ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

PROPOSING INFORMATION SECURITY AWARENESS PROGRAM FOR ENAT BANK IN ETHIOPIA

By

MILKYAS BOGALE

JUNE, 2018
ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

PROPOSING INFORMATION SECURITY AWARENESS PROGRAM FOR ENAT BANK IN ETHIOPIA

A Thesis Submitted to 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: MILKYAS BOGALE

Advisor: LEMMA LESSA (PhD)

JUNE 2018

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCE

SCHOOL OF INFORMATION SCIENCE

PROPOSING INFORMATION SECURITY AWARENESS PROGRAM FOR ENAT BANK IN ETHIOPIA

By: Milkyas Bogale

Name and signature of Members of the Examining Board

Lemma Lessa (PhD) Advisor	_____ Signature	_____ Date
Gashaw Kebede (PhD) Examiner	_____ Signature	_____ Date
Workshet Lamenew (PhD) Examiner	_____ Signature	_____ Date

Declaration

I declare that this thesis is a result of my own investigation, except where otherwise stated. I have undertaken the study independently with the guidance and support of my research advisor. Other sources are acknowledged by citations giving explicit references. A list of references is appended. Moreover, this thesis has not previously been accepted for any degree and is not being concurrently submitted in candidature for any degree in any university.

Signature: _____

Milkyas Bogale

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

Advisor's Signature: _____

Lemma Lessa (PhD)

Acknowledgements

First of all I would like to thank the almighty GOD who show me this day and beyond. Next to that, I would like to thank all, more specifically the following persons, for your valuable contribution during this thesis work.

My heartfelt gratitude goes to my Advisor Lemma Lessa (PhD), who also act as a mentor and instructor, for his energetic and motivating advices, invaluable support and very important comments.

I am also thankful to my parents Bogale and Yebirgual, my brothers Bisrat and Fisseha, and Aregash for your continual love and support that make me who I am today.

I would like to thank my fiancée Samri for your love and support.

I cannot thank enough all Enat Bank S.C managements and employees that directly or indirectly participate in the research especially ISD department staffs. This paper will not be complete without you.

Finally, my families, friends, classmates and colleagues who support me indefinitely from start to finish especially Abrish for opening your door, Shife for your kind support, Misir for your advices and genuine feedbacks, Jossy and my cousin Dr. Milli for your dedication and commitment, and giving me feedbacks.

Abstract

Information has become lifeblood asset of organizations and protection of these assets became one of the major aspects that organizations have to deal with. The issue is too serious when it comes to financial institutions due to their sensitivity to information security attacks. Enat Bank is one of such organizations, where data protection and corporate security are a serious concern. While huge amounts of money and time are invested in technical solutions like deploying intrusion-detection systems, organizations often pay too little attention to the most important and vulnerable security component which is the human part and more importantly the insider threats. Extant literature reveal that employees are the subject and objective for most information security attacks. This study, tried to fill this gap by proposing employees information security awareness program based on the Bank context by reviewing existing information security awareness programs and the current practice of information security awareness in Enat Bank.

In this regard, the researcher followed a quantitative research approach with case study method to achieve the research intended goals. Two types of questionnaires were distributed one for IT technical staffs and other for all other staffs of the bank to collect the required data. The data analysis was taken place by using SPSSv21 frequency analysis technique.

Findings of the study showed that the information security awareness level of Enat Bank employees is unsatisfactory. Hence, the researcher proposed a program that will assist the Bank in terms of creating information security awareness and good practices to its employees to strengthen its security posture by mitigating vulnerabilities for computer attacks. Besides an implementation strategy is also proposed to help the organization to put the program on the ground. One of the best ways to make sure employees will not make costly errors in regard to information security is to institute organization-wide security awareness initiatives that include, but not limited to face-to-face and multi-media based awareness, techniques that can be fairly inexpensive to implement such as posters, do and don't lists and warning banners. These methods can help ensure employees have a solid understanding of the organization security policy, procedure and best practices. Finally, recommendations are given for the bank to act in short and long-term basis to improve the information security awareness of its employees and in turn improve better information security practice in the bank.

Keywords: Information Security Policy, Security Awareness Program, Information Systems Security

Table of Contents

List of Tables

List of Figures

List of Acronyms

ARP	Address Resolution Protocol
CBS	CORE Banking System
CIO	Chief Information Officer
CIA	Confidentiality, Integrity and Availability
CORE	Centralized Online Real-time Exchange
DHCP	Dynamic Host Configuration Protocol
GPS	Global Positioning System
ISAP	Information Security Awareness Program
ISF	Information Security Forum
ISM	Information Security Management
ISP	Information Security Policy
IS	Information System
IT	Information Technology
ISO/IEC	International Organization for Standardization/International Electro technical Commission
IP	Internet Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
MAC	Media Access Control
MD5	Message Digest 5 Algorithm
NBE	National Bank of Ethiopia
NIST	National Institute of Standards and Technology
OSI	Open Source Interconnection
PCI-DSS	Payment Card Industry-Data Security Standard
RADIUS	Remote Authentication Dial-In User Service
TACACS/TACACS+	Terminal Access Controller Access Control System
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

CHAPTER ONE

INTRODUCTION

This chapter introduces the background to the research, statement of the problem, research questions and the objectives of the research. Furthermore, the chapter describes the significance of the study and the scope of the research.

1.1 Background to the research

Nowadays, Information Technology (IT) has been widely applied in every aspect of our day to day life in business, government, education etc. With our increasing dependency on information technology, the consequences of computer crime can be extremely serious (Mahncke, McDermid, & Williams, 2009).

According to Al-Alawi, Al-Kandari and Abdel-Razek (2016), information is considered as lifeblood and a backbone for most institutions, and an invaluable asset in today's IT enabled world. Maintaining information systems security among the employees in the form of information systems security awareness, is extremely important to protect the institutions' information systems. Information security awareness is used to refer to a state where users in an organization are aware of and ideally committed to their security mission, often expressed in end-user security guidelines (Siponen, Pahnila, & Mahmood, 2010). Siponen et al., (2010) further stated information security awareness is a serious business as information security techniques or procedures can be misused, misinterpreted or not used by end-users, thereby losing their real usefulness.

Although security awareness related matters range from simple information security guidelines to well-developed information security education programs in nearly all organizations in the age of the information society, their nature is not well understood, resulting for example, in ineffectiveness of security guidelines or programs in practice (Siponen, 2000). The failure of an organization's own employees to adhere to their information security policies constitutes a key threat (Puhakainen & Siponen, 2010); and to ensure that employees follow their organizations' security policies, developers have proposed several policy-compliance measures (Siponen et al., 2010).

According to Symantec Internet Security Threat Report (2016), over half a billion personal information records were stolen or lost in 2015. Among this loss the proportion of incidents involving insider theft grew from a point that was less than 1 percent in 2014 to 10 percent in

2015. Moreover the report indicates even though companies' chose not to report the true number of records exposed, hundreds of millions more people may have been compromised.

Enat Bank SC is a privately owned commercial bank established in 2011 in accordance with the "licensing and supervision of banking business proclamation No. 592/2008" of Ethiopia to undertake commercial banking activities. The Bank obtained its license from National Bank of Ethiopia (NBE) on 14 November 2012 and started its business activities on 05 March 2013. The Bank's mission is to remain true to its name and set a trend in the provision of best quality banking services with a special focus on the needs of women and play a catalytic role in stimulating social, economic developments and in creating shareholders' value. And with a vision to become a world-class bank mainly by leveraging women's capabilities according to the company profile. Currently the Bank has an estimated 4.84 billion birr total assets and a subscribed capital of 850 million birr. The Bank has collected a total deposit of 3.68 billion birr operating with 35 branches all over Ethiopia as of June 2017 (Enat Bank Annual Report, 2017).

Enat Bank is one example of such organizations where, as a financial institution securing information is not a choice rather a matter of existence for the business. If information security incident occurs, not only affect the banks huge investment but also its trustworthiness to its customers. One aspect of achieving this is by creating employees awareness to information security.

1.2 Statement of the problem

Information has become lifeblood asset of organizations and the protection of these assets became one of the major aspects that management has to deal with. The need for secured and protected information system asset in any organization has become a very important component. Banks are one of such organizations, where data protection and corporate security are a serious concern (Tse, et al., 2013).

While huge amounts of money and time are invested in technical solutions such as intrusion-detection systems, firewalls, antimalware etc., organizations often pay too little attention to the most important and vulnerable security component which is the human part (Alageel, 2003). Amare (2015) explains that banks cannot rely on just the technologies they have today as people are the weakest links. In order to cope with the increase in information security threats, not only technical solutions such as anti-virus software tools, but also information management methods and policies have been proposed (Alageel, 2003; Amare, 2015).

However, Siponen (2000) pointed employees rarely comply with these information security procedures and techniques, placing the organizations' assets and business in danger. According to PwC Global State of Information Security Survey (2014), employees are the most offenders of security incidents. Effective information security, therefore, requires employees to comply with information security policies and guidelines.

Da Veiga (2015) explains that information security awareness is required in organizations where employees process information in line with its confidentiality, integrity and availability requirements. Information security policy serves as a critical cornerstone in guiding employee behavior to direct the protection of information. Employees must be aware of and understand the information security policy requirements they have to follow in order to process information securely (Gundu & Flowerday, 2013). Tebkew (2013) added the lack of employees' information security awareness is one of the main challenges in designing and implementing information security management system.

Extant literature reveal that most information security attacks are based on employees, employees are the subject and objective for most information security attacks. As Connolly, Lang and Tygar (2017), humans are the weakest link in the information security chain and the root cause of numerous security incidents in organizations. If employees are not aware on information security, it will be difficult for them to protect the corporate data at the same time themselves from any kind of security attacks. Kruger, Drevin and Steyn (2006) similarly stated that the involvement of humans in information security is of equal importance and many examples of security issues such as phishing and social engineering where humans are involved exist. Many successful computer crimes could have been prevented if employees were aware of information security (Negussie, 2015). These imply employees must be aware of information security within their organization. Information security awareness programs must be established in line with banks information security policies and relevant measures (Abdyli, 2014). Abdyli (2014) further mentioned that employees training and education to build a secured culture in banks have influence on their engagement to security policies.

Woretaw and Lessa (2012) explained information security awareness in the Ethiopian banking sector is unsatisfactory. Though securing the information assets of banks nowadays is becoming a matter of existence for the business, there are scarce number of similar studies in information security awareness and adherence in Ethiopian banking industry. Although there are standards and other frameworks designed to assess information security awareness and adherence in organizations, existing standard can't fit to all organizational contexts. Rather,

contextual factors (organizational, national, environmental, etc.) affect the design of such programs. According to Alnatheer and Nelson (2009) major international Information security standards are written from a Western perspective, without knowing how applicable security concepts and practices are to other cultures, which has different social, organizational, and security cultures. Organizations should never randomly choose their information security awareness program, instead their program should be based on their specific need (Xiong, 2011). Choosing appropriate form of delivery method also should be based on the organization work processes and management system (Xiong, 2011). This research, therefore, tries to fill this gap by proposing employees information security awareness program based on Enat Bank context which enhance the existing knowledge. The proposed program, can also be used as a guideline by the Bank to conduct information security awareness program for its employees to strengthen the Bank's security posture.

