to find descriptive analysis.

The findings of the study show that most of the employees who work in the bank industry have the required skills and knowledge to perform the task associated with risk management of the e-banking. The majority of the respondents have been working in bank sector for a period between 6-8 years. The findings indicate that the failure of technology and the failure of segregated duties were rated highest in influencing bank high-risk management issues in e-banking in Kenya. This is due to failure of policies and procedures, lack of training, experience, internal audit, as well as lack of supervision.

The findings indicate that adherence to policy and procedures would reduce high-risk management issues in e-banking, internal audit, the segregation of duties, staff training and risk management solutions would reduce high-risk management issues in e-banking. In addition, the study found out that internal factors can affect e-banking to a high extent. This means internal factors do affect e-banking services if not managed. Banking management has to take an initiative to control them.

Regarding responsibility for the oversight role over risk management processes, the findings indicate that senior management has the biggest oversight role over the risk management process rest with senior management. In addition, the oversight role over the risk management process rests with senior management. On whether banks have different types of how they audit their services to reveal any issue in their systems. The findings indicate that most banks carry out an internal audit. Log review, core bank software, firewalls, IDS (Intrusion Detection System) and routine checks were mostly used by banks to monitor and manage risk, but the result shows that most common risk monitoring method was a review of logs followed by firewalls, then routine checks, core bank software and finally IDS.

Finally, the study recommends strategic fit information security solution and well-formulated management strategies. Security policies, and data management processes that are developed with the required flexibility were the key aspects of a faultless security solution.

Daniel et. al. (2013) conduct a study on the title "Education in IT Security: A Case Study in Banking Industry" in China. They employed focused group interview on two Hong Kong banks with five participants and used secondary data from worldwide study online of different countries and industries.

The interview finding shows information security awareness training was provided only for a new joiner, as a result, staff may not be aware of new threats or policies so that it was a challenge and non-IT staff thinks that information security was not their business; and the survey findings having many respondents were overconfident on their security program but do not have a process in place to handle it.

The authors discussed their finding as follows: security budget was not driven by security needs which were dropped from 51% in 2011 to 45% in 2012. Most companies think those resources should be used in better way such as generating more revenue. However, if the security program was ignored and the loss would be greater than they had earned. Less than half (47%) of the respondents had security training programs for employees that was not enough. There were many challenges when outsourcing IT projects, initially categorizing mission-critical data and services so that company staff should be aware of the risks or impacts.

In order to increase the information security awareness of the staff, security department of the banks should organize a formal security awareness program training with different topics, such as password management, social networking safety, and data loss protection.

Data Lost Prevention (DLP) strategies were one of the major challenges to the IT security industry. According to Ponemon Institute (2011) 70% of businesses have traced the loss of confidential information to USB devices and 55% of those incidents are likely related to malware-infected devices. How to manage the use of the USB device is a key area of concern.

Finally, the conclusion was that employees in Hong Kong banking industry didn't take vital training on information security training. Several methods which can increase the information security awareness were recommended. Information security training program should be designed and implemented. The management should allocate enough financial and human resources to implement this program. Once these suggestions are implemented in the bank, corporate security which keeps the banks information and physical assets secure in a proper way.

Chapter Three
Methodology

This chapter presented the methodology that used to conduct the study. Detail research approaches can visualize what the research methodology looks to be like, so that the research was governed by the following core topics and presented with the entire manner.

3.1. Research Design

In this study the researcher followed quantitative research approach to analyze the collected numerical data. Quantitative research is based on the measurement of quantity or amount. It is applicable to phenomena that can be expressed in terms of quantity and generates statistics through the use of large-scale survey research, using methods such as questionnaires or structured interviews. The study data bases on the questionnaire survey statistical data so that the researcher decided to follow the quantitative research method.

3.2. Study Population

The Ethiopian banking sector was selected to conduct this research because it is both critical to society and frequent prime target of insider and outsider attacks. According to Tripwire (2018) cyber hygiene report, the financial sector was the second target of cyber-attacks next to the manufacturing industry. The total population of the study was 18 commercial banks operating in Ethiopia. According to NBE report as of September 2018, among these 18 commercial banks 16 were private and the left two governmental. (Thales, 2015).

As shown in table 2 below, out of all 18 commercial banks three banks were selected by using stratified sampling and with the criteria of the year of core banking automation. All banks were divided into three strata and applying lottery method. The banks were classified into three strata based on the year of core banking automation. The first stratum is from the year 2000 - 2005, the second is from the year 2006 – 2010 and the final stratum contains year of core banking automation starting from 2011 up to now. This factor is selected due to the fact that as the bank starts using

the core banking system. It is obvious that there is internet access used to interconnect the branch to the central database server of the bank. While there is internet access there is a possibility to insider and outsider attack. However, there is an exception to this fact.

The selection process was discussed as follows. The first stratum which contains a couple of banks such as Wegagen Bank and Dashen Bank, and Dashen Bank was drawn. In the second stratum, there were five banks such as Berhan International Bank, Lion International Bank, Zemen Bank, Abay Bank, and Oromia International Bank. From this stratum, Abay Bank drawn. The third stratum contains eleven banks, those are Bank of Abyssinia, Development Bank of Ethiopia, Commercial Bank of Ethiopia, Nib International Bank, United Bank, Bunna International Bank, Awash International Bank, Addis International Bank, Debub Global, Enat Bank, and Cooperative Bank of Oromia. For this stratum, Commercial Bank of Ethiopia was drawn. Therefore, as per the lottery method Dashen Bank, Abay Bank, and Commercial Bank of Ethiopia were the populations of this study (NBE website, 2014).

Table 2: Ethiopian commercial banks, their year of automation, and selected sample banks (Source: (NBE website, 2014))

Bank Name	Year of automation	Stratum	Drawn sample bank
Wegagen Bank	2000	1	Dashen Bank
Dashen Bank	2003		
Berhan International Bank	2009	2	Abay Bank
Lion International Bank	2009		
Zemen Bank	2010		
Abay Bank	2010		
Oromia International Bank	2010		
Bank of Abyssinia	2011	3	Commercial Bank of Ethiopia
Development Bank of Ethiopia	2012		
Commercial Bank of Ethiopia	2012		
Nib International Bank	2012		

United Bank	2013		
Bunna International Bank	2013		
Awash International Bank	2014		
Addis International Bank	2014		
Debub Global Bank	2015		
Enat Bank	2015		
Cooperative Bank of Oromia	2017		

3.3. Data Source and Data Collection Instruments

The research numerical data collected from those selected three banks as shown in the above section. Based on stratified sampling and the year of automation criteria, Dashen Bank, Abay Bank and Commercial Bank of Ethiopia was the numerical data source of the study.

The researcher used the self-administered paper printed questionnaire as a primary data collection instrument. Cyber hygiene practice is the dependent variable of the research. The questionnaire contains 56 structured questions with 5 parts. Part one contains socio-demographic questions. Part two contains 16 questions regarding frequency of the dependent variable; cyber hygiene practice. Part three encloses 9 questions about the independent variable ISSP implementation level of agreement and 4 questions about the independent variable attitude with respect to ISSP. Part four was questions about level of awareness on ISSP which is the independent variable, procedure, and guidelines. Part five of the questionnaire plan to collect the data on the level of agreement regarding the independent variable computer and cyber hygiene training. The questionnaire was adapted from prior research. The nature of adoption of the questionnaire was taking basic cyber hygiene practice questionnaire ideas and prepared it based on the Ethiopian banking sector and to the perspective of this research. The questionnaire was distributed and collected physically to and from the respondent. In order not to disclose the respondents' identity the researcher stated no need to write the name or other unique identifications on the questionnaire. Moreover document analysis was another method to fulfill the research and strengthen the finding, such as policy and procedures of the banks.

3.4. Study Variables

The study variables were employees of the three selected Ethiopian banks; i.e. Dashen Bank, Abay Bank, and Commercial Bank of Ethiopia that include different hierarchical position and different departments of the head office organs such as IT, human resource (HR), and business officers. And from branch level employees such as customer service officer (CSO), banking business officer (BBO), branch control officer, customer relation officer (CRO), customer service manager (CSM) and branch manager.

3.5. Sampling Design

This research used convenience sampling. The researcher assumed that the banking business is homogenous throughout every bank in the country. Based on convenience sampling and the homogeneity of the banking business, the researcher takes 50 amount of sample size from each bank. Five branches from each bank and seven samples were taken from each branch (5*7=35), with a total of 105 samples. In addition, 15 samples from head office organs of each three banks (15*3=45) are also considered. A total of 150 samples were used from all three banks.

The place where the study was conducted at three selected banks such as the Dashen Bank, Abay Bank, and Commercial Bank of Ethiopia head quarter and selected branches which are found in Addis Ababa. The researcher believes that no need of mentioning the name of the branches, because of the banks security rule.

3.6. Data Analysis and Presentation Method

The data collection instrument used to collect the primary data was questionnaire and document analysis. The questionnaire encompasses three types of Likert scale questions. The first one which was inside part two of 16 questions and it was about the frequency of cyber hygiene practice. The scale range has 4 points, Always = 1, Frequently = 2, Rarely = 3, and Never = 4.

The second Likert scale was in part three, a total of (9+4) 13 questions. Its scale range has 5 points, range as Strongly Disagree = 1, Disagree =2, Undecided = 3, Agree = 4, and Strongly Agree= 5.

The third type of Likert scale questions was regarding the ISSP awareness level and classified under part four. It included 16 questions and which has 3 point scale ranges from Not Aware=1, Aware=2, and Fully Aware=3. Part five contains 6 questions which had 5 point scale ranges from Strongly Disagree = 1, Disagree =2, Undecided = 3, Agree = 4, and Strongly Agree= 5.

For further elaboration, the finding discussed using the weighted mean for a realistic average. To calculate the weighted mean the researcher used the following formula (C. R. Kothari, 2004).

$$\bar{X}_w = \frac{\sum W_i X_i}{\sum W_i}$$

Where $\bar{X}_w$ is Weighted item, Wi is Weight of i^{th} item X and X_i is Value of the i^{th} item X

The primarily collected data through the questionnaire was processed using tools SPSS version 20, Microsoft Excel, and the result would be presented by using tables in terms of statistical analysis such as frequency, percentage, mean, aggregate mean (mean of the mean) and chi-square representation.

3.7. Reliability of the research

Prior reliability test was conducted on the research instrument i.e. questionnaire. 10 questionnaires were used to the pilot study on system users of different profession purposively. As Taber (2017) identified, the value for α between 0.76 - 0.95 is said to be fairly high and acceptable. Table 3 below presents Cronbach alpha of the construct used for the survery.