1.3 Research questions

- What is the current information security awareness creation practice in Enat Bank?
- What should the topics of an information security awareness program for Enat Bank be?
- How should the information security awareness program be organized to deliver the necessary information to Enat Bank employees?

1.4 Objectives

The general objective of the study is to propose information security awareness program for Enat Bank.

Specific objectives include to:

- review existing information security awareness programs.
- review contents that needs to be included in the program.
- review information security awareness delivery techniques.

1.5 Significance of the study

The study has a significant contribution for both academic researchers and practitioners. Academic researchers will be benefited from the theoretical contribution since it tries to fill the existing literature gap particularly on information security awareness for Ethiopian bank context. Enat Bank decision makers are the primary practitioners that will use the proposed

program as a guideline to increase their employees' awareness to information security and strengthen the bank security posture.

It also serve as a benchmark for practitioners and researchers who want to conduct more research in information security awareness area in Ethiopian banks.

1.6 Scope of the study

The study assess the current practice of information security awareness in Enat Bank using existing international security standards, and propose a program towards information security awareness. The study was limited to awareness aspect of information security. The study is also limited to conduct information security awareness on sample Enat Bank's Addis Ababa city and outlying branches.

1.7 Organization of the thesis

The paper is organized in six chapters. They are;

Chapter 1: This chapter provides an introductory and background need for employees' information security awareness especially for financial institutions. It also includes the statement of the problem, research question, objective, significance and scope of the study.

Chapter 2: In this chapter literature review of information security, related concepts and models, and directly related works have been discussed.

Chapter 3: This chapter describes the research design and methodology used in order to conduct the research. Such as the approach and method used, the population and research area, the sampling technique, the data collection tools, analysis, and validation are discussed.

Chapter 4: This chapter present the findings and data analysis based on the information collected.

Chapter 5: This chapter presents the proposed information security awareness program for the Bank based on the findings of analysis of the research and reviewing existing security awareness programs. Furthermore, the chapter proposes possible delivery techniques for the program.

Chapter 6: This chapter provides summary and recommendation based on the findings.

CHAPTER TWO

LITERATURE REVIEW AND RELATED WORKS

2.1 Literature review

2.1.1. Information security

Information is one of a financial institution's most important assets. Protection of information assets is necessary to establish and maintain trust between the financial institution and its customers, maintain compliance with the law, and protect the reputation of the institution (Council, F.F.I.E, 2006). Similarly Tse, et al. (2013) stated banking systems contain a wealth of private financial information. These data are used as a shared secret between banks and their customers. As access to computer stored data has increased, information security has become respectively important. McGlasson (2007) stated that the most important part of a good bank IT security infrastructure is information security. In order to protect the information assets and prevent fraud activities, the banking industries should design and implement information security strategies. For this kind of scenarios McGlasson (2007) suggested two solutions, the first is establishing information security governance framework and the second is organizing information security awareness training program.

Security of the information assets is a requirement for all types of organization, whether to protect the business or to meet legal or regulatory requirement as organizations are totally dependent on their IT systems to capture, store, process and distribute company information (Jones, 2010). For this, information security is and has always been the discipline to mitigate risks impacting on the confidentiality, integrity and availability of a company's IT resources (Von Solms, 2006).

According to Nieles, Dempsey and Pillitteri (2017) information Security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability. Information security is the process by which an organization protects and secures its systems, media, and facilities that process and maintain information vital to its operations (Council, F.F.I.E, 2006). It is simply the process of keeping information secure protecting its availability, integrity, and privacy. Similarly Abdyli (2014) stated the most well-known theoretical model which treat information security is the CIA triad or CIA triangle as shown in Figure 1.

Figure 1 CIA triad

Source: Abdyli (2014).

According to Abdyli (2014) information security includes three aspects;

- Confidentiality – is described as the protection of information, application, system and network from unapproved access. It relies to the safeguard of information by illegal admission regardless in what form is stored.
- Integrity – is described as the protection of information, application, system and network from unauthorized change, be intentional or accidental.
- Availability – is the affirmation that information, assets and resources are available only to those authorized.

Effective Information Security incorporates security products, technologies, policies and procedures. Products such as firewalls, intrusion detection systems, and vulnerability scanners alone are not sufficient to provide effective information security.

Most of the research done on corporate that deals with security in Information Systems (IS) were focused mainly on the technical aspect of IT such as firewalls and anti-virus software which rely more on technology than the employees using the systems. Researchers are now starting to realize that the human interaction with the IS of the firm is just as important as the technical, and that information security cannot be achieved solely through these technological tools (Herath & Rao, 2009). Many researchers now believe the biggest threat to information security remains internal (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009), (Vroom & Von Solms, 2004), and (Kankanhalli, Teo, Tan, & Wei, 2003). Swartz (2007) outlined several cases in which employees stole data while still working for their company, yet the majority of

employee security breaches occur accidently or unintentionally (Keller, Powell, Horstmann, Predmore, & Crawford, 2005) and (Sumner, 2009). There are currently many theories on the best way to combat these issues. These range from the importance of cultivating an information security policy to significance of employee training and awareness.

According to Gebrehawariat (2017) a successful organization should have the following multiple layers of security in place for the protection of its operations.

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

Gebrehawariat (2017) added this is achieved through the application of policy, education, training and awareness, and technology.

2.1.2. Information security policy

Management of information requires a working set of procedures, guidelines and best practices that provide guidance and direction with regards to security. An information security policy is defined as an aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information (Nieles, Dempsey, & Pillitteri, 2017). Nieles et al., (2017) further stated in making these decisions, managers face difficult decisions with regard to resource allocation, competing objectives, and organizational strategy, all of which relate to protecting technical and information resources as well as guiding employee behavior. Information security policy is a well-defined and documented set of guidelines that describes how an organization manages, protects its information assets and makes future decisions about its information systems security infrastructure. Security procedures document precisely how to accomplish a specific task.

According to Diver (2007) a security policy should fulfil many purposes. It should:

- Protect people and information
- Set the rules for expected behavior by users, system administrators, management, and security personnel
- Authorize security personnel to monitor, enquiry, and investigate
- Define and authorize the consequences of violation
- Define the company consensus baseline posture on security
- Help minimize risk
- Help track compliance with regulations and legislation

Diver (2007) stated policies must be useable, workable and realistic. In order to achieve this, it is essential to involve and get commitment from major players in policy development and support such as senior management, audit and legal as well as from those people who will have to use the policies as part of the daily work. Another important element to achieve this is to communicate the importance and usefulness of policies to those who have to live by them.

According to Instant Security Policy (2008) a security policy must specifically accomplish three objectives. These are allow for the confidentiality and privacy of a company's information, provide protection for the integrity of a company's information and provide for the availability of a company's information. This is commonly referred to as the CIA Triad of confidentiality, integrity, and availability, an approach which is shared by all major security regulations and standards.

2.1.3. Information security in Ethiopia

Due to technology transformation in today's Ethiopian banking business, information security has become one of the key points for customer attraction, retention, and profitability (Negussie, 2015). Currently, banking sector in Ethiopia is one of the rapidly growing sectors of the country's economy. Tebkew (2013) in his study stated that in order to get national and international competitive advantages, information must be properly managed from its creation up to disposal. However, from information security aspect, each Ethiopian bank has applied some component of an information security policy such as: acceptable use policy of IT equipment, backup policy, anti-malware… etc. The scholar further stated Ethiopian banks have invested on IT security devices as part of their CORE Banking System (CBS) project. However, managing these IT security devices may be challenging since they do not have

overall or comprehensive Information Security Management (ISM) framework which serve as a guide to develop and implement their own information security policy based on their own requirement in line with National Bank of Ethiopia's (NBE) directives. On the other hand, Tebkew (2013) discussed Ethiopian banking business competition has motivated the advancement of services enabled by IT which in turn increased the information security risk. These threats to information and information systems can include intentional attacks, environmental disruptions and human/machine errors, and result in great harm to the national and financial security interests of the country since Ethiopian IT capabilities are still in a developing phase and are immature compared with leading western countries which are technically developed.

Negussie (2015) stated information security issue is not only a problem that technology can address alone but also a problem of a management to solve. Legal frameworks in the form of policy and standards are the primary prerequisites to establish efficient and reliable security governance systems in Ethiopian banks. Negussie (2015) further stated in almost all Ethiopian banks, management does not give that much emphasis to information security, for implementing a good and effective information security governance management commitment and support is highly mandatory. There are challenges to formulating, implementing and compliance of Information Security Policy (ISP) in Ethiopian banks such as management commitment and support due to lack of awareness, lack of a special training to information security personnel, complexity of the subject matter, and resistance with employees to comply with ISP and lack ongoing employees' awareness on security issues (Negussie, 2015). Nowadays, NBE is forcing each bank to recruit dedicated information security personnel so that he/she directly engage in the process of protecting the organization's information assets. However, since information security industry needs such a huge initial infrastructure investment and personnel technical efficiency, banks face similar challenges when trying to secure their organization.

Woretaw and Lessa (2012) explained the level of information security awareness in Ethiopian banking sector is unsatisfactory. One of the greatest threats to information security could actually come from within a company or organization. According to Amare (2015) most organizations are not even aware of insider threat problem. Inside attacks have been noted to be some of the most dangerous since these people are already quite familiar with the infrastructure. It is not always dissatisfied workers and corporate spies who are a threat. Most of the times, it is the non-malicious, uninformed employee (Brodie & Wanner, 2009). The

majority of insiders do not consider the consequences of their actions when undertaking an attack. Educating employees about the consequences of such attacks from the perspective of both the business and the wrongdoer may act as a preventive to such attacks. When employees learn to behave securely through training, these beliefs will influence attitude and ultimately behavior.

2.1.4. Information security in Enat Bank

Enat bank S.C started operating on March 2013. As one of the youngest banks in formation, the number of branches are less compared to the industry giants. However, this also helps it to build its IT infrastructure using a state-of-the-art technology such as a datacenter using virtualization, servers, and other network equipment (Enat Bank Annual Report, 2017).

As most organizations, Enat Bank S.C has invested huge amounts of money and time in technical solutions such as firewalls, antivirus, intrusion-prevention system, etc., However, as (Alageel, 2003; Amare, 2015) stated organizations often pay too little attention to the most important and vulnerable security component, the human part. Enat Bank is one example of such organizations which need to implement technical as well as human aspects when it comes to securing the organization assets. The reason is humans are the weakest link when it comes to security (Alageel, 2003; Amare, 2015; Siponen, 2000). The Bank has developed an information security policy which is a good start on going forward to tell staffs what is right and wrong when it comes to securing the organization's assets. There is a saying "a chain is only as strong as its weakest link" meaning an organization especially a process or a business is only as strong or powerful as its weakest person. One staff is enough to compromise systems or even to have a security breach without knowing the consequences because of the lack of awareness to information security.

2.1.5. Information security awareness

Awareness is something that happens in one's mind, paying attention to certain issues, knowing about and understanding certain things (Haeussinger, 2015). Several authors defined information security awareness in several ways such as in NIST (2003) the purpose of awareness presentations is simply to focus attention on security. In ISF (2007) security awareness is defined as the extent to which staff understand the importance of information security, the level of security required by the organization and their individual security responsibilities, and act accordingly. According to Siponen (2000), the term information security awareness is used to refer to a state where users in an organization are ideally

committed to their end-user security guidelines. It is very important as information security techniques or procedures can be misused, misinterpreted or not used by end-users, thereby losing their real usefulness. These multiple definitions of information security awareness help us to understand the concept behind this crucial matter.