Table 3: Reliability statistics

Cronbach's Alpha	No. of Items
.825	54

Similarly, this research pilot study α value was as indicated in table 3 above .825. It shows that α value lies in the acceptable range. So that the researcher concluded that the pilot study α value was acceptable and reliable.

Chapter Four
Findings and Discussion

4.1. Overview

In this chapter, the collected primarily data through a self-administered questionnaire is statistically presented, analyzed, and finally interpreted. The statistics of the collected quantitative data is presented using percentage and frequency distribution to show the truth of the fact finding. The purpose of this quantitative data survey is to measure the level of employee cyber hygiene practices. SPSS version 20 was used to analyze the collected primary data.

4.2. Data presentation

The data collected from the employees of Commercial Bank Ethiopian were analyzed using descriptive analysis and the detailed finding was presented with the following sub topics.

4.2.1. Summary of Sample Banks Profile

As mentioned earlier in section 3.2, the sample banks participated in the survey were selected using stratified sampling considering criteria, such as the year of core banking automation. The researcher took three banks; namely, Dashen bank, Abay bank, and Commercial bank of Ethiopia (CBE). Their profile is stated in the following table 4.

Table 4: Sample bank profile

As of 2019 1st quarter (March 31)			
Name of the bank	**Year of service start**	**Capital (in million Birr)**	**Number of branches**
Dashen bank	1996	3,898.5	389
Abay bank	2010	1,517.5	179
Commercial bank of Ethiopia	1943	45,801.6	1420

4.2.2. Questionnaire Response Rate

The questionnaire response rate of the three selected sample banks (Dashen bank, Abay bank, and Commercial bank of Ethiopia) are shown in table 5 below.

Table 5: Questionnaire response rate

Sample banks	Head offices		Sample Branches		Branches			Total	
	No. of dispatched questionnaires	Collected questionnaires			No. of dispatched questionnaires	Collected questionnaires		Sum	In %
Dashen Bank (DB)	15	13	DB	B1	7	5	22	35	70%
				B2	7	4			
				B3	7	5			
				B4	7	4			
				B5	7	4			
Abay Bank (AB)	15	10	AB	B1	7	5	22	32	64%
				B2	7	4			
				B3	7	4			
				B4	7	5			
				B5	7	4			
Commercial Bank of Ethiopia (CBE)	15	12	CBE	B1	7	5	24	36	72%
				B2	7	5			
				B3	7	4			
				B4	7	5			
				B5	7	5			
Total	45	35			105	68	68	103	68.7 %

As illustrated in the above table 5, from the total of 150 questionnaires distributed to the three banks, 103 of the questionnaire were collected, which gives 64.8% response rate. Lindemann (2019) stated that in-person survey is most used and effective survey method and the average survey response rate is 33%; the response rate of this research consider as acceptable.

4.2.3. Socio-Demographic Characteristics

Socio-demographic profile of survey participants is presented as follows. The first one is respondents' Educational level, summary of which is indicated in table 6 below. As shown in the table, most of the respondents that accounts for 76.7% are first-degree holder. Followed by 18.5% respondents having master's degree.

Table 6: Respondents educational level

Education level	Frequency	Percentage
Diploma/10+	1	1%
First Degree	79	76.7%
Master's	19	18.5%
Other	2	1.9%
Total	103	100%

A lot of respondents with 35 different types of job titles were participated in this research (see Appendix C). Table 7 below shows summary of respondents' job assignment. Accordingly, out of the total respondents participated in this research, 49.5% of them were business officers, 27% technical IT officers and, 26.2% business managers.

Table 7: Respondents job position

Job assignment	Frequency	Percentage
Business managers	5	4.9%
Business officers	51	49.5%
Technical IT managers	2	1.9%
Technical IT officers	27	26.2%
Total	103	100%

Further analysis of respondents work experience reveals the following and summary of respondents work experience is shown in table 8 below; 44.7% of work experience were between 5 and 10 years. 32% of the participants were less than 5 years of work experience. 18.4% of

employees with more than 10 years of experience. This shows that most of the participants have 5 and greater than 5 years of work experience.

Table 8: Respondents year of experience

Year of experience	Frequency	Percentage
Less than 5 years	33	32%
5-10 years	46	44.7%
Greater than 10 years	19	18.4%
Total	103	100%

Further, Table 9 below shows respondents' age, most participants that accounts for 56.3% of age were between 20 and 30 years old. This is followed by 37.9% respondents are with age between age 31 and 40 years old. 3.9 % respondents were between age 41 and 50. And only one respondent was aged less than 20 years old.

Table 9: Respondents age

Age	Frequency	Percentage
Less than 20 years old	1	1%
20-30 years old	58	56.3%
31-40 years old	39	37.9%
41-50 years old	4	3.9%
Total	103	100%

The respondents' level of computer usage experience to perform their day to day activities is also summarized in table 13. Most respondents (52.4%) have experienced greater than 5 years. 11.7% have computer experience between 4 and 5 years to perform their task. 6.8% respondents have computer experience that range between 1 and 3 years.

Table 10: Respondents computer experience

Year of experience in the use of computer	Frequency	Percentage
1-3 years	7	6.8%
4-5 years	12	11.7%
Greater than 5 years	54	52.4%
Total	103	100%

4.2.4. Computing Cyber Hygiene Practices

Cyber hygiene plays a critical role in protecting businesses. It also provides the foundations for protecting the infrastructure and customer data which businesses rely on. Organizations should practice cybersecurity strategy which aims to improve and enhance, the way they protect themselves from cyber threats (ENISA, 2016).

The whole finding of this research is interpreted based on the range and the mean value. The mean value was calculated using the weighted mean equation.

Table 11 below shows 16 questions to assess employees' cyber hygiene practice in Ethiopian commercial banks. From 16 listed questions, 56.25% of them shows that respondents never participated in the dangerous activities of their cyberspace. On the other hand, 43.75% of the result shows that the bank employees sometimes participated in it. The aggregate mean value was 3.18 which rated that employees are never participated in bad or wrong cyber hygiene practice. Among computing cyber hygiene practices related dependent variables addressed in the questionnaire, updating the password in different systems used in the bank have the lowest mean value and the staff should protect the cyber-hygiene.

Concerning respondents visit non-work related websites, 48.5% noted that, they abuse the internet access of their bank by using it for personal purpose. 46.6% of the system users occasionally used their work station to perform their personal work. Further, 45.6% of the Ethiopian commercial

banks' system users rarely use USB devices, which were not allowed by the respective management and department.

This research finding shows that the system users score 42.7% of rarely participated in the danger or bad cyber activities for both users not updating their work computer antivirus and not log off properly from the system or forgot to log off. Similarly, 32% of the banks' staff didn't take their work backup from their work computer to another device that can help them to restore it whenever their system faces problem.

On the other hand, as stated previously on average more than half of the listed cyber hygiene practices of the Ethiopian commercial bank's employee's shows positive practice, and is stated as follows. The user shall log out of the workstation when leaving workstation even if for a short period or for long time. For the case of this research, 48.5% of the respondents haven't experienced in leaving their workstation without logout their computers.

The employees of Ethiopian commercial banks' should protect their organization's sensitive data by not storing it over the cloud. This might lead to loss of control on their file. The majority, 49.5% of the respondents never used clouds like Gmail or Yahoo to sore or transfer their work files.

Writing or sticking a password on office desks is obviously a bad habit that can easily disclose it to the public, so that the system user shall keep passwords secretly. The user shall avoid keeping a paper or electronic record of the password. In this study, 82.5% of the respondents taking care of their password and they were not sticking it to their office desk. In the same way, 60.2% of the staffs were not sharing the password to their colleague.

Most respondents, 59.2% had no experience of downloading restricted software by using the organization facility. Employees should avoid risky practice like disclosing sensitive or confidential information. Information should be safeguarded. This research founded that 57.3% of participants safely handled secured, confidential or sensitive data. So that system users are responsible for protecting information assets resulting from its usages like data files, and reports against unauthorized access and misuse.

The banks' system access is solely protected using a password. The system itself has its own standard of password combinations like a minimum of eight or more character length and must be the combination of lower case, upper case, number, and special characters. In addition to this the bank system user required to set a strong password. The finding displayed in table 11 below presents that more than half, 52.4% of the entire respondents' never set an easily predictable or weak password.

Table 11: Respondents computing cyber hygiene practices

Experience of doing the following danger activities	Never		Rarely		Frequently		Always		Mean
	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	
Responding to the unknown email sender/spam	57	55.3%	34	33%	6	5.8%	5	4.9%	3.40
Not updating your password regularly	12	11.7%	38	36.9%	37	35.9%	15	14.6%	2.46
Visiting non-related website	28	27.2%	50	48.5%	15	14.6%	6	5.8%	3.01
Not updating antivirus/ antispyware	15	14.6%	44	42.7%	33	32%	9	8.7%	2.64
Forgetting to log off secure system	42	40.8%	44	42.7%	10	9.7%	4	3.9%	3.24
Writing or sticking my password on office desks	85	82.5%	10	9.7%	2	1.9%	4	3.9%	3.74
Allowing an unauthorized person to use your computer	57	55.3%	37	35.9%	5	4.9%	2	1.9%	3.48
Unsafe handling of secured/ confidential/sensitive data	59	57.3%	29	28.2%	8	7.8%	3	2.9%	3.45
Downloading restricted software	61	59.2%	25	24.3%	9	8.7%	5	4.9%	3.42
Sharing my password to others	62	60.2%	35	34%	4	3.9%	-	-	3.57
Leaving work computer without logout	50	48.5%	36	35%	12	11.7%	3	2.9%	3.32
Doing personal work by using a work computer	32	31.1%	48	46.6%	17	16.5%	5	4.9%	3.05

Experience of doing the following danger activities	Never		Rarely		Frequently		Always		Mean
	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	
Storing work files in cloud-like Gmail, Yahoo	51	49.5%	29	28.2%	16	15.5%	4	3.9%	3.27
Not backing up work files	22	21.4%	33	32%	28	27.2%	18	17.5%	2.58
Plugging an unauthorized portable device like USB	26	25.2%	47	45.6%	21	20.4%	8	7.8%	2.89
Using easily predictable or weak password	54	52.4%	36	35%	11	10.7%	1	1%	3.40
							Aggregate mean		3.18

4.2.5. ISSP and Procedure Implementation

ISSP is the guiding principle for all rules of information security and its resources of the organization. Employees who properly follow their organization's ISSP are assets to organizational security. Table 12 below shows the finding regarding the Ethiopian commercial banks ISSP and procedure implementation practice.

The overall aggregate mean result for the ISSP, guideline and procedure implementation practice is found 3.6 which were rated in the agreement category.