Nowadays, computer misuse and illegal conducts are increasing with the growth of computerization. In order to let the staff familiar with the complicated information security issues, Payne (2003) suggested that the corporations should also deliver an information security awareness and training program for all levels of staff members in an efficient and effective manner. Payne (2003) further stated that there were several ideas on delivering the awareness and training, e.g. conducting classroom sessions, seminars and workshop, distributing information security handbooks, creating online quizzes or games. Meanwhile, Chen et al., (2006) suggested that the training could be delivered using an e-learning platform. The system would provide rich and interactive content via internet and intranet. The content could be provided according to target groups and according to their job nature or expertise. Unlike traditional classroom training, the system would emphasize more on employee involvement and effective communication instead of one-way content delivery (Chen et al., 2006).

According to Hagen, Albrechtsen and Hovden (2008) the creation and maintenance of security awareness include both individual and collective activities that is education and awareness-raising initiatives, e.g. emails, pamphlets, mouse pads, formal presentations, and discussion groups. Many researchers now believe that employee awareness is one of the best ways to protect a company's data (D'Aubeterre, Singh, & Iyer, 2008) and (Chang & Yeh, 2006). In fact, empirical research found that awareness creation is the most effective information security measure (Hagen, et al., 2008). Security awareness and training programs should aim to make employees recognize the legitimacy of information security policy to safeguard the firm (Son, 2011). Therefore it is vital that organizations have a security awareness program in place to ensure employees are aware of the importance of protecting sensitive information, what they should do to handle information securely, and the risks of mishandling information (PCI Security Standards Council, 2014).

2.1.6. Information security awareness programs

An effective information security program cannot be implemented without implementing an employee awareness and training program to address policy, procedures, and tools (Peltier, 2005). Below are some examples of security awareness programs.

2.1.6.1. National Institute of Standards and Technology-NIST

NIST which is based in the United States, is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all organization operations and assets.

NIST Special Publication 800-50 NIST (2003), titled "Building an Information Technology Security Awareness and Training Program", provides guidance for building an effective information technology security program. The program stated senior managements, Chief Information Officers (CIO), program officials, and IT security managers have key responsibilities to ensure that an effective program is established organization wide, not forgetting everyone has a role to play in the success of a security awareness and training program. The scope and content of the program must be tied to existing security program directives and established organization security policy. Within organization IT security program policy, there must exist clear requirements for the awareness and training program.

The document identifies four critical steps in the life cycle of an IT security awareness and training program:

- Awareness and Training Program Design: In this step, an organization wide needs assessment is conducted and a training strategy is developed and approved. This strategic planning document identifies implementation tasks to be performed in support of established organization security training goals.
- Awareness and Training Material Development: This step focuses on available training sources, scope, content, and development of training material, including solicitation of contractor assistance if needed.
- Program Implementation: This step addresses effective communication and roll out of the awareness and training program. It also addresses options for delivery of awareness and training material (web-based, distance learning, video, on-site, etc.).

- Post-Implementation: This step gives guidance on keeping the program current and monitoring its effectiveness. Effective feedback methods are described (surveys, focus groups, benchmarking, etc.).

The document also discussed three models used in managing a security training function.

- Centralized: All responsibility resides with a central authority (e.g., CIO and IT security program manager).
- Partially Decentralized: Training policy and strategy lie with a central authority, but implementation responsibilities are distributed.
- Fully Decentralized: Only policy development resides with a central authority, and all other responsibilities are delegated to individual organization components.

The type of model considered should be based on an understanding and assessment of budget and other resource allocation, organization size, consistency of mission, and geographic dispersion of the organization (NIST, 2003).

2.1.6.2. International Organization for Standardization ISO 27001:2013

ISO/IEC (2013) (the International Organization for Standardization) and IEC (the International Electro technical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity.

The objective of the standard is to provide requirements for establishing, implementing, maintaining and continuously improving an information security management system. The design and implementation of an organization's information security management is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. The standard stated it is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization. The standard further stated any personnel doing work under the organization's control shall be aware of the information security policy, their

contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and the implications of not conforming with the information security management system requirements.

2.1.6.3. SANS Institute

SANS Institute was created as cooperative research and education organization that offers programs to over 165,000 security professionals. It is one of the trusted and largest source for information security training and security certification. The institute offers trainings designed to help anyone, from auditors to CIOs to defend systems and networks against most dangerous threats according to their official website. Their security awareness program provides organizations with a complete and comprehensive security awareness solution like phishing training, end-user, engineer, developer and healthcare, enabling them to easily and effectively manage cyber security risks (SANS Institute, 2018).

SANS (SysAdmin, Audit, Network, Security) offer training through several delivery methods - live & virtual, classroom-style, online at your own pace or webcast with live instruction, guided study with a local mentor. Its computer security courses are developed by industry leaders in numerous fields including cyber security training, network security, forensics, audit, security leadership, and application security (SANS Institute, 2018).

2.2 Related works

Author	Objective	Key Finding
(Abdyli, 2014)	examine the level of technical observation on information security with a special focus on information security policies	Identified banking sector in the Republic of Kosovo is ready to implement the information security policies
(Alageel, 2003)	Research various prominent computer security training programs information assurance training and education	developed an information security awareness training program for the organization
(Alnatheer & Nelson, 2009)	to identify issues and factors that assist the implementation and the adoption of IS culture and practices within the Saudi environment	proposed a framework for understanding information security culture and practices in the Saudi context
(Amare, 2015)	to examine the insider threat of the Ethiopian banking industry	identified insider threat and motivations within the Ethiopian banking industry, recommends best practices to mitigate those insiders malicious activities within the Ethiopian banking sectors
(Connolly, Lang, & Tygar, 2017)	investigate how procedural security countermeasures tend to affect employee security behavior	indicated that procedural security countermeasures tend to increase information security awareness, which, in turn, has a tendency to encourage compliant behavior
(Da Veiga, 2015)	To examine the level of information security culture between employees who had read the information security policy and employees who had not read the policy	provided statistical evidence that reading the information security policy contributes to influencing the information security culture positively

(Durmus, 2014)	to outline the awareness level of internet users and IT security personnel in public institutions	- identified that absence of security measures has caused some vulnerabilities in organization network - propose participants with relative website and a suggestion document
(Gundu & Flowerday, 2013)	introduce an information security awareness process, which included behavioral intention models based on three persuasive theories; the Theory of Reasoned Action, the Protection Motivation Theory and the Behaviorism Theory	showed that information security awareness levels greatly influence behavioral intentions
(Kruger, Drevin, & Steyn, 2006)	to describes a suggested framework that may assist management of evaluating ICT security awareness	proposed a framework for evaluating ICT security awareness
(Negussie, 2015)	to assess information security and ISP practices, and to identify the challenges and prospects of information security policy in the Ethiopian banking industry	proposed recommendations in formulating and implementing ISP
(Siponen, 2000)	to construct a conceptual foundation for information systems/organizational security awareness	a theoretical framework and selected current methods for increasing awareness
(Tebkew, 2013)	to propose and develop information security management framework which will work in banking industry in Ethiopia	developed information security management framework for the bank

(Tse, et al., 2013)	to evaluate current information security practices in the banking industry and assess the information security awareness level for the employees in the industry	suggested that IT security education should be made to different level of staffs such as executives, professional and general staffs
(Woretaw & Lessa, 2012)	to assess the current information security culture and identify key problems	recommended measures that can be implemented by practitioners to enhance the information security culture in the banking sector in Ethiopia
(Xiong, 2011)	building a program to increase information security awareness for employees	proposed training curriculums of an information security awareness program for the organization

2.3 Summary

It is a must for the banking industry to pay more attention to the information security issues within the organization nowadays. The banks should establish information security governance framework and organize information security awareness program.

According to NIST (2003), a strong IT security program cannot be put in place without significant attention given to training organization IT users on security policy, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to secure IT resources. In addition, those in an organization who manage the IT infrastructure need to have the necessary skills to carry out their assigned duties effectively. Failure to give attention to the area of security training puts an enterprise at great risk because security of organization resources is as much a human issue as it is a technology issue.

Existing security frameworks and awareness programs are contextual and are not customized for Ethiopia. Contextual factors such as organizational, national and environmental affect the design of such programs. There is also a local research gap in this area.

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

This chapter discusses the research design and techniques used to answer the research questions. Hence; research approach and method, research area and population, sampling technique data collection instrument, analysis, validity and reliability are discussed.

3.1 Research design

Research design is the conceptual structure within which research is conducted (Kothari, 2004). Accordingly, the researcher of this study design arrangements as follows;

3.1.1 Research approach and method

Research approach is a plan and procedure for research that range the steps from broad assumptions to detailed methods of data collection, analysis, and interpretation (Creswell, 2013). The two basic approaches to research are quantitative and qualitative, not forgetting a mixture of both. Quantitative approach involves the generation of data in quantitative form which can be subjected to rigorous quantitative analysis in a formal and rigid fashion (Kothari, 2004). It generates statistics through the use of large-scale survey research, using methods such as questionnaires and structured interviews. Whereas qualitative approach tries to explore attitudes, behavior and experiences through such methods as interviews or focus groups (Dawson, 2002). Qualitative approach also attempts to get an in depth opinion from participants. The researcher used quantitative research approach to express employees' awareness level in terms of quantity. The researcher also used a case study also known as a method for in depth study. "A case study method is a careful and complete observation of an individual or a situation or an institution is done; efforts are made to study each and every aspect of the concerning unit in minute details and then from case data generalizations and inferences are drawn" (Kothari, 2004).

3.1.2 Research area and population

The study was conducted on employees of Enat Bank located in different regions across the country. The target population were all employees of Enat Bank that have access to a computer system from junior levels to executives of head office and branches.

3.1.3 Sample

Sampling is a process of choosing a smaller, more manageable number of people to take part in a research. For most researches, unless you have a huge budget, limitless timescale and large team of interviewers, it will be difficult to contact to every person within your research population (Dawson, 2002).

The researcher used stratified random sampling technique to select participant employees from different branches since the target population is heterogeneous in terms of such as awareness, familiarity and usage of IT, and related contexts. Stratified sampling is a type of probability sampling where if a population from which a sample is to be drawn does not constitute a homogeneous group (Kothari, 2004). Under stratified sampling the population is divided into several sub-populations that are individually more homogeneous than the total population, called strata and then we select items from each stratum to constitute a sample. Employees of branches found in Addis Ababa, as a capital city, are better exposed to IT. They are more or less better aware and familiar, easily adopt and practice information technologies compared to employees of outlying branches since they get frequent interaction with the Bank IT personnel's which are located in the same city. The number of branches found in Addis Ababa are also far more than that of the outlying cities. Most of the outlying branches are newly opened which lacks adequate use of the technology unlike Addis Ababa branches employees. Accordingly, the researcher used two strata, Addis Ababa and outlying branches.

For respondents selection the researcher used simple random sampling to give equal probability to each employees of the selected branches. Simple random sampling is a type of probability sampling, which gives each element in the population an equal probability of getting into the sample and all choices are independent of one another (Dawson, 2002).