The Ethiopian commercial bank staff should avoid unhygienic practices to safeguard their workstation and its organization at large. In contrast, among the listed 9 questions of the ISSP and its implementation, only 42.4% of the staff knows how to avoid unhygienic cyber practices. It was the least result of all the finding regarding ISSP and its implementation of the Ethiopian commercial banks.

Majority of the respondents, 85.5% followed their organizations ISSP, related procedure and guideline. This can help to minimize risks related to cyber hygiene issues. Most of the Ethiopian commercial banks' staffs, 72.8% were certain to follow the rule and regulation that their organization state in the ISSP and its related procedure and guideline. Likewise, 70.8% of the staffs

were in the position of complying with the organization's information policy and its related procedure and guideline.

IS resources should be used as per the bank ISSP to form positive employee behavior on cyber hygiene. 60.2% of the employees agreed that their organization has established the rule of behavior for the use of computer resources and other digital assets. The banks day to day activity is performed under the organization's ISSP and related guidelines. 56.3% of the participants approved that their organization has a specific governing policy and related rules that describe acceptable use of the IS resource, that is used to manage the information security. In the same way, 54.3% of the respondents stated that their organization ISSP forbids employees to engage in the unhygienic cyber practice. Detail ISSP and related procedures could clearly lead the employee for better cyber hygiene practices. 52.4% of the respondents agreed that the existences of specific guidelines that govern what employees are allowed to do with their computer. 46.6% of the respondents had the skills and expertise to avoid engaging unhygienic cyber practices.

In summary, the Ethiopian commercial banks' had specific and formal ISSP, guideline and procedure that describe and govern the IS resources. It established rules of behavior among employees or users to certainly follow and develop an intention to continue following it. Though there is a need to boost the skills and expertise to avoid engaging in unhygienic cyber practices, the this study revealed that all the three sample banks (Dashen Bank, Abay Bank, and Commercial Bank of Ethiopia) have their own ISSP for their corporate banking business operation.

Table 12: ISSP and its practices

Agree or disagree with each of the following ISSP and implementation	Strongly Disagree		Disagree		Undecided		Agree		Strongly Agree		Mean
	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	
Certainly follow organization's ISSP, and related procedure and guidelines	5	4.9%	9	8.7%	11	10.7%	44	42.7%	31	30.1%	3.87

Agree or disagree with each of the following ISSP and implementation	Strongly Disagree		Disagree		Undecided		Agree		Strongly Agree		Mean
	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	
Likely follow organization's ISSP, and related procedure and guidelines	2	1.9%	7	6.8%	4	3.9%	53	51.5%	35	34%	4.11
Intention to continue to comply with organization's ISSP, and related procedure and guidelines	6	5.8%	6	5.8%	14	13.6%	43	41.7%	30	29.1%	3.86
The organization has specific procedure and guidelines that describe acceptable use of its IS resources	9	8.7%	15	14.6%	19	18.4%	41	39.8%	17	16.5%	3.42
The organization has specific procedure and guidelines that govern what employees are allowed to do with their computer	5	4.9%	14	13.6%	24	23.3%	35	34%	19	18.4%	3.51
The organization has a formal policy that forbids employees from engaging in an unhygienic cyber practice	6	5.8%	12	11.7%	23	22.3%	43	41.7%	13	12.6%	3.46
The organization has established rules of behavior for use of computer resources and other digital assets	3	2.9%	12	11.7%	21	20.4%	47	45.6%	15	14.6%	3.60
Individuals have basic knowledge on how to avoid unhygienic cyber practices	9	8.7%	18	17.5%	20	19.4%	38	26.9%	16	15.5%	3.34
Individuals have the skills and expertise to avoid engaging in unhygienic cyber practices	11	10.7%	19	18.4%	23	22.3%	35	34%	13	12.6%	3.20
									Aggregate mean		3.6

4.2.6. Users' Attitude on Following ISSP

Employees who were participated in this research were asked to express their opinion regarding the commitment to follow and obey for their organizations ISSP. As shown in table 13 below, for all four statements the respondents agreed. Accordingly, the first statement, "following the organization's ISSP is a good idea" is rated 84.4%; on the other hand, the statement "Following the organization's ISSP is necessary" is rated 87.3%. "Following the organization's ISSP is a beneficiary" is also further rated 89.3%. And 71.9% of respondents agreed with the statement "following the organization's ISSP is pleasant".

Most participants strongly agreed with the aggregate mean of 4.12. Therefore, the employees' attitude concerning following their organizations ISSP were good idea, necessary, beneficiary, and also pleasant. So that each user or employee is responsible and accountable for what he/she did to perform an activity on a day to day basis.

Table 13: Respondents ISSP attitude

Agree or disagree with each of the following ISSP attitudes	Strongly Disagree		Disagree		Undecided		Agree		Strongly Agree		Mean
	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	
Following the organization's ISSP is a good idea	7	6.8%	2	1.9%	5	4.9%	43	41.7%	44	42.7%	4.14
Following the organization's ISSP is a necessary	6	5.8%	1	1.0%	4	3.9%	47	45.6%	43	41.7%	4.19
Following the organization's ISSP is a beneficiary	5	4.9%	2	1.9%	2	1.9%	45	43.7%	47	45.6%	4.26
Following the organization's ISSP is pleasant	3	2.9%	7	6.8%	16	15.5%	45	43.7%	29	28.2%	3.90
									Aggregate mean		4.12

4.2.7. Awareness Level of ISSP

With the growing demand of IS, many authors have stressed the importance of eliminating weaknesses to understand and implement the organization ISSP, that are apparent in many organizations. Such weaknesses appear when people unconsciously disrupt ISSPs due to lack of awareness about related terms and conditions (De Lange J, 2016).

The following table 14 shows that the finding related to the ISSP level of awareness on the banks' employees, the mean range from 1.99 the lowest up to 2.46 the highest. The total aggregate mean of the finding was 2.23 which was greater mean than 2. Even if the mean was greater than 2 but it was closer to 2 which means that users were on the aware category about the listed ISSP practices.

As stated above, the greatest scored mean was password sharing with 2.46, this shows that the user aware about it. Using a complex password and since the bank provides it to the system user for only self-usage purpose it should not be shared to another user. As the research finding shows, 90.3% of the respondents aware of sharing their password to others is violating their organization ISSP. Furthermore, 88.4% respondents' aware of keeping their password at office desk is violating the organization ISSP.

Employee who uses computer to perform their day-to-day business activity is responsible and accountable for the tasks permitted to do's and not to do'. According to the organization IT rules and regulation (ISSP), this should bear in mind to every staff of the bank. As a result most respondents of this research 86.4% were aware of leaving work computer without logout against to the organization ISSP.

One of the purposes of the ISSP implementation in the bank is to safeguard the sensitive data and to not access by the unauthorized party. The finding indicates that 84.5% employees of the Ethiopian commercial banks aware about risk of mishandling confidential information regarding the ISSP of their organization. Mostly, the poorly selected password may expose to the password theft since it can easily be predictable. In the same way 87.4% of the respondents aware that using this easily predictable or weak password was the violation of ISSP.

The only person responsible for system transaction and for the outgoing email by using self-account is the user owner itself. Subsequently, 85.5% participants understood that leaving unattended system is highly risky practice of violating ISSP. System users are required to change their password within the given timeframe. This will help the employee to safeguard its workstation from password theft attack. Likewise, the finding of this research indicates 84.4% of respondent shows that employees were aware of regular password updating is required.

Allowing an unauthorized person to use our computer can easily encounter cyber threats. The user should understand the consequence of such type of practice and the finding shows that 85.4% of the respondents had an awareness on the issue. Most of the users were aware of their banks ISSP Hackers may use phishing as one of the ways of thieving someone's user which was used to email purpose. The user should recognize it to counter the way of self-exposing to these types of attack. Likewise, 87.4% respondents were aware that, they didn't respond for the unknown email sender or vulnerable for phishing attack.

System users are required to confirm that whenever they accessing the internet it is not allowed as well as it is violating the banks' ISSP. And the finding shows that 85.3% of the respondents were aware about downloading and using restricted software from any source could be a risky practice. This study finding shows the participants 88.4% understand that browse restricted site was violating to ISSP and so that the system user could lead to safeguarding its workstation and the bank at large. Every workstation is preferred to have updated antivirus in order to encounter the incoming malware attack. Complementary to this, the finding shows that 83.5% respondents were aware of not updating antivirus/antispyware was against the organization ISSP.

It is also revealed that 77.7% of the response concerning employee understanding doing private job by using a work computer was risky practice and violation of ISSP. One of the main task that the system user should take into consideration within a given time frame is backup work files and required to store it offline. As the respondents approved that 77.6% employees were aware of not performing periodic backup on work files will result in loss, damage or data theft and unable to easily restore it. Literature recommends not to store sensitive information on public computers or

clouds as a result it is misplace and will loss of control over it, and the 71.8% respondents had awareness of it.

Table 14: Respondents awareness level of ISSP

The extent to which you aware or not aware of each of the following as ISSP	Fully aware		Aware		Not aware		Mean
	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	
Phishing attack	36	35%	54	52.4%	11	10.7%	2.25
Update your password	40	38.8%	47	45.6%	14	13.6%	2.26
Browse restricted site	31	30.1%	60	58.3%	10	9.7%	2.21
Upgrading antivirus/antispyware	27	26.2%	59	57.3%	14	13.6%	2.13
Unattended secure system	39	37.9%	49	47.6%	12	11.7%	2.27
Keep password at office work area	46	44.7%	45	43.7%	11	10.7%	2.34
Permitting an unauthorized individual to utilize work computer	38	36.9%	50	48.5%	12	11.7%	2.26
Risky dealing with of secured/confidential/sensitive information	41	39.8%	46	44.7%	13	12.6%	2.28
Download and using of restricted software	39	37.9%	49	47.6%	14	13.6%	2.25
Password sharing	54	52.4%	39	37.9%	8	7.8%	2.46
Leave job computer with no logout	46	44.7%	43	41.7%	13	12.6%	2.32
Do private job with a job computer	32	31.1%	48	46.6%	21	20.4%	2.11
Loss of information through the misplacement	27	26.2%	47	45.6%	28	27.2%	1.99
Backup work files	30	29.1%	50	48.5%	22	21.4%	2.08
Plugging portable device	32	31.1%	51	49.5%	18	17.5%	2.14
Easily predictable password	41	39.8%	49	47.6%	12	11.7%	2.28
					Aggregate mean		2.22

4.2.8. Computer and Cyber Hygiene Training

A bank shall provide anti-fraud training to all employees and member of the board of director (BoD) whenever necessary. The bank shall promote fraud awareness by conveying the importance of fraud prevention to employees and BoDs of the bank, and shall provide adequate fraud risk management training (NBE, 2014; CBE, 2017).