Yamane (1973) provides a simplified formula to calculate sample sizes that can be presented as:

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

Where n is the sample size, N is the population size, and e is the level of precision. The researcher used Yamane's simplified formula for proportions. When this formula is applied with the total population of 402 and a precision level 0.05 we get the sample size of 201. The

size of employees in Addis Ababa and outlying branches is 313 and 89 respectively. The researcher followed the method of proportional allocation under which the sizes of the samples from the different strata are kept proportional to the sizes of the strata. Accordingly, if *Pi* represents the proportion of population included in stratum *i*, and *n* represents the total sample size, the number of elements selected from stratum *i* is ***n.Pi*** (Kothari, 2004). And *Pi* is calculated as *Si*/*N* where *Si* is the size of stratum *i* and *N* is the total population. Accordingly, when we substitute the numbers in the formula the sample size for Addis Ababa stratum is 157 and for outlying branches stratum 44.

3.2 Research methodology

3.2.1 Data collection tools

During the research, both primary and secondary data were collected. Primary data are collected fresh and for the first time and thus happen to be original in character. On the other hand, secondary data are collected by someone and which have been passed through the statistical process (Dawson, 2002). During the study, primary data were collected using a closed-ended. A closed-ended questionnaire is used to generate statistics in quantitative research (Dawson, 2002). A secondary data is collected by analyzing the bank's reputable documents and publications about employees' information security awareness, and by analyzing existing information security awareness programs. 210 questionnaires were distributed to respondents however only 180 questionnaires were returned. The questionnaire was adapted from Durmus (2014) and slightly modified to match the context. The questionnaire had two categories general and technical. The general category again had seven chapters namely 'Demographic Feature', 'Security Incident and Reporting', 'E-mail Security', 'Safely Use of Internet and Computer', 'Threats and Preventive Measures', 'Password Management and Security', and 'Information Security Terms and Social Engineering'. These chapters tries to assess the end users awareness level and identify gaps that needs to be filled with the appropriate measures. The technical category also had ten chapters namely 'Demographic Features', 'Security Standards, Procedures and Training', 'Firewall, IPS, Management, Penetration and Traffic Control', 'Wireless Network Security', 'Application Layer Security', 'Transport Layer Security', 'Network Layer Security', 'Data Link Layer Security', 'Physical Layer Security' and 'End Point Security'. Here, as the name implies it focuses on technical matters and was distributed to the Bank's technical staffs to assess their awareness and review their current practices.

3.2.2 Data analysis tools and techniques

Analysis may be categorized as descriptive and inferential. Inferential analysis also known as statistical analysis is concerned with the estimation of population parameters, and the testing of statistical hypotheses (Kothari, 2004). Whereas descriptive analysis is largely the study of distributions of one or more variables. It concerns the development of certain indices from the raw data. The researcher of this study used descriptive analysis. The collected data was edited, coded and classified using IBM SPSS tool since, SPSS provides better results as it reduce errors and make the data analysis task easier by eliminating hours of tedious data management and presentation. Tables has been used for data presentation as tables are very useful to summarize ideas. Frequency analysis was used for data analysis and presented in table format including frequencies and percentage.

3.2.3 Validity and reliability

The questionnaire was piloted on sample of intended respondents for easy understanding and ambiguity check. After taking their feedback and made correction, the improved questionnaire was distributed from executives to the junior level staffs of the given branches. The researcher used Cronbach's alpha value from SPSS tool as a measure of internal consistency or reliability and an acceptable (0.74) CA has been found. In order to strengthen the reliability of data collected by using questionnaires, the researcher also reviewed information security awareness documents and related policies and procedures.

3.3 Ethical concerns

A support letter written from the university to do the study is used to contact Enat Bank administration. The data collected from the respondents is used for this study only. Their identity never been exposed to third party by any means, and handled in a professional manner.

CHAPTER FOUR

PRESENTATION AND ANALYSIS

This chapter describes the findings and discusses the results. General category and technical category questionnaires are presented in section using frequency analysis test in SPSS v21 tool.

4.1 General category result

A total of 198 questionnaires were distributed in person and using file sharing software for the end users however due to different reasons such as unwillingness of respondents only 168 were responded. The general category questionnaire is categorized into seven sections. These are demographic feature, security incident and reporting, e-mail security, safely use of internet and computer, threats and preventive measures, password management and security, and information security terms and social engineering. The data were analyzed using frequency analysis. The presentations and findings are as follows.

4.1.1 Demographic feature

Demographic characteristics of the respondents that contain gender, age, academic qualification, job category and work experience are analyzed as follows in Table 1.

Table 1 Frequency analysis of General category demographic features

Question	Option	Frequency	Percent
Q1. Gender	a. Male b. Female	73 87	45.6 54.4
Q2. Age	a. 18- 24 b. 25- 34 c. 35- 44 d. 45- 54	23 121 22 1	13.8 72.5 13.2 0.6
Q3. Qualification	a. Diploma/Level IV b. BA/BSc c. MBA/MA/MSc	5 128 33	3.0 77.1 19.9
Q4. Job Category	a. Management level b. Senior level c. Officer level d. Junior level	24 65 51 22	14.8 40.1 31.5 13.6
Q5.Work experience	a. 0-1 year b. 1-3 years c. 3-5 years d. 5-10years e. Above 10 years	8 55 35 44 24	4.8 33.1 21.1 26.5 14.5

When we see the gender distribution among the respondents, females take 54.4% whereas males got 45.6%. This shows female staff participants are 8.8% greater than male staff participants. Regards the age distribution, staffs whose age range are [18-24] and [35-44] covers 13.8% and 13.2% respectively next to the age range [25-34] which covers 72.5% of the total participants. The academic qualification of respondents lays 77.1% on undergraduate degree 19% postgraduate degree and 3% college diploma in descending order. Among the respondents senior level staffs are covering the highest percentage of 40.1%, 31.5% officer level staffs, 14.8% management and 13.6% are junior level. Employees work experience ratio is 33.1% for [1-3] years of experience being the highest followed by 26.5% [5-10] years of experience and 21.1% [3-5] years of experience respectively. The least participants about 5% are employees which have less than one year of work experience.

4.1.2 Security incident and reporting

In the second section respondents' internet usage and time spent on it, their experience of information security incidents and whether they report to responsible party or not if any incident occurred were asked and their response is summarized as shown in Table 2.

The internet usage of respondents have a ratio of 96.4% in favor of usage. The rest 3.6% respondents don't use internet that indicates most of the respondents has the experience of using Internet that might further indicates the likeliness of the bank's employee subjected to security incidents. Among those who use internet, 43.7% can be categorized as an 'average spending time' while 24.1% and 17.7 % of them can be categorized as 'little spending time' and 'very little spending time' respectively. The respondents who spend "much" and "very much" time to use internet were 8.2% and 6.3% respectively. The cumulative 58.2 % of respondents were categorized as internet users who spend an average and beyond average time that likely identified them as Employees' spend average of their time on internet that it makes them possible targets in untrusted network internet. This emphasize how the information security concerns are more important issues to be realized. Of course, whatever time spent, there is a security risk since there is internet involvement. Membership for social media such as Facebook, Instagram, and WhatsApp is getting more attraction nowadays as seen from the respondents answer with having a highest 91.9% compared to those who doesn't 8.1%. This also indicates respondents may be subjected to any security incidents far more using social media. Therefore, it is important to aware them how to act in using such media. Durmus (2014) also agreed in the importance of awareness for social media users on how to act along with the code of conduct in social media.

Table 2 Frequency analysis of security incidents and reporting

Question	Option	Frequency	Percent
Q6.Do you use internet?	a. Yes b. No	161 6	96.4 3.6
Q7.How much time do you spend on the Internet?	a. Very Little b. Little c. Average d. Much e. Very Much	28 38 69 13 10	17.7 24.1 43.7 8.2 6.3
Q8.Do you have a membership for any social media platform like Facebook, Twitter, Instagram and so on?	a. Yes b. No	148 13	91.9 8.1
Q9.Which personal information that you mostly share in social media? (You can select more than one option)	Picture Video Name, surname Birthdate Name, surname of family members Identification number Phone number E-mail address Researches/studies Emotions Thoughts Hobbies	148 93 31 41 23 11 0 20 32 20 18 43	91.9 55.4 18.5 24.4 13.7 6.5 0 11.9 19.0 11.9 10.7 25.6
Q10.Have you ever faced with incident about information security?	a. Yes b. No	52 107	32.7 67.3
Q11.Do you think that you will probably face with such incidents in the future?	a. Yes b. No	107 54	66.5 33.5
Q12.You faced with a content or post in a social media or a website that violate your personal rights1. Where do you report?	a. My family and/or friend b. The nearest police department c. Relative website admin d. Internet Service Provider e. Cyber Security Office (Information Network Security Agency-INSA) f. Prosecution Office g. I do not know where to report h. I do not report	29 7 17 8 11 1 51 32	18.6 4.5 10.9 5.1 7.1 0.6 32.7 20.5

Q13.When you faced with unwanted content or post (encourage/help suicide and prostitution, harmful drugs, gambling, nudity, sexual harassment and crimes against Ethiopia etc.). Where do you report?	a. My family and/or friend b. The nearest police department c. Relative website admin d. Internet Service Provider e. Cyber Security Branch Office (Information Network Security Agency-INSA) f. Prosecution Office g. I do not know where to report h. I do not report	20 23 10 12 19 1 44 28	12.7 14.6 6.4 7.6 12.1 0.6 28.0 17.8

Respondents were asked about which personal information they mostly share in social media. Respondents' respond picture more than 90%, video more than 55%, hobbies 25% and birthdate 24% in decreasing order. Most of the time when we join a social network information such as name, surname, picture, emotions, thoughts, hobbies and researches/studies are asked to share. However, sensitive information such as identification number, phone number and sometimes email address should not be given or shared to anyone. We should also reconfigure the privacy settings of social media we use otherwise everything we do will be public or visible to everyone. The respondents' security practice is a little bit above average but needs progressive awareness because one way or another their social media usage and sharing may conflict with the organization policies and procedures.

Almost one third of the respondents have faced information security incident and 66.5% of the total respondents think that they will probably face with such incidents anytime in the future including those didn't face yet. This indicates that employees may need to have a basic understanding how to use the internet in order to protect them from cyber-attacks such as social engineering and phishing attacks.

According to Durmus (2014) if a person face with a post or a content that violates his/her rights the correct way of behaviour is to consult to "relative website admin", "cyber security branch offices" affiliated to police department in the city you live and "prosecution offices". In this context, the respondents who will report to relative website admin, cyber security office and prosecution office are 10.9%, 7.1% and 0.6% respectively. Employees that will report to the nearest police department are 4.5% where 18.6% report to their families and 5.1% report to internet service provider. However, this result is unsatisfactory compared with the respondents who do not know where to report or even do not report any having more than 53%. Respondents know less about the authority in charge of concerning cyber-attacks and violation of personal rights on the internet when they are violated.

The respondents awareness level is somehow similar with the previous question when it comes to facing with unwanted content or post (encourage/help suicide and prostitution, harmful drugs, gambling, nudity, sexual harassment and crimes against Ethiopia etc.). And where they report if any? Here 14.6% report to the nearest police department, 12.1% report to cyber security office and 12.7% report to their families or friends even if it didn't concern them. However, 28% do not know where to report and 17.8% totally do not report indicating the awareness level is unsatisfactory. This means more than 45% of the respondents do not take any countermeasures for this kind of cybercrimes.