The below table 15 contains statements that used to identify the employees of the Ethiopian commercial banks whether there were computer and cyber hygiene training conducted or not. According to the finding the aggregate mean value 2.93 which was closer to 3, it shows that the overall response of the respondents was with the agreement side of the existence of computer and cyber hygiene training.

Four questions mean value score was less than three but it was nearly three. Such as “my organization provides employees with education on computer issues”, “my organization provides training to help employees improve their awareness of computer and information security issue”, “my organization educates employees on their computer security responsibilities”, and “my organization, employees are briefed on the consequences of engaging in an unhygienic cyber practice”, the mean value was 2.96, 2.91, 2.89, and 2.83 respectively.

The highest mean score was 3.19, it was about the organization employee briefed on the consequences of using computer resources in an unauthorized way. Notably, 44.6% of the total respondents disagreed that there was formal computer and information security training conducted other than for newcomers while 34% agreed on formal training was conducted in addition to induction training. Therefore even if overall the aggregate mean value 2.93 of the finding shows it lies in the undecided group but it was closest to 3 which lies to the agreement category that means the employee assure that there was formal training was conducted other than induction.

Table 15: Respondents opinion regarding training

Please indicate the extent to which you agree or disagree with each of the following statements	Strongly Disagree		Disagree		Undecided		Agree		Strongly Agree		Mean
	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.	
The organization provides training to help employees improve their awareness of computer and information security issue	23	22.3%	24	23.3%	11	10.7%	27	26.2%	17	16.5%	2.91
The organization provides employees with education on computer issues	19	18.4%	23	22.3%	12	11.7%	39	37.9%	9	8.7%	2.96
In the organization, employees are briefed on the consequences of using computer resources in an unauthorized way	9	8.7%	23	22.3%	23	22.3%	34	33%	13	12.6%	3.19
In the organization, there is formal computer and information security training conducted other than induction training for newcomers	23	22.3%	23	22.3%	21	20.4%	23	22.3%	12	11.7%	2.78
The organization educates employees on their computer security responsibilities	18	17.5%	25	24. 3%	23	22.3%	22	21.4%	14	13.6%	2.89
In the organization, employees are briefed on the consequences of engaging in an unhygienic cyber practice	15	14.6%	31	30.1%	23	22.3%	22	21.4%	11	10.7%	2.83
									Aggregate mean		2.93

4.2.9. Cross-Tabulations

The cross-tabulation test highlighted the relationship between attributes of the study to identify whether they associate each other or they don't have a relationship at all. The researcher believed that the cyber hygiene practice is the core and central topic of the study. So that only taking the cross tabulation between cyber hygiene practice and other variables such as education level, work experience, and computer usage experience.

Based on the cross-tabulation of cyber hygiene practice (dependent variable) and education level (independent variable) in table 16 revealed that on average 56.3% of the respondents score greater sum than others, were first degree and master's degree holders who were not or never participated in exposing their day to day tasks to cyber-attack.

Table 16: Cross-tabulation between cyber hygiene practice and education level

Computing cyber hygiene practice frequency		Education level		
		Diploma/10+	First Degree	Master's
Responding to the unknown email sender	Never	1	42	11
	Rarely	0	26	7
	Frequently	0	5	1
	Always	0	5	0
Not updating password regularly	Never	0	9	2
	Rarely	0	28	9
	Frequently	1	26	8
	Always	0	15	0
Visiting non-related website	Never	1	23	4
	Rarely	0	37	11
	Frequently	0	11	3
	Always	0	5	1
Not updating antivirus/antispyware	Never	0	8	1
	Rarely	0	27	4
	Frequently	1	30	12
	Always	0	12	2
Forgot to log off secure system	Never	1	31	8
	Rarely	0	35	8
	Frequently	0	6	3
	Always	0	4	0

Computing cyber hygiene practice frequency		Education level		
		Diploma/10+	First Degree	Master's
Writing or sticking my password on office desk	Never	1	64	16
	Rarely	0	8	2
	Frequently	0	2	0
	Always	0	3	1
Allow an unauthorized person to use your computer	Never	1	42	10
	Rarely	0	32	5
	Frequently	0	2	3
	Always	0	1	1
Unsafe handling of secured/confidential/sensitive data	Never	1	47	10
	Rarely	0	18	8
	Frequently	0	7	1
	Always	0	3	0
Downloading restricted software	Never	1	44	13
	Rarely	0	20	4
	Frequently	0	8	1
	Always	0	4	1
Sharing my password to other	Never	1	47	10
	Rarely	0	28	7
	Frequently	0	2	2
Leaving work computer without logout	Never	1	39	7
	Rarely	0	27	8
	Frequently	0	9	3
	Always	0	2	1
Doing personal work by using a work computer	Never	1	26	4
	Rarely	0	35	11
	Frequently	0	13	3
	Always	0	4	1
Storing work files in a cloud like Gmail, Yahoo	Never	1	39	9
	Rarely	0	21	6
	Frequently	0	13	3
	Always	0	4	0
Not backing up work files	Never	0	18	3
	Rarely	1	21	10
	Frequently	0	24	3
	Always	0	14	3
Plugging an unauthorized portable device like USB	Never	1	20	3
	Rarely	0	35	11
	Frequently	0	16	4
	Always	0	7	1
	Never	1	39	12

Computing cyber hygiene practice frequency		Education level		
		Diploma/10+	First Degree	Master's
Using an easily predictable or weak password	Rarely	0	29	6
	Frequently	0	9	1
	Always	0	1	0

The cross-tabulation test result between cyber hygiene practice and work experience (independent variable) in the below table 17 shows that out of the total 16 questions, 9 or 56.3% of the response were respondents who have work experience 5 and greater years and who were not participated in the unhygienic activities score greater sum than other. This shows that whenever the year of experience becomes greater the tendency of system users to expose their cyber space to threat will be less.

Table 17: Cross-tabulation between cyber hygiene practice and work experience

	Computing cyber hygiene practice frequency	Work experience		
		<5 years	5-10 years	>10 years
Responding to the unknown email sender	Never	18	26	12
	Rarely	9	19	4
	Frequently	3	1	2
	Always	2	0	1
Not updating password regularly	Never	3	5	2
	Rarely	13	17	6
	Frequently	11	20	6
	Always	5	4	5
Visiting non-related website	Never	13	8	6
	Rarely	14	26	9
	Frequently	3	8	2
	Always	1	2	2
Not updating antivirus/antispyware	Never	8	5	0
	Rarely	9	21	12
	Frequently	11	14	7
	Always	4	5	0
Forgot to log off secure system	Never	14	16	9
	Rarely	16	22	6
	Frequently	1	6	2
	Always	1	1	1

	Computing cyber hygiene practice frequency	Work experience		
		<5 years	5-10 years	>10 years
Writing or sticking my password on office desk	Never	27	41	15
	Rarely	4	3	2
	Frequently	0	1	1
	Always	0	1	1
Allow an unauthorized person to use your computer	Never	20	23	11
	Rarely	12	19	6
	Frequently	0	2	1
	Always	0	1	1
Unsafe handling of secured/confidential/sensitive data	Never	21	26	12
	Rarely	7	15	4
	Frequently	2	3	2
	Always	1	0	1
Downloading restricted software	Never	24	21	13
	Rarely	7	16	2
	Frequently	1	5	2
	Always	0	2	2
Sharing my password to other	Never	20	25	15
	Rarely	10	18	4
	Frequently	1	3	0
Leaving work computer without logout	Never	20	17	10
	Rarely	8	20	7
	Frequently	3	8	1
	Always	0	1	1
Doing personal work by using a work computer	Never	15	7	8
	Rarely	15	24	7
	Frequently	2	11	3
	Always	0	4	1
Storing work files in a cloud-like Gmail, Yahoo	Never	18	20	11
	Rarely	6	16	5
	Frequently	8	8	0
	Always	0	1	2
Not backing up work files	Never	8	7	5
	Rarely	9	16	6
	Frequently	11	15	2
	Always	4	7	6
Plugging an unauthorized portable device like USB	Never	15	5	4
	Rarely	12	21	12
	Frequently	3	15	2
	Always	2	5	1

	Computing cyber hygiene practice frequency	Work experience		
		<5 years	5-10 years	>10 years
Using an easily predictable or weak password	Never	19	21	12
	Rarely	10	19	5
	Frequently	2	6	2
	Always	1	0	0

The cross tabulation finding in the following table 18 indicates that the cyber hygiene practice who were not participating in the unhygienic cyber practice and who have experience of using computer greater than five score 50% and when the number of years of experience of using computer increased the amount of the respondents also increased at the frequency of never category, for instance, the number of respondents of responding to the unknown email sender were 3 for computer experience 1-3 years, then it increased to 5 when the usage of computer experience was between 4 and 5 years. And it became 32 when the usage of computer experience greater than 5 years. Out of the total 16 questions, 75% of the response falls into never category which increased whenever the years of experience on computer usage increased. The number of respondents that have years of experience on computer usage greater than 5 was greater than the one that have between 4 and 5 years, and the number of respondents that had years of experience on computer use between 4 and 5 years was greater than that of which have between 1 and 3 years.

Table 18: Cross-tabulation between cyber hygiene practice and usage of computer experience

	Computing cyber hygiene practice frequency	For how long have you been using a computer to accomplish your task?		
		1-3 years	4-5 years	> 5 years
Responding to the unknown email sender	Never	3	5	32
	Rarely	3	4	19
	Frequently	1	0	2
	Always	0	3	1
Not updating password regularly	Never	0	2	5
	Rarely	6	2	22
	Frequently	1	3	20
	Always	0	5	7
Visiting non-related website	Never	3	4	12
	Rarely	3	4	31
	Frequently	1	1	7
	Always	0	2	3

	Computing cyber hygiene practice frequency	For how long have you been using a computer to accomplish your task?		
		1-3 years	4-5 years	> 5 years
Not updating antivirus/antispyware	Never	2	3	6
	Rarely	3	3	26
	Frequently	2	6	17
	Always	0	0	5
Forgot to log off the secure system	Never	3	2	21
	Rarely	3	7	28
	Frequently	1	1	5
	Always	0	1	0
Writing or sticking my password on office desk	Never	5	6	51
	Rarely	2	3	2
	Frequently	0	0	0
	Always	0	3	1
Allow an unauthorized person to use your computer	Never	4	6	27
	Rarely	3	4	23
	Frequently	0	2	2
	Always	0	0	2
Unsafe handling of secured/confidential/sensitive data	Never	3	5	37
	Rarely	3	2	13
	Frequently	0	3	2
	Always	1	2	0
Downloading restricted software	Never	6	7	28
	Rarely	1	1	19
	Frequently	0	1	5
	Always	0	2	2
Sharing my password to other	Never	4	6	34
	Rarely	3	6	18
	Frequently	0	0	2
Leaving work computer without logout	Never	5	6	20
	Rarely	1	4	24
	Frequently	1	1	8
	Always	0	1	2
Doing personal work by using a work computer	Never	4	4	10
	Rarely	3	7	27
	Frequently	0	1	13
	Always	0	0	4
Storing work files in a cloud-like Gmail, Yahoo	Never	4	8	27
	Rarely	1	1	18
	Frequently	2	1	7
	Always	0	2	1

	Computing cyber hygiene practice frequency	For how long have you been using a computer to accomplish your task?		
		1-3 years	4-5 years	> 5 years
Not backing up work files	Never	3	2	12
	Rarely	1	4	13
	Frequently	3	4	18
	Always	0	2	10
Plugging an unauthorized portable device like USB	Never	6	3	8
	Rarely	0	4	25
	Frequently	1	5	13
	Always	0	0	8
Using an easily predictable or weak password	Never	4	7	27
	Rarely	3	4	21
	Frequently	0	1	5
	Always	0	0	1

4.2.10. Cross Tabulation between ISSP Practices and ISSP Attitude

The cyber hygiene practice is dependent on the ISSP implementation practice and its attitude. So that the researcher preferred to identify whether the association between these ISSP practice and ISSP attitude variables are statistically significant.

Null Hypothesis: H_0: There is no significant association between ISSP practice and ISSP attitude.

Alternative Hypothesis: H_a: There is a significant association between ISSP practice and ISSP attitude.

The cross-tabulation between ISSP practices and ISSP attitude result is shown in the below consecutive tables. Out of the all 36 combinations of the cross-tabulation only the following 5 chi-square p-value was greater than alpha level of .05 that means 31 cross-tabulation combination (found in the appendix D) chi-square p-value result was smaller than alpha level of .05. Therefore, there is enough evidence to reject the null hypothesis.

Table 19: Chi-square test between having basic knowledge to avoid unhygienic cyber practices and following the organization's ISSP is a good idea

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	21.314a	16	.167
Likelihood Ratio	24.989	16	.070
Linear-by-Linear Association	3.747	1	.053
N of Valid Cases	101		

Table 20: Chi-square test between having basic knowledge to avoid unhygienic cyber practices and following the organization's ISSP is a beneficiary

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	26.249a	16	.051
Likelihood Ratio	27.720	16	.034
Linear-by-Linear Association	1.274	1	.259
N of Valid Cases	101		

Table 21: Chi-square test between having basic knowledge to avoid unhygienic cyber practices and following the organization's ISSP is pleasant

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	18.826a	16	.278
Likelihood Ratio	19.690	16	.235
Linear-by-Linear Association	.772	1	.379
N of Valid Cases	100		

Table 22: Chi-square test between having the skills and expertise to avoid engaging in unhygienic cyber practices and following the organization's ISSP is a good idea

Chi-Square Tests

	Value	Df	Asymp. Sig. (2-sided)
Pearson Chi-Square	20.942a	16	.181
Likelihood Ratio	23.166	16	.109
Linear-by-Linear Association	.303	1	.582
N of Valid Cases	101		

Table 23: Chi-square test between having the skills and expertise to avoid engaging in unhygienic cyber practices and following the organization's ISSP is pleasant

Chi-Square Tests

	Value	Df	Asymp. Sig. (2-sided)
Pearson Chi-Square	14.622a	16	.552
Likelihood Ratio	17.538	16	.352
Linear-by-Linear Association	.008	1	.927
N of Valid Cases	100		

4.3. Discussion

4.3.1. Employee Cyber Hygiene Status of the Ethiopian Banking Industry

Cyber hygiene focuses on the human or user aspect rather than technological infrastructure and the employee of the organization can keep their organization cybersecurity safe or not exposed to any threat. They could intentionally or unintentionally result as a threat for the organization. As per the finding and as compared to other practices, the first least result was employees won't update their password within the time frame to secure their workstation specifically and their organization at large. Most banks' system enforce user to change password within a given time frame like a minimum of three or six months.

The second least result was shown that employees were not interested to backup their work file, so that if their workstation faces software or hardware temporary or permanent failure to the level of missing sensitive business data it could result in missing this critical work data and it is unable to restore it. The user should know and consider periodically backup these important data and the important thing to remember is to store this data “offline”, meaning transferring the important files to a storage device that detached from the computer after copied all of the files.

The thirdly least result was observed employees were not exercise updating their workstation antivirus. This may result the workstation to easily attack by malware, and the client computer should install the latest antivirus with an up-to-date definition. So the user is responsible to ensure updated anti-virus is employed to the workstation.

The final least result was practices of using unauthorized portable devices. USB sticks mostly infected with malware are an ever-present threat; once plugged in, hackers quickly spread throughout an organizations system and begin to do serious damage. Most banks are not allowed to use personally owned portable devices which was not approved by respective person (Abay Bank, 2015; Union Bank of India, 2015; Commercial Bank of Ethiopia, 2016; US, 2016; Lillie, 2018).

Moreover, there was a bit gap observed that the Ethiopian commercial banks employees experience doing their personal work by using a work computer. Also they were participated in visiting non-related and not allowed website which can expose the workstation to cyber-attack.

The finding shows that the rest of the cyber hygiene practices like users were not participated in responding to the unknown email sender. User shall guard against responding to emails asking them to provide their username and password even if originated from the bank staff reasoning for system maintenance or support. Forgot to log off from the system is one of the unhygienic practice and also they were not practicing it. The Ethiopian commercial bank system users were keeping their password safely since they are responsible for the task performed using their user ID. They were not allowing unauthorized person to use their workstation, they kept their bank critical data safely. They were not downloading restricted software and no one is allowed to perform any task

using other user ID. Users shall ensure unattended computing equipment has appropriate protection, the Ethiopian commercial bank employees had good cyber hygiene practice regarding this issue. Once storing work file to cloud, then after it can't be manageable, the staffs keep their file from such unhygienic habit. Users were practiced of using strong password to make it difficult to hack. (Abay Bank, 2015; Commercial Bank of Ethiopia, 2016).

The cross tabulation finding shows that employees who have education level greater and equal to first degree perform good cyber hygiene practice than employees who have education level less than first degree. And employees who have work experience greater and equal to 5 years participated in good cyber hygiene practice than others.

4.3.2. Employee Cybersecurity Awareness Level of the Ethiopian Banking Industry

Every organization should have well taken care of the information assets. Sensitive data of the bank should be kept safe than other ordinary information. And if staffs are not educated, the confidential data simply flow to the external parties. Therefore, employee awareness on the cybersecurity of the organization is a key issue to overcome the cyber threat and attack. The Ethiopian commercial banks' employees were aware on most of the unhygienic activities which violate the bank's ISSP. This doesn't mean that there is sustained awareness level and implementation. Awareness alone is nothing without implementation.

4.3.3. Information Security Policy Application in the Ethiopian Commercial Banks

ISSP of an organization represents a very important components of the overall security policy and it is the rule for all the procedure and guidelines. If an employee abides by the ISSP it provides acceptable use and prohibited use, and finally it will become a corporate culture. In a number of ISSP documents, users are warned to avoid inappropriate use of the organizational facilities and information assets. The finding indicates that the Ethiopian commercial bank staffs were adhered and implemented to their bank's ISSP, procedure and guideline. The finding shows that there was a significant association between ISSP practice and ISSP attitude.

Negussie (2015) concluded that even if the level of implementation vary, all Ethiopian commercial banks own ISSP that they formulated and developed to fulfill the order of regulatory body, rather the policy should formulate to reflect and promote the corporate culture.

4.3.4. Ethiopian Banking Industry Cyber Hygiene Improvement Strategies

Having a well understood information security policy and documented procedures help to protect organizations and reduce risk from both internal and external cyber threats. The finding shows that there were lack of training in the Ethiopian commercial banks employees. The insider threat (2018) research reported that the primary policy-based management of the organizations has been in place. The use of company policies and training was covered 68%, internal audits 63%, and background checks 56%. The organizations that offer training to their staff were 82%. Fiorentino (2018), also stated that safety product manufacturer implemented a training program and within the first year, their rate of employees failing the simulated phishing attacks reduced from 25% to between 5% and 8%.

Chapter Five
Conclusion and Recommendation

This chapter presents the key findings of the research and state recommendations related to the finding. This research explores the cyber hygiene practices of Ethiopian commercial bank's employees.

5.1. Conclusion

The overall conclusion of the cyber hygiene practices amongst employees of Ethiopian commercial banks that emerge from the finding and discussion presented as follows. There were computer and cyber hygiene training conducted but was with a little extent. The lack of staff training was noted. Since the Ethiopian commercial banks' employees lack regular computing cyber hygiene training, it is obvious to observe the gap on computing cyber hygiene practice. As the banking sector has become one of the most significant growth catalysts for the nation's economy, it is one of the most targeted victims of the cyber-attacks. Ayalew (2016) concluded that the bank security management dependent on the employees' ability to effectively protect the bank information asset.

Awareness plays a big role for the organization's successful cyber hygiene. The research indicates that 31% of the insider attack was due to lack of awareness. Organizations should realize that prevention and awareness are key cornerstones in the defense against insider security breaches. Negussie (2015) concluded that people are considered as the weakest link for the information security but they are powerful assets to minimize security threat by using reducing their weakest parts while users' security awareness enhanced to comply with information security policies. Woretaw and Lessa (2012) found that there were unsatisfactory information security awareness existed in the Ethiopian commercial banks (Schulze H., 2018)

Regarding the implementation of ISSP and its related procedure and guideline, the employees of the Ethiopian commercial banks were aware to the ISSP, procedure and guideline of their organization. They were willing and committed to follow so that creating safe and workable

cyberspace for their workstation. This culture should be continual to meet the organization's short, medium and long term goal of the cyber hygiene and cybersecurity.

On the other hand, experienced Ethiopian commercial banks employees had better ISSP awareness level. Also employees who experienced using of computer had very good awareness level of their bank's ISSP, so that such types of employee can be considered as an asset to the organization.

Finally, every employee should take its own part to safeguard its own workstation individually and in group, this will result to safe the bank cyberspace community and the banking industry in the nation at large.

5.2. Recommendation

CEO's decision is required for the plan and implementation of different cyber hygiene or security management strategic measures which can improve the cyber hygiene practice. Regular assessment should be conducted to provide adequate training in the security procedures and the correct use of information processing facilities. Therefore based on the regular assessment, strategic training plan could be designed and implemented; this is one of the improvement strategy for the organizations to ensure the cybersecurity among the employees.