4.1.3 E-mail security

This section covers security areas such as email usage, spam email, phishing links. The findings are shown in Table 3;

Table 3 Frequency analysis of email security

Question	Option	Frequency	Percent
Q14.Do you use e-mail address?	a. Yes b. No	147 18	89.1 10.9
Q15.What is Email Spam?	a. Spam is an antivirus solution b. Spam is a firewall c. Spam is an unwanted and mass e-mails d. Spam is an e-mail attachment	10 12 102 18	7.0 8.5 71.8 12.7
Q16.What do you do when you got an e-mail asking to update your personal info by clicking the link in the e-mail body?	a. I click the link if logo and address of the bank is right b. I do the same if my close friends update their info c. I make a call to bank to get information about the e-mail d. I do not have any idea	42 20 34 48	29.2 13.9 23.6 33.3
Q17.What do you do when you got an e-mail saying that a little girl is lost for a while and ask you to forward the e-mail as many people as you can?	a. I forward to all of my contacts b. I forward to closest contacts c. I create a new post to ask sender not to forward chain e-mail d. I do not have any idea	29 39 34 39	20.6 27.7 24.1 27.7
Q18.What do you do when you got an e-mail from your friend but file extension of the attachment and domain	a. It is safe to open up attach as the sender is friend of mine. b. I reply to e-mail to confirm if it is really sent by my friend	14 40	10.1 29.0

name of the address (the section after '@' sign) is weird?	c. I create new post to send to my friend's address in my contact to for confirmation d. I do not have any idea	26 58	18.8 42.0

In terms of email address 89.1% of the respondents use email to communicate whereas 10.9% do not use it. Among this, 71.8% of the respondents know about spam email which is a satisfactory result.

Participants' response when they got an email to update their personal information by clicking the link in the email body is unsatisfactory with only 23.6% make a call to bank to get information about the e-mail. The rest 29.2% click the link if the logo and address of the bank is right, 13.9% do the same if their close friends update their information, and 33.3% do not have any idea what to do with it. This result is unsatisfactory regards phishing attacks awareness.

Almost 28% of the respondents replied I do not have any idea what to do when they got a phishing email and asked to forward to other people. The respondents that forward to all of their contacts results 20.6% and that forward to their closet contacts count 27.7%. Only 24.1% of respondents notify the sender not to forward chain e-mails which is a good security behavior. The same is true when respondents receive file extension of the attachments and domain name addresses are confusing where 42% replied I do not have any idea what to with it. 10.1% of them replied it is save to open up attach and 29% of them reply to the email while 18.8% do the right thing by creating a new post to confirm their friends. This shows the respondents' knowledge to phishing links is unsatisfactory. This finding shows that more than 75% the respondents will probably be vulnerable to phishing attacks by e-mail.

4.1.4 Safely use of internet and computer

This section present findings which includes precautions taken in case stolen computers, locking user account and distinguishing a safe website. The results are shown in Table 4.

For the distribution of respondents regarding which precautions they take in case their laptop is stolen, all the choices are correct. However, one thing to consider is that their importance level varies based on priority. The first thing is to note down the serial number and physical address of the laptop a separate safe place to find easily lately (Durmus, 2014). This indicates keeping its serial number and physical MAC address is highly important to find a stolen

device. Here 36.3% of the respondents' backup sensitive data and 24.4% set password for their user accounts. Even if the answers are right, the respondents who keep its physical MAC address (6.5%) and keep its serial number (17.3%) are unsatisfactory level as compared with the first two. The list continues with 6.5% both encrypt their sensitive data and install a GPS software to trace, 5.4% install an alarm software and 3% mark a sign on their laptop. Among all the choices the respondents are interested in backup their sensitive data and set passwords for their user accounts rather than being able to keep its serial number and/or MAC address in the first place. This finding shows although the choices are correct, the level of especially keeping its serial number is very unsatisfactory.

Table 4 Frequency analysis of safety use of internet and computer

Question	**Option**	**Frequency**	**Percent**
Q19.Which precautions do you take in case your laptop is stolen?	a. Keep its physical (MAC) address	11	6.5
	b. Keep its serial number	29	17.3
	c. Backup my sensitive data	61	36.3
	d. Encrypt my sensitive data	11	6.5
	e. Install an alarm software	9	5.4
	f. Set passwords for my user accounts	41	24.4
	g. Mark a sign to unrecognizable place on my laptop	5	3.0
	h. Install a GPS software to trace remotely	11	6.5
Q20.Do you lock your user account with password when you took a little break from work or leave your seat?	a. I only lock in my business laptop	11	6.7
	b. I only lock in my personal computer	32	19.6
	c. I use it in both	75	46.0
	d. I do not lock as I go back to work in short time	31	19.0
	e. I do not lock as my data is not that critical	14	8.6
Q21.How do you distinguish if a website is safe to surf or not?	a. Websites that offer freeware are safe	9	6.1
	b. Online casinos are safe	4	2.7
	c. It is safe if a security logo exists	31	21.1
	d. It is safe if the web browser shows small gold lock pad	8	5.4
	e. It is safe if its address starts with "https://" instead of "http://"	22	15.0
	f. It is safe if it appears to be popular	6	4.1

	g. I am having difficulty in distinguishing	67	45.6

The next part is whether the respondents lock their user account with password when they took a little break from work or leave their seat. Respondents that use password in both business and personal computer counts less than 50% which is unsatisfactory level. The rest 19.6% only lock their personal computer and 6.7% only lock their business laptop whereas 19% and 8.6% do not lock as they go back to work in short time and their data is not that critical respectively. Literatures such as Abdyli (2014), Durmus (2014) and Xiong (2011) tell us the correct way of behavior is to use password protection in both personal and business computers even if we will go back in a minute in a home and business environment or even if data we stored is not much critical. This is just a way of developing a proper security habit before gaining it as behavior.

Employees were also asked how to distinguish if a website is safe to surf or not. There are two answers here, it is safe if the web browser shows small gold lock pad and if its address starts with “https://” instead of “http://”. However, only 5.4% and 15% respectively select those choices. More than 45% of the respondents have difficulty in distinguishing. This is also very unsatisfactory level and need high attention.

4.1.5 Threats and preventive measures

This section presents findings related to file sharing software and threats generated by them, software updates, antivirus usage and backup as follows. The results are illustrated in Table 5.

Table 5 Frequency analysis of threats and preventive measures

Question	Option	Frequency	Percent
Q22.Have you ever used file sharing software like uTorrent, BitTorrent, eMule and so on?	a. Yes b. No	31 127	19.6 80.4
Q23.Which ones are the threats originated by file sharing software?	a. I may violate copyright of music, video or any other software b. The program I downloaded may include malicious software c. I may allow bad guys with bad intentions to see my personal data	27 52 17	16.1 31.0 10.1
Q24.What do you think about updates of your types of software installed in your computer?	a. I install at once if there is available update b. I install few days later after I take care of my other tasks c. I get help from my closest friends d. I do not have any idea	49 22 21 28	40.8 18.3 17.5 23.3
Q25.What type of antivirus software do you use in your computer?	a. I use free antivirus software b. I use cracked antivirus software c. I use license paid antivirus software d. I do not use antivirus software e. I do not have any idea	91 12 32 9 16	56.9 7.5 20.0 5.6 10.0
Q26.How often do you make security scanning in your computer?	a. Never b. Rare c. Average d. Often e. Very often	21 46 63 18 14	13.0 28.4 38.9 11.1 8.6
Q27.How often do you backup your data in your computer?	a. Never b. Rare c. Average d. Often e. Very often	25 37 71 21 9	15.3 22.7 43.6 12.9 5.5
Q28.Which one of the statements below is true?	a. Only firewall is sufficient in a computer b. Only antivirus software is sufficient in a computer c. Both antivirus software and firewall perform same functionalities d. Both antivirus software and firewall need to be used updated in a computer	6 16 42 90	3.9 10.4 27.3 58.4

Employees that have ever used file sharing software such us uTorrent and BitTorrent are 20%. Out of which 16% respondents knows these file sharing software may violate copyright of music, video or any other software, 31% knows the downloaded program may include malicious software and 10.1% knows it may allow bad guys with bad intentions to see their personal data. All answers are correct however, the percentage is very less. This awareness level is not enough and seen as below average.

Regarding updating installed software 40.8% of employees install at once if there is available update. This is number is way below average resulting unsatisfactory level. 18.3% install updates days later after they take care of other things and 17.5% get help from their close friends while 23.3% do not have any idea what to do.

More than 80% respondents use different types of antivirus for their computer system while 10% do not have any idea about the types of antiviruses and 5% do not use any. Employees using a free antivirus software are 56.9%, using cracked antivirus software are 7.5% and using licensed software are 20%. Employees close to 60% perform security scanning in average or often period while the rest rarely or never perform security scanning. Most types of free antivirus software do not provide full protection. They commonly come with features to scan hard-drives and external drives while licensed one's are able to provide full protection like anti-spam filtering, identifying unsafe phishing websites, and malware and firewall protection. As for the cracked antivirus software, too few of them are free of trojans or backdoors (Durmus, 2014). Therefore, using a license paid antivirus is better and also costly compared to the rest. As an organizational level we can force all employees to use license paid antivirus by installing on each device. However we cannot force users what to use since each have its pros and cons, but we can teach them the differences.

Employees' take backup of their computer data on average and above level of more than 60% of the total respondent. They were also asked about firewall and antivirus. 58.4% of the employees answered that both antivirus software and firewall need to be used updated in a computer. This is average level and needs to be communicated compared to the rest incorrect choices counting 41.6%.

4.1.6 Password management and security

This section describes findings related to setting a password, interval of changing it and sharing to other people as follows in Table 6.

Table 6 Frequency analysis of password management and security

Question	Option	Frequency	Percent
Q29.What do you think about changing your passwords?	a. I change my password only if I doubt that somebody stole it	52	32.3
	b. Changing process is boring	9	5.6
	c. I change my password regularly	65	40.4
	d. I change my password only if I have to give it to my friend	35	21.7
Q30.How do you set your password?	a. I use the password preset by the system	13	7.9
	b. I set short password not to forget	42	25.6
	c. I set all of my passwords same not to forget	19	11.6
	d. I set my password including upper, lower letters, numbers and special characters	68	41.5
	e. I set my passwords with 8 characters at least if the system allows	19	11.6
	f. I use password generator tool	3	1.8
Q31.With whom do you share your computer's authentication password?	a. I share with my trusted friend	56	34.8
	b. I share with my trusted relative	11	6.8
	c. I share with IT division in my corporate	17	10.6
	d. I don't share with anyone	77	47.8

There were three correct answers for the password setting questions namely I set my password including upper, lower letters, numbers and special characters, second I set my passwords with 8 characters at least if the system allows and third I use password generator tool. Respondents that select the mentioned answers count 55%. However, 45% of them selected the wrong answers I use the password preset by the system, I set short password not to forget and I set all of my passwords same not to forget. These are not good security practices and need focus because password is critical aspect when dealing with authentication and authorization of system. Employees that change their passwords regularly take 40% while those who change their password only if they doubt that somebody stole it and those who change their password only if they have to give it to a friend counting 32.3% and 21.7%

respectively. This is close to average level regarding changing on regular basis but a lot need to be done to make this critical aspect understood by employees so that all of them should follow these good practices regards password. There is a bad security practice related to password sharing. The number of employees that do not share their password only counts 47.8% which is unsatisfactory result and the rest share their password to their close relative, friend or the IT department. It is a must to create awareness to employees about password management.