There shall be one compulsory session of security in all the information technology courses and should address various security issues facing the bank. This session is required to have sustained awareness together with implementation. The training should consider the advancement of technology as well as parallel to the pace of the attackers so that the employee can have a better understanding and motivated to implement the bank ISSP and the cyber hygiene.

Management decision is required to utilize employees who termed as an asset of the bank i.e. who had a very good understanding and implementation experience on their bank's ISSP, to conduct training whether it could be class-based or on the job training.

Moreover, the bank should distribute the ISSP to its employee whenever newcomers are recruited. Whenever there is ISSP update or amendment, it should distributed or broadcast it by using

company mail or through other communication media for everyone who uses computer. This will increase the employees' awareness level and it can encourage users to its implementation.

5.3. Future Work

This study focused on the cyber hygiene practices of the Ethiopian commercial bank's employee. Further studies can be focused for the future on the impact of training or awareness creation in the cyber hygiene or cyber security of the banking sector in Ethiopia. It is used to understand the perceptions of system users of the banks towards of protect the cyberspace of their banks.

Framework design for the cyber hygiene and its related topics could be another area of the future researcher work to show new finding patter to the domain, and the impact of unhygienic cyber practice in Ethiopia could be another wide research topic for the future work.

References

Abay Bank. (2015, April). Information Technology Policy. Information Technology Policy. Addis ababa: VP-System and E-banking.

Ali, e. a. (2011). SQL-injection vulnerability scanning tool for automatic creation of SQL-injection attacks. Procedia Computer Science, pp. 453–458.

Alqahtani, F. H. (2017). Developing an Information Security Policy: A Case Study Approach. Procedia Computer Science, 691-697.

Ayalew, G. (2016). Assessment of Information Security Culture In the Banking Industry: The Case Study of Development Bank of Ethiopia. Addis Ababa, Ethiopia: MSc Thesis, St' Mary University School of Graduate Studies.

Babu, B. B. (2018). Cyber security in banks. The Journal of Indian Institute of Banking & Finance, 26-32.

Bauer S. et. al. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. Computers & Security, 145-159.

Benardo, B. &. (2015, November). A Framework for Cybersecurity. Supervisory insight. Washington: FFIEC.

Bendovschi, A. (2015). Cyber Attacks Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 24-31.

Brook, C. (2018). Digital Guardian's Blog. Retrieved January 2019, from Digital Guardian's Blog website: https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more

C. R. Kothari. (2004). Research Methodology. In C. R. Kothari, Research Methodology (p. 132). New Delhi: New Age International.

CBE. (2013). CBE. Retrieved December 2018, from CBE portal: cbe.portal (unpublished)

CBE. (2017, April). Fraud Management. Fraud management and anti-money laundring/combating financing of terrorism policy. Addis ababa, Ethiopia: CBE.

Cisco. (2018). Annual cyber security report, Impacts on public center. Cisco.

Cisco. (2018). Cisco. Retrieved May 2019, from Cisco blog website: https://blogs.cisco.com/security/how-panaseer-is-leading-the-way-in-cyber-hygiene-for-enterprise-security

Cisco special report. (2018). Cybersecurity special report; Small and Mighty. Cisco.

COBIT. (2004). COBIT Security Baseline – An Information Security Survival Kit. COBIT (Control Objectives for Information and related Technology). USA: IT Governance Institute.

Commercial Bank of Ethiopia. (2016, May). Information System Policy. CBE Information System Policy. Addis Ababa: CBE.

CSBS. (2014). CYBERSECURITY101: A Resource Guide for BANK EXECUTIVES. A Resource Guide for BANK EXECUTIVES Executive Leadership of Cybersecurity. Washington, D.C.: Conference of state bank supervisors.

CSIR. (2017). 6th CSIR Conference. Retrieved January 2019, from 6th CSIR Conference website: https://conference2017.csir.co.za/

Daniel et. al. (2013). Education in IT Security: A Case Study in Banking Industry. Hong kong.

David. (2011). Organizational Security and the Insider Threat: Malicious, Negligent and Well-Meaning Insiders. Organizational Security and the Insider Threat: Malicious, Negligent and Well-Meaning Insiders. Symantec.

Dawson, C. (2002). Research Methods. Oxford: Cromwell Press.

De Lange J, V. S. (2016). Information security management in local government. IST-Africa Week Conference (pp. 1-11). Durban, South Africa: IIMC International Information Management Corporation.

Eggenschwiler et.al. (2016). Insider Threat Response and Recovery Strategy of Financial Services Firms. In E. et.al., Computer Fraud & Security. University of Oxford.

ENISA. (2016, December). Review of Cyber Hygiene practices. Review of Cyber Hygiene practices. Greece, Athens: European Union Agency For Network and Information Security.

Ethiopia. (2004, May). Criminal Code of the Federal Democratic Republic of Ethiopia. Federal Negarit Gazeta Proclamation No. 414/2004, Arts 706-711. Addis Ababa: Federal Negarit Gazeta.

Ethiopian Ministry of Justice. (2016, June). Computer Crime Proclamation. Federal Negarit Gazeta Proclamation No. 958/2016. Addis Ababa: Federal Negarit Gazeta.

Falanx. (2017). cyber special report WannCry attack. Falanx .

Fernando and Yukawa. (2014). Internal control of information sharing through user security behavioral profiling. Global Journal of Human Social Science.

FFA. (2015). Financial fraud action uk annual review: working together to prevent fraud. Retrieved January 2019, from http://www.financialfraudaction.org.uk/

Fiorentino N., e. a. (2018). The Impact of Cybersecurity Incidents on Financial Institutions. The Impact of Cybersecurity Incidents on Financial Institutions. General Global Assistance.

FraudWatch International. (2019). FraudWatch International. Retrieved Feb. 2019, from FraudWatch International: https://fraudwatchinternational.com/security-awareness/what-is-cyber-security-awareness-training/

Funkhouser & Ritti. (2014). organizational culture chapter 16. In Ritti R. & Funkhouser G., organizational culture.

George et. al. (2012). Carnegie Mellon University. Retrieved August 2016, from Common Sense Guide to Mitigating Threats: http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf

Griffiths. (2016). Cyber security as an emerging challenges to South African national security. Pretoria: University of Pretoria.

Guire, M. (2017). Financial news. Retrieved May 2019, from Financial news website: https://www.fnlondon.com/articles/bank-security-chief-touts-basic-cyber-hygiene-to-combat-rising-threats-20171116

H1, M. t. (2017). Malware trend report. Mines Resort: cyber security Malaysia.

Habitu8. (2019, June). habitu8. Retrieved 2019, from info habitu8: https://info.habitu8.io/security-awareness-program-plan-and-strategy-guide

Hagen et.al. (2008). Implementation and effectiveness of organizational information security measures. Information Management & Computer Security, 16(4), 377-397.

Hailu. (2015). The State of Cybercrime Governance in Ethiopia. Malta: University of Malta.

Hassan. (2017). African cyber security report, Demystifying Africa's Cyber Security Poverty Line. Serianu Limited.

Hirschheim & Newman. (1991, March). Symbolism and information systems development: Myth, metaphor and magic. Information Systems Research. Maryland: Information Systems Research.

Horne. (2014, December). The cyber threat to banking. The cyber threat to banking, A global industry challenge. London: BBA The cyber threat to banking.

INSA. (2013). A Proclamation to Legislate, Prevent and Control Computer Crime. Draft Version 1.0. Addis Ababa: INSA.

ISACA. (2010). ISACA. Retrieved December 2018, from Business Model for Information Security: http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx

ISACA. (2011). Creating a Culture of Security. Retrieved March 2011, from ISACA: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Creating-a-Culture-of-Security.aspx

ISF. (2000). Information Security Culture – A Preliminary. Information Security Culture – A Preliminary. UK: ISF.

ISO/IEC 17799 (BS 7799-1). (2005). Information technology- Security techniques-Code of practice for information security management, Britain. ISO/IEC.

ISO/IEC 27001:2009. (2009). Information technology – Security techniques – Information security management systems – Overview and Vocabulary. Retrieved from Information technology – Security techniques – Information security management systems – Overview and Vocabulary: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en

Jackie, c. (2018). Cybersecurity Research Essential to a Successful Digital Future. Engineering 4, 9-10.

Jowi & Abade. (2016). Evaluation of Information Security Risk Assessment for Internet Banking Among Commercial. American Journal of Networks and Communications, 51-59.

k. Yilma. (2014). Developments in Cybercrime Law and Practice in Ethiopia. African Journals Online, 448-458.

Kaspersky Lab. (2015). The Great Bank Robbery: Carbanak cybergang steals $1bn from 100 financial institutions worldwide. Retrieved December 2015, from Kaspersky Lab: https://www.kaspersky.com/about/press-releases/2015_the-great-bank-robbery-carbanak-cybergang-steals--1bn-from-100-financial-institutions-worldwide

Kassa. (2017). African cyber security report, Demystifying Africa's Cyber Security Poverty Line. Serianu Limited.

KragBrotby. (2009). Information Security Governance: Guidance for Information Security Managers. IT Governance Institute. IT Governance Institute.

L. Hadlington. (2018). Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom. International Journal of Cyber Criminology, 262-274.

Lillie, B. (2018). HUFFPOST. Retrieved May 2019, from HUFFPOST website The Evolution Of Cyberspace: https://www.huffingtonpost.co.uk/bryan-lillie/the-evolution-of-cyberspa_b_15277788.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAGIl-Hg5PC0-TCAXipWtcO_ZwQ1KUBfrwZoC-hV12vR7q-aIovowMWqdHZ3FszbKbhmheGo85KD-GNHkK084FW

Lindemann, N. (2019, August 8). SurveyAnyplace. Retrieved from surveyanyplace Blog: https://surveyanyplace.com/average-survey-response-rate/

Mark and Hardy. (2014). Risk, Loss and Security Spending in the Financial Sector. A SANS Survey. SANS Institute.

Martins & Eloff. (2002). Information Security Culture. In Security in the information society. Boston: Kluwer Academic.

Martins and Eloff. (2006). Information Security Culture In Security in the information society. Boston: Kluwer Academic.

Merriam-Webster. (2019). Merriam-Webster. Retrieved April 2019, from Merriam-Webster dictionary: https://www.merriam-webster.com/dictionary

Mulwa. (2012). A survey of insider information security threats management in commercial banks in Kenya. Nairobi: University of Nairobi.

Mundra. (2016). Information technology and cyber risk in banking sector - the emerging fault lines. Mumbai: Centre for Advanced Financial Research and Learning.

Munir & Manarvi. (2010). Information Security Risk Assessment for Banking Sector-A Case study of Pakistani Banks. Global Journal of Computer Science and Technology.

NBE. (2014). Licensing and Supervision of Banking Business Fraud Monitoring Directives No. SBB/59/2014. Licensing and Supervision of Banking Business Fraud Monitoring Directives No. SBB/59/2014. Addis Ababa, Ethiopia: NBE.

NBE website. (2014). National Bank of Ethiopia web site. Retrieved December 2018, from National Bank of Ethiopia web site: https://www.nbe.gov.et/financial/banks.html

Negussie A. (2015). Practices, Challenges and Prospects of Information Security Policy in Ethiopian Banking Industry. Addis ababa: AAU.

Ngwenya & Malufu. (2012). Perceptions Towards On-line Banking Security: An Empirical Investigation of a Developing Countrys Banking Sector, how secure is On-line Banking. International Journal of Computer Science and Network (IJCSN), 1(16).

Ousley. (2013). Complete Reference: Information Security (2nd ed.). USA: McGraw.

Oxford. (2018). oxford dictionary. Retrieved December 2018, from oxford dictionary website: https://www.lexico.com/en/definition/culture

Parmvir. (2015). The role of Banking and Financial Services industry in economic recovery. Online International Interdisciplinary Research Journal, 187-193.

Ponemon Institute. (2011). Ponemon Institute,. Retrieved November 2012, from The State of USB Drive Security: http://media.kingston.com/images/usb/pdf/MKP_272_Ponemon_WP.pdf

Rajendran. (2018, January-March). Banking on IT's Security. The Journal of Indian Institute of Banking & Finance, 13-17.

Roer. (2015). Building a security culture. IT Governance Publishing.

SANS. (2009). How to Establish a Security Awareness Program. How to Establish a Security Awareness Program. SANS Institute.

Schein. (1992). Organizational Culture and Leadership. Jossey-Bass.

Schulze H. (2018). 2018 Insider theat report. cyber security insiders.

Schulze, H. (2016). Insider threat. Crowd Research Partners.

Serianu. (2017). African cyber security report, Demystifying Africa's Cyber Security Poverty Line. Nairobi : Serianu Limited.

Shamal & Ivan. (2010). A Model of Security Culture for e-Science. A Model of Security Culture for e-Science. Oxford: University of Oxford.

Siponen, P. a. (2007). Employees' adherence to information security policies: An exploratory field study. Information & Management, 134-143.

Skoudis, E. (2012). Evolutionary Trends in Cyberspace. In E. Skoudis, Chapter 6.

Straub & Welke. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making.". MIS Quarterly, 22(4).

Strauss. (2017). Cyber Threats and Responses in the banking sector. CSIR Conference. CSIR: CSIR.

Sudan Tribune. (2017). Sudan tribune. Retrieved January 2019, from sudan tribune website: http://www.sudantribune.com/spip.php?article62497

Symantec corporation. (2019). Norton. Retrieved May 2019, from Norton corporation website How to good cyber hygiene: https://us.norton.com/internetsecurity-how-to-good-cyber-hygiene.html

Taber. (2017, June 7). The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. Cambridge: Science Education Centre, Faculty of Education, University of Cambridge, 184 Hills Road, .

Tessem & Skaraas. (2005). Creating a security culture. Retrieved January 2006, from Creating a security culture: www.telenor.com/telektronikk/volumes/pdf/1.2005/Page_015–022.pdf

Thales. (2015). Vormetric Thales. Retrieved January 2019, from Vormetric Insider Threat Report: https://dtr.thalesesecurity.com/insiderthreat/2015/

Thales. (2018). Thales. Retrieved January 2019, from Thales data threat report: ttps://dtr.thalesesecurity.com/

The East African. (2016, December). The East African business. Business. The East African.

Thebestvpn. (2019). thebestvpn. Retrieved May 2019, from thebestvpn website: https://thebestvpn.com/cyber-security-statistics-2019/

Travelers. (2015). Travelers Business Risk Index. Sciences IJECS-IJENS, 23-29.

Tripwire Inc. (2018). Tripwire State of Cyber Hygiene Report. portland, Oregon: Tripwire Inc.

Udeh & Dhillon. (2008). An Analysis of Information Security Governance Structures: the Case of Société Générale Bank. 3rd Annual Symposium on Information Assurance, pp. 41-46.

Ula et. al. (2011). A Framework for the governance of information security in banking system. Journal of Information Assurance & Cyber Security, 1-12.

Union Bank of India. (2015, May). Information Security Policy of Union Bank of India. Information Security Policy of Union Bank of India. Mumbai: Union Bank of India,.

US, S. S. (2016). Cyber hygiene & cyber security recommendations. Washington: U.S. Department of Homeland Security.

Veiga. (2008). Cultivating and Assessing Information Security Culture. Pretoria: Pretoria University.

Von Solms et. al. (2011). Information security governance control through comprehensive policy architectures. In Information Security South Africa, 1-6.

Websense. (2015). 2015 Industry Drill-Down Report. Retrieved December 2015, from Websense Security Labs: https://www.websense.com/assets/reports/report-2015-industry-drill-down-finance-en.pdf

Woretaw & Lessa. (2012). Information Security Culture in the Banking Sector in Ethiopia. ICTET.

Appendix A: Letter of Cooperation

አዲስ አበባ ዩኒቨርሲቲ
የተፈጥሮ ሳይንስ ኮሌጅ
የኢንፎርሜሽን ሳይንስ ት/ቤት

ADDIS ABABA UNIVERSITY
College of Natural Science
School of Information Science

Date: - February 27, 2019
Ref: - SIS/40/2019/11

To whom it may Concern

Dear Sir/Madam,

Student Biruk Deferew (ID.No GSE/0086/07) is a graduae student at the School of Information Science, Addis Ababa University. He is currently conducting a MSc. Thesis research under the title "Cyber hygiene Practices amongst employees of Ethiopian Commercial Bank".

I would like to thank you in advanced for all the assistance that you would provide to the student.

With Regards,

Tibebe Beshah (PhD)
Head, School of Information Science

Appendix B: Questionnaire

CYBER HYGIENE RESEARCH QUESTIONNAIRE

Dear Sir/Madam,

This questionnaire is prepared in order to investigate the employees of Ethiopian commercial banks cyber hygiene practices. Hence, I kindly request you to share some time to fill this questionnaire. The collected data will be statistically analyzed, and a conclusion will be finalized; based on the finding, the result will be used to recommend the identified gap. Your assistance and cooperation will be highly appreciated. Besides, all your responses will be used only for academic purpose and it is confidential, so please no need to write your name or other unique identification matters.

Biruk Deferew

Thank you in advance for your kind cooperation!

PART ONE: Questions related to your demographic data

Please respond to the following questions either by ticking "✓" in the appropriate box or by writing your answer in the space provided.

1. Your education level:

☐ Diploma/10+ ☐ First Degree ☐ Master's other _____

2. Job title: _____

3. Years of experience: ☐ <5 years ☐ 5-10 years ☐ >10 years

4. Age: ☐ less than 20 ☐ 20-30 years ☐ 31-40 years

☐ 41-50 years ☐ More than 50 years

5. For how long have you been usinga a computer to accomplish your task?

☐ <1 year ☐ 1-3 years ☐ 4-5 years ☐ >5 years

PART TWO: C**omputing cyber hygiene practices**

Never = 4, Rarely = 3, Frequently = 2, Always = 1

Experience of doing the following danger activities	**Never**	**Rarely**	**Frequently**	**Always**
1. Responding to the unknown email sender/spam				
2. Not updating your password regularly				
3. Visiting non-related website				
4. Not updating antivirus/antispyware				
5. Forgot to log off the secure system				
6. Writing or sticking my password on office desks				
7. Allowing an unauthorized person to use your computer				
8. Unsafe handling of secured/confidential/sensitive data				
9. Downloading restricted software				
10. Sharing my password to other				
11. Leaving work computer without logout				
12. Doing personal work by using a work computer				
13. Storing work files in cloud-like Gmail, Yahoo				
14. Not backing up work files				
15. Plugging an unauthorized portable device like USB				
16. Using an easily predictable or weak password				

PART THREE: Information system security policy (ISSP), procedure and guideline implementation

Strongly Agree = 5, Agree = 4, Undecided = 3, Disagree = 2, Agree = 1

Agree or disagree with each of the following ISSP and implementation	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree
1. I am certain that I will follow my organization's ISSP, and related procedure and guidelines					
2. I am likely to follow my organization's ISSP and related procedure and guidelines in the future					
3. It is my intention to continue to comply with my organization's ISSP and related procedure and guidelines					
4. My organization has specific guidelines that describe acceptable use of its IS resources					
5. My organization has specific guidelines that govern what employees are allowed to do with their computer					
6. My organization has a formal policy that forbids employees from engaging in an unhygienic cyber practice					
7. My organization has established rules of behavior for use of computer resources and other digital assets					
8. I have basic knowledge on how to avoid unhygienic cyber practices					
9. I have the skills and expertise to avoid engaging in unhygienic cyber practices					

Attitude regarding ISSP

Agree or disagree with each of the following ISSP attitudes	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree
1. Following the organization's ISSP is a good idea					
2. Following the organization's ISSP is a necessary					
3. Following the organization's ISSP is a beneficiary					
4. Following the organization's ISSP is pleasant					

PART FOUR: Awareness level of ISSP

Fully aware = 3, Aware = 2, Not aware = 1

The extent to which you aware or not aware of each of the following ISSP activities	Fully aware	Aware	Not aware
1. Phishing attack			
2. Update your password			
3. Browse restricted site			
4. Upgrading antivirus/antispyware			
5. Unattended secure system			
6. Keep password at office work area			
7. Permitting an unauthorized individual to utilize work computer			
8. Risky dealing with of secured/confidential/sensitive information			
9. Download and using of restricted software			
10. Password sharing			
11. Leave job computer with no logout			
12. Do private job with a job computer			
13. Loss of information through the misplacement			

14. Backup work files			
15. Plugging portable device			
16. Easily predictable password			

PART FIVE: C**omputer and cyber hygiene training**

Please indicate the extent to which you agree or disagree with each of the following statements	**Strongly Disagree**	**Disagree**	**Undecided**	**Agree**	**Strongly Agree**
1. My organization provides training to help employees improve their awareness of computer and information security issue					
2. My organization provides employees with education on computer issues					
3. In my organization, employees are briefed on the consequences of using computer resources in an unauthorized way					
4. In my organization, there is formal computer and information security training conducted other than induction training for newcomers					
5. My organization educates employees on their computer security responsibilities					
6. In my organization, employees are briefed on the consequences of engaging in an unhygienic cyber practice					