4.1.7 Information security terms and social engineering

This last section presents findings of information security terms and social engineering as shown in Table 7.

Table 7 Frequency analysis of information security terms and social engineering

Question	Option	Frequency	Percent
Q32.Who is responsible for Information Security?	a. Information owner	47	29.6
	b. Information user	85	53.5
	c. Information manager	27	17.0
Q33. "A chain is as strong as its weakest link." What does this motto mean to you?	a. It could cause security vulnerability if an IT personnel walk out	11	7.7
	b. An information security awareness level in a place is as much as a person who has least information security knowledge in place	75	52.4
	c. Information security is provided only if you have skilled technical team	33	23.1
	d. A corporate can be exposed to vulnerability if an untrusted employee is recruited	24	16.8
Q34.What does "social engineering" mean?	a. It is a security add-on checking if a website is safe	37	26.2
	b. It is an art of deception that makes use of getting information that need to be kept secret in normal circumstances by using convincing and influencing abilities	89	63.1
	c. To be exposed to insultation by an entity you have just met on social media	15	10.6

Employees answer to who is responsible to information security among Information owner, Information user and Information manager choices, 53.5% of them answered information user while the other two choices have very less percentage. Here all choices have more or less equal impacts on information security however the respondents only focus on one entity. This awareness is unsatisfactory and all the three parties should have been selected with close percentage since they have proportionally high impact on security.

Employees were asked to obtain if a general security statement has a meaning for them, a chain is as strong as its weakest link. Where 52.4% of the employees got the correct answer an Information Security Awareness level (ISA) in a place is as much as a person who has least information security knowledge in place which is average level getting that humans are the weakest links (Alageel, 2003; Connolly et al., 2017 and Kruger et al., 2006). They were also asked about what a social engineering means in security term where 63% of the respondents have average and above level of know-how that it is an art of deception that makes use of getting information that need to be kept secret in normal circumstances.

4.2 Technical category result

A total of 12 questionnaires were distributed in person for the technical users and all of them were responded. The technical category questionnaire is categorized into ten sections. The first is related to demographic features and the rest nine sections deals with technical aspects related to information security awareness. The data were analyzed using frequency analysis. The presentations and findings are as follows.

4.2.1 Demographic features

The first section includes findings of gender, age, qualification, job category and work experience and presented in Table 8.

Table 8 Frequency analysis of Technical category demographic features

Question	Option	Frequency	Percent
Q1. Gender	Male Female	10 2	83.3 16.7
Q2. Age	18- 24 25- 34 35- 44 45- 54 > 55	2 6 1 2 1	16.7 50.0 8.3 16.7 8.3
Q3. Professional qualification	Diploma Degree Masters PhD	0 9 3 0	0 75.0 25.0 0
Q4. Job category	Management Senior Level Officer Level Junior Level	5 1 1 4	45.5 9.1 9.1 36.4
Q5. Work experience	0-1 year 1-3 years 3-5 years 5-10 years Above 10 years	0 4 0 4 3	0 36.4 0 36.4 27.3

As we can see from Table 8 the technical questionnaire respondents are composed of 83.3% to 16.7% in favor of male participants. Most of the age range [25-34] fall 50% while [18-24] and [45-54] take 16.7% each. More than 75% of the respondents have first degree at least. The job category distribution has 45.5% of management level staffs and the rest contains senior, officer and junior level employees. Respondents who have 5-10 years or above experience are more than 60% and one third of the respondents have 1-3 years of experiences.

4.2.2 Security standards, procedures and training

This section includes findings of nine questions related to security standards, procedures and training and presented using tables.

Table 9 Frequency analysis for use of security technologies

Question	Option	Frequency	Percent
Q6.Which security technologies do you use in your organization? (You can select more than one option)	Antivirus software	10	83.3
	Firewall appliance	8	66.7
	Web Application Firewall	2	16.7
	Database Firewall	3	25.0
	Antispyware software	0	0
	Virtual Private Network	4	33.3
	Vulnerability/Patch Management	12	100.0
	Data encryption on storage units	1	8.3
	Web / URL filtering	4	33.3
	Application Firewall	3	25.0
	Log management software	1	8.3
	End point security / NAC (Network	12	100.0
	Admission Control)	1	8.3
	Data loss prevention / content monitoring	4	33.3
	Server-based ACLs (Access Control Lists)	12	100.0
	Information Forensic Tools	12	100.0
	Public Key Infrastructure (PKI)	2	16.7
	Smart cards and keys	12	100.0
	Wireless security	12	100.0
	Virtualization specific tools	3	25.0
	Static accounts user name and passwords	12	100.0
	Biometric	1	8.3
	Information Security Management System	2	16.7
	Other		

As seen in Table 9 employees have answered antivirus software, firewall appliance, vulnerability/patch management, end point security, information forensic tools, public key infrastructure, wireless security, virtualization and biometrics are mostly used in the organization. However, the organization doesn't have/use technologies such as web application and database firewall, and data loss prevention or content monitoring. This is a major issue since we cannot say we are secured without confirming that our data and web applications are secured in the first place. This implies the organization's data and web applications are not secured enough and their content is not monitored properly even if the organization has firewalls which works on network layer level. It is further shown that information security management system is not used as well.

Table 10 Frequency analysis of Q7- Q9

Question	Option	Frequency	Percent
Q7.Do you follow a standard for network and information security in your organization? (You can select more than one option)	a. ISO/IEC 27001/2	2	20.0
	b. PCI DSS (Payment Card Industry Data Security Standard)	1	10.0
	c. COBIT (Control Objectives for Information Technology)	0	0
	d. NIST (National Institute of Standards and Technology)	1	10.0
	e. Another information security standard	0	0
	f. None	1	10.0
	g. I do not have any idea	5	50.0
Q8. Do you have any procedure in case of being exposed to cyber-attack?	a. Yes	1	10.0
	b. No	2	20.0
	c. We use another technology/method	2	20.0
	d. I do not have any idea	5	50.0
Q9. Which information security policies do you put into practice in your organization?	a. Network policies	8	66.7
	b. User policies	7	58.3
	c. Laptop policies	4	33.3
	d. Intrusion Detection/Prevention policies	2	16.7
	e. Patch/Updating policies	1	8.3
	f. Another policy	0	0
	g. None of them	0	0
	h. I do not have any idea	3	25.0

As we can see from Table 10, 50% of the technical staffs do not have any idea and 10% answered we do not use or follow any standard. This implies there may not be a specified standard for network and information security in the organization and if there is one, it is not well communicated for all the staffs and not well enforced as we can see from these contradicting responses. On the other hand, 70% respondents do not know or have any procedure in case of being exposed to cyber-attack. This is a frightening finding since nowadays no single organization is safe from cyber-attacks and having no or poor countermeasures will jeopardise the business (Siponen, 2000). Multiple information security polices used in the organization, network polices having the highest percentage 66.7%. However, intrusion detection/prevention polices and patch/updating polices are far less which are a major gap. The lack of these polices cause such as vulnerabilities in systems and may highly increase attack level (Siponen, Pahnila, & Mahmood, 2010). Abdyli (2014) stated without standards that provide objective criteria for information security choices, information security experts make choices based on undeserved aspects that might include lack of

knowledge, supposed constraints, inappropriate confidence and personal motivation. Abdyli (2014) further stated it is recommended that internal policies defined by the bank are to be applicable and in line with these international standards. The support of management of the bank is also necessary on the implementation phase of these standards.

Table 11 Frequency analysis of Q10-Q14

Question	**Option**	**Frequency**	**Percent**
Q10. Are your employees being trained about information security awareness?	a. Yes b. Sometimes c. No d. Another	0 3 9 0	0 25.0 75.0 0
Q11. How often do you train your employees about information security?	a. Once a year b. Once a week c. Few times a year d. Once a month	0 0 2 0	0 0 16.7 0
Q12. Do you follow any resources, materials for oncoming technologic news and developments?	a. I follow some resources at home b. I subscribe to news bulletins and get e-mail regularly c. I benefit from the organization web portal d. I sometimes follow magazines e. Organization training is enough for me f. I do not follow any resource g. Another	4 7 1 4 0 1 0	33.3 58.3 8.3 33.3 0 8.3 0
Q13.Have you ever experienced any security incident in your organization network? (e.g. threat, attack, malicious software) If any, how many times did you face?	a. 1- 5 times b. 6-10 times c. More than 10 d. Never experienced	1 0 0 10	9.1 0 0 90.9
Q14. How long does it take to close the security breaches?	a. Between 0-3 months b. Between 3-6 months c. Between 6-9 months d. Between 9-12 months	0 0 1 0	0 0 8.3 0

In Table 11 respondents were asked about whether their employees are being trained about information security awareness where 75% of them answered they are not. Out of the 25% who answered they sometimes do train, only 16.7% of them train their employees few times a year. This is very unsatisfactory result. It is one objective of this paper that employees have

information security awareness program. For instance, if employees are not aware on information security, it will be difficult for them to protect the corporate data at the same time themselves from any kind of security attacks (Connolly, Lang, & Tygar, 2017). This implies employees must be aware of information security within their organization, and information security awareness programs must be established in line with banks information security policies and relevant measures (Abdyli, 2014). Employees stay informed with IT materials by subscribing to news bulletins and get email regularly taking 58% of the total respondents. While following magazines and following some resources at home take 33.3% each. This indicates more than 80% of the respondents stay informed about information technology including security aspects which is a good security practice. Employees who experienced a security incident were 10% and the time it took to close the security breach is between 6-9 months. This finding doesn't mean the organization is this much secured or cyber-attacks were not attempted as the numbers were expected to raise since it is a financial institution. There may be different reasons for this outcome for instance, the less incident number may indicate that there were not really any major attacks or may be employees are protecting the organization's reputation or image against outsiders.

4.2.3 Firewall, IPS, management, penetration and traffic control

This section presents findings of ten questions related to firewall, IPS, management, penetration and traffic control. The table presentation is as follows.

Table 12 Frequency analysis of Q15-Q19

Question	Option	Frequency	Percent
Q15. Do you use SSL encryption?	Yes No I do not have any idea	8 1 3	66.7 8.3 25.0
Q16. Do you use Virtual Private Network (VPN) on your network?	Yes No I do not have any idea	8 1 3	66.7 8.3 25.0
Q17. Do you perform daily logging on your wired network?	Yes No I do not have any idea	7 1 2	70.0 10.0 20.0
Q18. Do you use xflow protocols on your network? (e.g. Netflow, netstream, sflow)	Yes No I do not have any idea	3 2 7	25.0 16.7 58.3

Q19. Do you use authentication protocol in your network structure? (You can select more than one option)	TACACS/TACACS+ We do not use RADIUS Smart Card Biometric We use another authentication protocol I do not have any idea	3 1 1 0 0 0 7	25.0 8.3 8.3 0 0 0 58.3

As illustrated in Table 12, 66.7% of respondents' uses SSL encryption and VPN connection each to use it for webservers that need encrypted sessions and to communicate with branch network connection through Ethio-Telecom respectively. Employees were asked if they perform daily logging and 70% of the respondents answered they do perform. And only 25% of the respondents use xflow protocols on the network, protocols which can enable admins to gather information about traffic flow by sorting particular categories like application or IP address. Employees that uses TACACS/TACACS+ and RADIUS authentication protocols in the network infrastructure are more than 30% while 58.3% do not have any idea what they are using. These are authentication protocols to access network devices where TACACS is vendor specific and RADIUS is vendor independent. These findings shows employees awareness to SSL and VPN are average level where as the use of xflow protocols and authentication protocols is unsatisfactory. This needs to be improved in terms of implementation and communicate or get people to be aware of what they are using for what purpose if it is already implemented.