Appendix C: Respondents' Job Title

Education level	Frequency	Percentage
Accountant	1	1%
Application developer	1	1%
Associate quality assurance	1	1%
BBO	9	8.7%
Branch controller	2	1.9%
Branch manager	3	2.9%
Branch transaction control officer	6	5.8%
Business operation officer	1	1%
CRO	2	1.9%
CSM	1	1%
CSO	16	15.5%
Database administrator	1	1%
E-banking officer	2	1.9%
Hardware technician	2	1.9%
Head, E-banking	1	1%
Internal control officer	1	1%
Head, IT division	1	1%
IT officer	2	1.9%
IT security officer	2	1.9%
JCO	3	2.9%
Junior IT officer	2	1.9%
Manager, Branch business	1	1%
MIS officer	1	1%
Team leader, MIS	1	1%
Network administrator	2	1.9%
Secretary	1	1%

Senior banking operation	2	1.9%
Senior CSO	1	1%
Senior database administrator	3	2.9%
Senior database engineer	1	1%
Senior e-banking officer	1	1%
Senior internal controller	3	2.9%
Senior system administrator	2	1.9%
Senior talent acquisition officer	3	2.9%
System administrator	3	2.9%
Total	103	100%

Appendix D: Cross Tabulation between ISSP Practices and ISSP Attitude

*Certain to follow the organization's ISSP and related guidelines * Following the organization's ISSP is a good idea*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	71.928[a]	16	.000
Likelihood Ratio	44.892	16	.000
Linear-by-Linear Association	24.740	1	.000
N of Valid Cases	100		

*Certain to follow the organization's ISSP and related guidelines * Following the organization's ISSP is a necessary*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	58.824[a]	16	.000
Likelihood Ratio	33.704	16	.006
Linear-by-Linear Association	17.382	1	.000
N of Valid Cases	100		

*Certain to follow the organization's ISSP and related guidelines * Following the organization's ISSP is a beneficiary*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	37.733[a]	16	.002
Likelihood Ratio	26.361	16	.049
Linear-by-Linear Association	11.973	1	.001
N of Valid Cases	100		

*Certain to follow the organization's ISSP and related guidelines * Following the organization's ISSP is pleasant*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	53.216[a]	16	.000
Likelihood Ratio	46.206	16	.000
Linear-by-Linear Association	20.970	1	.000
N of Valid Cases	99		

*Likely to follow the organization's ISSP and related guidelines in the future * Following the organization's ISSP is a good idea*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	74.319[a]	16	.000
Likelihood Ratio	42.806	16	.000
Linear-by-Linear Association	26.782	1	.000
N of Valid Cases	101		

*Likely to follow the organization's ISSP and related guidelines in the future * Following the organization's ISSP is a necessary*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	67.437[a]	16	.000
Likelihood Ratio	38.385	16	.001
Linear-by-Linear Association	28.168	1	.000
N of Valid Cases	101		

*Likely to follow the organization's ISSP and related guidelines in the future * Following the organization's ISSP is a beneficiary*

hi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	69.716[a]	16	.000
Likelihood Ratio	39.589	16	.001
Linear-by-Linear Association	29.050	1	.000
N of Valid Cases	101		

*Likely to follow the organization's ISSP and related guidelines in the future * Following the organization's ISSP is pleasant*

hi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	65.222[a]	16	.000
Likelihood Ratio	42.844	16	.000
Linear-by-Linear Association	21.153	1	.000
N of Valid Cases	100		

*An intention to continue to comply with the organization's ISSP and related procedure and guidelines * Following the organization's ISSP is a good idea*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	99.529[a]	16	.000
Likelihood Ratio	61.964	16	.000
Linear-by-Linear Association	30.239	1	.000
N of Valid Cases	99		

*An intention to continue to comply with the organization's ISSP and related procedure and guidelines * Following the organization's ISSP is a necessary*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	88.118[a]	16	.000
Likelihood Ratio	55.993	16	.000
Linear-by-Linear Association	39.300	1	.000
N of Valid Cases	99		

*An intention to continue to comply with the organization's ISSP and related procedure and guidelines * Following the organization's ISSP is a beneficiary*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	80.130[a]	16	.000
Likelihood Ratio	51.332	16	.000
Linear-by-Linear Association	35.950	1	.000
N of Valid Cases	99		

*An intention to continue to comply with the organization's ISSP and related procedure and guidelines * Following the organization's ISSP is pleasant*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	51.284[a]	16	.000
Likelihood Ratio	38.508	16	.001
Linear-by-Linear Association	26.806	1	.000
N of Valid Cases	98		

*The organization has specific guidelines that describe acceptable use of its IS resources * Following the organization's ISSP is a good idea*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	53.595[a]	16	.000
Likelihood Ratio	39.783	16	.001
Linear-by-Linear Association	18.093	1	.000
N of Valid Cases	101		

*The organization has specific guidelines that describe acceptable use of its IS resources * Following the organization's ISSP is a necessary*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	64.246[a]	16	.000
Likelihood Ratio	44.741	16	.000
Linear-by-Linear Association	16.675	1	.000
N of Valid Cases	101		

*The organization has specific guidelines that describe acceptable use of its IS resources * Following the organization's ISSP is a beneficiary*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	47.982[a]	16	.000
Likelihood Ratio	32.744	16	.008
Linear-by-Linear Association	11.305	1	.001
N of Valid Cases	101		

*The organization has specific guidelines that describe acceptable use of its IS resources * Following the organization's ISSP is pleasant*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	67.027[a]	16	.000
Likelihood Ratio	55.297	16	.000
Linear-by-Linear Association	23.793	1	.000
N of Valid Cases	100		

*The organization has specific guidelines that govern what employees are allowed to do with their computer * Following the organization's ISSP is a good idea*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	35.193[a]	16	.004
Likelihood Ratio	29.879	16	.019
Linear-by-Linear Association	12.259	1	.000
N of Valid Cases	97		

*The organization has specific guidelines that govern what employees are allowed to do with their computer * Following the organization's ISSP is a necessary*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	43.684[a]	16	.000
Likelihood Ratio	27.464	16	.037
Linear-by-Linear Association	9.664	1	.002
N of Valid Cases	97		

*The organization has specific guidelines that govern what employees are allowed to do with thier computer * Following the organization's ISSP is a beneficiary*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	34.304[a]	16	.005
Likelihood Ratio	27.767	16	.034
Linear-by-Linear Association	7.788	1	.005
N of Valid Cases	97		

*The organization has specific guidelines that govern what employees are allowed to do with thier computer * Following the organization's ISSP is pleasant*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	46.830[a]	16	.000
Likelihood Ratio	42.306	16	.000
Linear-by-Linear Association	20.602	1	.000
N of Valid Cases	96		

*The organization has a formal policy that forbids employees from engaging from unhygienic cyber * Following the organization's ISSP is a good idea*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	66.782[a]	16	.000
Likelihood Ratio	45.185	16	.000
Linear-by-Linear Association	14.771	1	.000
N of Valid Cases	97		

*The organization has a formal policy that forbids employees from engaging from unhygienic cyber * Following the organization's ISSP is a necessary*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	63.930[a]	16	.000
Likelihood Ratio	46.690	16	.000
Linear-by-Linear Association	14.732	1	.000
N of Valid Cases	97		

*The organization has a formal policy that forbids employees from engaging from unhygienic cyber * Following the organization's ISSP is a beneficiary*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	51.672[a]	16	.000
Likelihood Ratio	39.897	16	.001
Linear-by-Linear Association	16.244	1	.000
N of Valid Cases	97		

*The organization has a formal policy that forbids employees from engaging from unhygienic cyber * Following the organization's ISSP is pleasant*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	55.987[a]	16	.000
Likelihood Ratio	51.895	16	.000
Linear-by-Linear Association	22.956	1	.000
N of Valid Cases	96		

*The organization has established rules of behavior for use of computer resources and other digital assets * Following the organization's ISSP is a good idea*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	55.011[a]	16	.000
Likelihood Ratio	36.774	16	.002
Linear-by-Linear Association	20.339	1	.000
N of Valid Cases	98		

*The organization has established rules of behavior for use of computer resources and other digital assets * Following the organization's ISSP is a necessary*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	71.280[a]	16	.000
Likelihood Ratio	38.698	16	.001
Linear-by-Linear Association	20.579	1	.000
N of Valid Cases	98		

*The organization has established rules of behavior for use of computer resources and other digital assets * Following the organization's ISSP is a beneficiary*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	44.967[a]	16	.000
Likelihood Ratio	31.825	16	.011
Linear-by-Linear Association	18.635	1	.000
N of Valid Cases	98		

*The organization has established rules of behavior for use of computer resources and other digital assets * Following the organization's ISSP is pleasant*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	64.930[a]	16	.000
Likelihood Ratio	37.298	16	.002
Linear-by-Linear Association	18.620	1	.000
N of Valid Cases	98		

*Having basic knowledge on how to avoid unhygienic cyber practices * Following the organization's ISSP is a good idea*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	21.314[a]	16	.167
Likelihood Ratio	24.989	16	.070
Linear-by-Linear Association	3.747	1	.053
N of Valid Cases	101		

*Having basic knowledge on how to avoid unhygienic cyber practices * Following the organization's ISSP is a necessary*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	27.112[a]	16	.040
Likelihood Ratio	29.865	16	.019
Linear-by-Linear Association	4.827	1	.028
N of Valid Cases	101		

*Having basic knowledge on how to avoid unhygienic cyber practices * Following the organization's ISSP is a beneficiary*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	26.249[a]	16	.051
Likelihood Ratio	27.720	16	.034
Linear-by-Linear Association	1.274	1	.259
N of Valid Cases	101		

*Having basic knowledge on how to avoid unhygienic cyber practices * Following the organization's ISSP is pleasant*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	18.826[a]	16	.278
Likelihood Ratio	19.690	16	.235
Linear-by-Linear Association	.772	1	.379
N of Valid Cases	100		

*Having the skills and expertise to avoid engaging in unhygienic cyber practices * Following the organization's ISSP is a good idea*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	20.942[a]	16	.181
Likelihood Ratio	23.166	16	.109
Linear-by-Linear Association	.303	1	.582
N of Valid Cases	101		

*Having the skills and expertise to avoid engaging in unhygienic cyber practices * Following the organization's ISSP is a necessary*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	26.337[a]	16	.049
Likelihood Ratio	29.287	16	.022
Linear-by-Linear Association	1.780	1	.182
N of Valid Cases	101		

*Having the skills and expertise to avoid engaging in unhygienic cyber practices * Following the organization's ISSP is a beneficiary*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	26.919[a]	16	.042
Likelihood Ratio	28.454	16	.028
Linear-by-Linear Association	.697	1	.404
N of Valid Cases	101		

*Having the skills and expertise to avoid engaging in unhygienic cyber practices * Following the organization's ISSP is pleasant*

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	14.622[a]	16	.552
Likelihood Ratio	17.538	16	.352
Linear-by-Linear Association	.008	1	.927
N of Valid Cases	100		