Table 13 Frequency analysis of Q20-Q24

Question	**Option**	**Frequency**	**Percent**
Q20. Do you make penetration test for web environment?	Yes No I do not have any idea	1 6 3	10.0 60.0 30.0
Q21. Do you make necessary filtering for web software?	Yes No I do not have any idea	6 0 4	60.0 0 40.0
Q23. Is your network infrastructure wired or wireless?	Only Wired Both Wired and wireless	1 10	9.1 90.9
Q24. Do you have IPS or IDS appliance on your wired network?	We do not use any of them We have IPS appliance but IDS We use both appliances I do not have any idea	1 1 2 7	9.1 9.1 18.2 63.6

Employees that answered they do not perform penetration test count 60% and who do not know whether it has been done or not count 30% of the respondents as seen on Table 13. This is not an example of good security practice since the organization cannot identify its vulnerabilities and mitigate the risks before attackers exploit them. Although 60% of the respondents do filter web software to protect the traffic, the result is not good enough. The result should also have included the rest of the group to get a better result. The next question was whether the organization has wired or wireless infrastructure or both and 90% of the employees answered it has both infrastructures. The usage of IPS and/or IDS by respondents is less than 30% and is very unsatisfactory. These important system if applied properly enable an organization to protect and detect intrusions before they cause disaster to the organization.

4.2.4 Wireless network security

This section presents findings of five question related to wireless network security as shown in Table 14.

Table 14 Frequency analysis of Q25-Q29

Question	Option	Frequency	Percent
Q25. Do you have wireless IPS or IDS appliance on your wireless network?	We do not use any of them We have IPS appliance but IDS We have IDS appliance but IPS We use both appliances I do not have any idea	1 0 0 0 9	10.0 0 0 0 90.0
Q26. Are your wired and wireless IPS appliances integrated each other?	Yes No	0 4	0 33.3
Q27. Do you use guest portal on your wireless network?	Yes No We use another technology/ method I do not have any idea	1 5 0 4	10.0 50.0 0 40.0
Q28. Do you perform daily logging on your wireless network?	Yes No We use another technology/method I do not have any idea	1 6 0 3	10.0 60.0 0 30.0
Q29. Do you use WEP on your wireless network security?	Yes No We use another technology/method I do not have any idea	0 4 0 6	0 40.0 0 60.0

The first two questions asked whether the respondents have wireless IPS/IDS and if they do have, are they integrated with the wired network. The respondents replied as they do not use any of them and there is no integration as a result. More than 85% respondents said either the organization doesn't have a guest portal service that isolate guest VLANs from production environment and ease user management or do not have any knowledge about the service. The same is true when it comes to daily logging on wireless network out of which 90% of the respondents answered there is no such thing and they do not recall. On the other hand, 40% of the respondents answered Wired Equivalent Privacy (WEP) security is not implemented on the wireless at all. This is a good measure since WEP is the oldest and the weakest of the available encryption protocols. Since WEP was highly vulnerable it was replaced by Wi-Fi Protected Access (WPA) and WPA2 which intended to address many of the problems that overwhelmed WEP. Hence, if we have a wireless network and it is not secured by a means of for example, IPS/IDS there will be definitely an issue. Wireless networks are very vulnerable compared to wired networks and multiple security measures should be taken to protect them such as using WPA/WPA2 protocol, using guest portal etc.

4.2.5 OSI Application layer security

This section includes two questions related to voice application and encryption as described in Table 15.

Table 15 Frequency analysis of Q30 and Q31

Question	Option	Frequency	Percent
Q30. Do you use voice applications?	Yes No	0 11	0 91.7
Q31. Are they encrypted?	Yes No I do not have any idea	1 0 3	25.0 0 75.0

The two questions were concerned whether respondents use voice applications in the organization and are they encrypted if any. However, more than 90% replied they do not use any, as a result there is no need to discuss about encryption. If there were any voice application, the data should be encrypted.

4.2.6 OSI Transport layer security

This section describes the respondents perception regards port based packet filtering as presented in Table 16.

Table 16 Frequency analysis of Q32

Question	Option	Frequency	Percent
Q32. Do you find port-based filtering enough?	Yes No I do not have any idea	2 3 6	18.2 27.3 54.5

Port filtering is allowing or blocking network packets into or out of a device or the network based on their port number. More than a quarter of respondents do not apply port filtering and half of the total respondents do not have the knowledge of port based filtering when it comes to accessing different types of servers/services within the organization. This is unsatisfactory result and all respondents should be aware of such things. For instance, insiders may violate this vulnerability unintentionally or even intentionally.

4.2.7 OSI Network layer security

This section presents findings of respondents related to network layer security as shown in Table 17.

Table 17 Frequency analysis of Q33 and Q34

Question	Option	Frequency	Percent
Q33. Which security feature is configured on your Layer 3 Switches or routers?	ACL (Access Control List) We do not use these	2 2	50.0 50.0
Q34. Is authentication configured on your routers?	Yes (MD5) No	3 2	60.0 40.0

According to respondents who attempted Q33, 50% answered only Access Control List (ACL) is used among the given alternatives. In simple words ACLs are used to filter IP addresses from source to destination based on requirements, that is permit or deny access. However, this feature is not the only one and other security features should be configured on network devices to increase the security posture. Regards whether authentication configured on routers, 60%

of respondents said Message Digest 5 (MD5) encryption algorithm is configured between routers to authenticate routing packets.

4.2.8 OSI Data link layer security

This section describes thirteen question results related to data link layer security such as switch. The results are shown in Table 18 and Table 19.

Table 18 Frequency analysis of Q35-Q40

Question	Option	Frequency	Percent
Q35. Are unused ports disabled?	Yes No I do not have any idea	4 2 5	36.4 18.2 45.5
Q36. Is port security enabled on your network?	Yes No I do not have any idea	3 1 7	27.3 9.1 63.6
Q37. Do you use only one VLAN on your network?	Yes No I do not have any idea	1 5 5	9.1 45.5 45.5
Q38. Do you use Private VLAN (PVLAN) on your network?	Yes No I do not have any idea	3 1 6	30.0 10.0 60.0
Q39. Do you use 802.1x protocol on your network?	Only in wired network In both of them I do not have any idea	1 2 7	10.0 20.0 70.0
Q40. Do you use protected port?	Yes No I do not have any idea	4 2 4	40.0 20.0 40.0

From the above table we learn that unused ports are not disabled enough (36.4%) and similarly port security is not enabled enough (27.3%) in the organization. If properly configured these features assist the organization to protect it from unauthorized malicious user from accessing the network. The respondents' response they have multiple VLANs (45.5%) and also use PVLAN (30%). Even if the percentage is not enough, these features enable the respondents to have a well-managed, secured and segmented network not forgetting decreasing the load of network traffic. Most of the respondents do not have any idea whether they are using 802.1x authentication protocols and 40% of the respondents answered they use protected ports which

disables employees in the institution communicating with each other while they can access to internet via router. Overall, disabling unused ports, using port security and having multiple VLANs are not showing satisfactory results and should be improved to secure the organization.

Table 19 Frequency analysis of Q41-Q47

Question	**Option**	**Frequency**	**Percent**
Q41. Is DHCP Snooping enabled on your network?	Yes I do not have any idea	4 6	40.0 60.0
Q42. Is ARP Inspection enabled on your network?	Yes I do not have any idea	2 8	20.0 80.0
Q43. Is IP Source Guard enabled on your network?	Yes I do not have any idea	2 8	20.0 80.0
Q44. Is Root Guard enabled on your network?	Yes I do not have any idea	1 9	10.0 90.0
Q45. Is Loop Guard enabled on your network?	Yes I do not have any idea	1 9	10.0 90.0
Q46. Do you use Storm Control feature on your network?	Yes I do not have any idea	1 9	10.0 90.0
Q47. Is MAC Security configured on your network?	Yes No I do not have any idea	2 1 7	20.0 10.0 70.0

As shown in Table 19, DHCP snooping and ARP inspection are enabled in the network. Enabling IP DHCP snooping verifies MAC-IP address mappings and stores valid mappings in a database. Both features need to prevent ARP poisoning, attempts to contaminate a network with improper gateway mappings. All the five IP source guard, root guard, loop guard, storm control and MAC security are somehow enabled however, the respondents who do not know about the above concepts is much bigger than expected and should be aware in order to understand their benefits and implement them in the organization. If IP source guard is not enabled switches can be exposed to IP spoofing attacks because they do not filter IP addresses on untrusted layer 2 ports depending on DHCP snooping binding table. Root Guard is used to identify and assign the root bridge for frames so that other switches cannot make change accidentally or intentionally by a malicious user. Setting a false bridge can make switches converge incorrectly and misdirect the traffic to unintended way. Loop guard feature

provides extra loop-free topology in some circumstances on highly switched network environments. Storm control feature on switched environments drops the traffic that exceeds certain preconfigured threshold value. As shown from the responses the organization can be exposed to denial of service attacks due to misconfiguration in switches which cause loops or due to unnecessary services sending abnormally excessive messages. Few of the respondent response they are using MAC security feature. MAC security feature filters MAC address to provide access to a network so that unauthorized malicious user who has a physical access to ports cannot access the network.

4.2.9 OSI Physical layer security

This section describes the findings of seven question related to physical layer security as shown in Table 20.

Table 20 Frequency analysis for Q48-Q57

Question	Option	Frequency	Percent
Q48. Do you perform user id authentication in all of the gates of your organization?	Yes No I do not have any idea	5 3 2	50.0 30.0 20.0
Q49. Do you have any user authentication mechanism at the entrance of system rooms?	Yes We use another technology/method I do not have any idea	8 1 1	80.0 10.0 10.0
Q50. Do you use shredder to destroy document assets of your organization?	No I do not have any idea	6 5	54.5 45.5
Q51. Do you have fire sensors in system rooms?	Yes No We use another technology/method I do not have any idea	10 0 0 0	83.3 0 0 0
Q52. Do you have cooling sensors in system rooms?	Yes No We use another technology/method I do not have any idea	11 0 0 0	91.7 0 0 0
Q53. Do you have power redundancy in system rooms?	Yes I do not have any idea	9 2	81.8 18.2
Q54. Do you have cameras in system rooms?	Yes No We use another technology/method I do not have any idea	11 0 0 0	91.7 0 0 0
Q55. Are the cabinets locked in system rooms?	Yes I do not have any idea	10 1	90.9 9.1
Q56. Do you label the cables plugged in to network devices?	Yes I do not have any idea	10 1	90.9 9.1
Q57. Do you have disaster recovery center?	Yes No We use another technology/method I do not have any idea	2 9 1	16.7 75.0 8.3

Half of the respondents respond that the organization uses user id authentication in all the gates while the other half answered either they do not have any knowledge about it or it is not

performed at all. However, 80% of the respondents answered there is such mechanism at the entrance of system rooms. More than 50% of the respondents' response they do not use shredder to get rid of sensitive documents. Both fire and cooling sensors are implemented in the organization to notify the employees if any abnormalities occur in system room. Redundant power source such as generators and uninterruptable power supplies (UPS) are also configured to run the system room 24/7. Cameras are also deployed to record and monitor any action in the system room. The organization datacenter cabinets are locked to protect network equipment. Respondents also answered that labelling of cables that are plugged to networking devices has been done. These measures help to protect the organization's network equipment and to easily trace the cables if needed. More than 70% of respondents answered there is no disaster recovery site which is a major input for business continuity. This may cause a business down time the organization cannot afford. Organizations just cannot rely on a single datacenter without having properly tested disaster recovery site which is physically far from the existing datacenter.

4.2.10 End point security

This last section describes the findings of three questions related to end point security as described using Table 21.

Table 21 Frequency analysis of Q58-Q60

Question	Option	Frequency	Percent
Q58. Do you use a technique that prevents passwords from holding in RAM?	Yes No I do not have any idea	3 4 3	30.0 40.0 30.0
Q59. Do you use BIOS password in end point stations?	Yes No I do not have any idea	2 5 3	20.0 50.0 30.0
Q60. Do you get WHOIS service?	Yes No I do not have any idea	2 1 6	22.2 11.1 66.7

More than 40% of respondents do not use a technique to prevent password from holding in RAM. Similarly, more than 50% of respondents do not use BIOS password in endpoint stations. These measures increase endpoint password management however the organization is not benefited since it didn't applied them. The last question was if respondents use WHOIS service. WHOIS is a system that asks the question, who is responsible for a domain name or

an IP address? A service used to identify and checks the legitimacy of websites. And more than 75% of respondents replied either they have no knowledge about it or they do not use the service at all.

4.3 Summary

In this chapter, based on the information collected from the sampled branches using questionnaire, the gap towards information security awareness were identified and discussed. Hence, the result found from the Bank staffs were analyzed using SPSS v.21 tool and presented in table using frequency and percentage. Summary of the findings is as follows;

- Password management is poor (respondents' password setting, changing and protection practices are unsatisfactory)
- Respondent security practices in relation to antivirus usage and security scanning are not performed regularly in timely manner
- The organization doesn't use information security standards
- Doesn't have a well-organized procedures in case of cyber attacks
- Most of employees are unable how to distinguish whether a website is safe to surf or not
- The respondents have unsatisfactory knowledge of safe internet usage
- Employees knowledge to phishing attack links is poor
- Respondents' knowledge to social engineering needs improvement
- Respondents are not performing backup regularly in timely manner
- Respondents don't have adequate knowledge about handling of incidents
- Respondents awareness to IT infrastructure physical threats is inadequate
- Respondents' knowledge to information security responsibility needs improvement
- The organization wireless and other network implementation and security management are not good
- Respondents are not updating software regularly in timely manner
- Respondents security practices related to software installation and usage needs improvement
- User ID authentication in all gates of the organization are not satisfactory
- Personal computers security precautions are not practiced well enough
- Respondents don't use encryptions while transferring corporate data

- Respondents security practice with related to sharing of files and other resources needs improvement

Overall, the findings shows that the information security awareness level of Enat Bank employees is unsatisfactory. In the next chapter, the proposed program is discussed.

CHAPTER FIVE

PROPOSED INFORMATION SECURITY AWARENESS PROGRAM

The chapter presents the proposed information security awareness program for the Bank based on the findings of analysis of the research and reviewing existing security awareness programs. Furthermore, the chapter proposes possible delivery techniques for the program.

5.1 Proposed Information Security Awareness Program – ISAP

Organizations should never randomly choose the topics on their information security awareness program. Instead it should be selected based on their specific need. Choosing appropriate form of delivery method also should be based on the organization work processes and management system (Xiong, 2011). Security awareness should also be conducted as an on-going program to ensure that training and knowledge is not just delivered as an annual activity, rather it is used to maintain a high level of security awareness on a daily basis (PCI Security Standards Council, 2014). The proposed program should be tailored and focused on key weakness of employees' security awareness, and it should be changed as technology advances.

Accordingly, an information security awareness program for Enat Bank is proposed based on the key findings of the data analysis and corresponding topics generated from the literature review. As it was discussed in chapter II, NIST and SANS defined topics that must be included in ISAPs. Moreover, PCI-DSS and ISO documents have main concerns on these topics. Hence, as shown in Table 22 the key findings of the analysis are associated with the candidate topics that must be included in the ISAP for Enat Bank.

Table 22 Mapping key findings to candidate topics

Key findings	Candidate topics
- Password management is poor Respondents' password setting, changing and protection practices are unsatisfactory	**Password usage and management**
- Respondent security practices in relation to antivirus usage and security scanning are not performed regularly in timely manner	**Protection from malware**
- The organization doesn't use information security standards - Doesn't have a well-organized procedures in case of cyber attacks	**Organizational information security policies and procedures**
- Most of employees are unable how to distinguish whether a website is safe to surf or not - The respondents have unsatisfactory knowledge of safe internet usage - Employees knowledge to phishing attack links is poor - Respondents' knowledge to social engineering needs improvement	**Safe internet usage**
- Respondents are not performing backup regularly in timely manner	**Data backup and storage**
- Respondents don't have adequate knowledge about handling of incidents	**Incident management**
- Respondents awareness to IT infrastructure physical threats is inadequate	**Changes in system environment**
- Respondents' knowledge to information security responsibility needs improvement	**User responsibility**
- The organization wireless and other network implementation and security management are not good	**Device security issues**

- Respondents are not updating software regularly in timely manner	**Timely application of system patches**
- Respondents security practices related to software installation and usage needs improvement	**Supported/allowed software on organization systems**
- User ID authentication in all gates of the organization are not satisfactory	**Visitor control and physical access to spaces**
- Personal computers security precautions are not practiced well enough	**Desktop security**
- Respondents don't use encryptions while transferring corporate data	**Data transmission security**
- Respondents security practice with related to sharing of files and other resources needs improvement	**File sharing and copyright**

As it is presented above, 15 candidate topics are identified to design the ISAP for Enat Bank. Though the detail contents can be prepared during operationalize the ISAP, brief description of each topic presented below as shown in Table 23.

Table 23 Description of candidate topics

No	Candidate Topic	Brief description and main content
1	Password usage and management	Password creation, frequency of changes, and password protection.
2	Protection from malware	Protection from viruses, worms, Trojan horses, and other malicious code, scanning, updating definitions.
3	Organizational information security policies and procedures	Based on organizational policies and procedures aware the employees do and don't, implications of noncompliance.
4	Safe internet usage	Allowed versus prohibited, monitoring of user activity, phishing (unknown e-mail/attachments), spam, social engineering.
5	Data backup and storage	Backup interval and how long it will be stored
6	Incident management	What to do when incidents occurred and whom to contact.
7	Changes in system environment	Protection of hardware and infrastructure from accidents like flood, fire, and other physical issues such as dirt, dust and physical access.
8	User responsibility	Internal staff and business partners' responsibility.
9	Device security	Address both physical and wireless security issues.
10	Timely application of system patches	Applying patches update based on the vendor recommendation.
11	Supported/allowed software on organization systems	Identifies the list of allowed software to run in the bank.
12	Visitor control and physical access to spaces	Discuss applicable physical security policy and procedures, e.g., monitor or log visitors, challenge outsiders, report unusual activity.
13	Desktop security	Discuss use of screensavers, restricting visitors' view of information on screen preventing or

		limiting shoulder surfing, allowed access to systems.
14	Data transmission security	Specifies securing the data movement from one location to another.
15	File sharing and copyright	Peer-to-peer and bit-torrent programs including the legal consequences of illegal file sharing and downloading.

The proposed program has been evaluated by the Banks senior IT executives with special focus on the key findings, relevancy of selected topics and how to address them (the delivery techniques). As a result few of the proposed program candidate topics has been rephrased or restated to really address the awareness gaps. Tuning of the mapping between key findings and candidate topics were also performed. In addition, the delivery modes has been evaluated based on the Bank facility assessment which showed that there is no well-organized facility. For example, the organization doesn't have a separate training room equipped with resources. The awareness and training need has been identified, the short and long term program schedules has also been cleared. Furthermore, the frequency of delivery, and internal human resource and external party involvement to provide the program were also identified.

5.2 Delivery techniques for the awareness material

As Brodie and Wanner (2009) stated one of the best ways to make sure company employees will not make costly errors in regard to information security is to institute company-wide security-awareness initiatives that include but are not limited to classroom style sessions, security awareness website, helpful hints via e-mail, or even posters. These methods can help ensure employees have a solid understanding of company security policy, procedure and best practices. According to NIST (2003) many techniques exist to get an IT security awareness messages distributed throughout an organization. And the technique chosen depend upon resources and the complexity of the messages. Below are some techniques the organization may consider:

- Messages on awareness tools (e.g., pens, key fobs, post-it notes, notepads, diskettes with a message, bookmarks, clocks)
- Posters, "do and don't lists," or checklists
- Screensavers and warning banners/messages

- Desk-to-desk alerts (e.g., a hardcopy, bulletin distributed through the organization's mail system)
- organization wide e-mail messages
- Videotapes
- Web-based sessions
- Computer-based sessions
- In-person, instructor-led sessions
- IT security days or similar events
- Awards program (e.g. mugs, letters of appreciation)
- Pop-up calendar with security contact information, monthly security tips, etc.

According to NIST (2003) delivery techniques that offer the distribution of a single message include the use of awareness tools, posters, access lists, screensavers and warning banners, desk-to-desk alerts, organization wide e-mail messages and awards programs. While techniques that can more easily distribute a number of messages include "do and don't lists," newsletters, videotapes, web-based sessions, computer-based sessions and in-person instructor-led sessions. In addition to making awareness material interesting and current, repeating an awareness message and using a variety of ways of presenting that message can greatly increase users' retention of awareness lessons or issues. These techniques help ensure employees have a solid understanding of company security policy, procedure and best practices. They will also assist the organization to raise information security awareness of employees, improve their knowledge, and change their attitude and behavior.

CHAPTER SIX

CONCLUSION AND RECOMMENDATION

The final chapter presents the conclusion of the study and the recommendation based on the findings of the research. Furthermore, the chapter proposes possible ideas for future studies.

6.1 Conclusion

This paper tried to overcome issues that human are the weakest link in information security and are a major threat for organizations information security by proposing employees security awareness program. Information security awareness program is one way of overcoming this critical issue. The proposed program will assist the Bank in terms of creating information security awareness and good practices to its employees to strengthen its security by mitigating vulnerabilities for computer attacks. The researcher asked three questions; What is the current information security awareness creation practice in Enat Bank? What should the topics of an information security awareness program for Enat Bank be? And How should the information security awareness program be organized to deliver the necessary information to Enat Bank employees? The researcher used a quantitative research approach using a case study method and questionnaire as a data collection technique to meet the desired objectives such as review existing information security awareness programs, review the current practice of information security awareness in the Bank and propose a program that will guide information security awareness for Enat Bank.

The key findings are categorized into two categories general and technical. In the general category first section "security incident and reporting" the respondents have unsatisfactory knowledge of safe internet usage and incident response. In "email security" employees knowledge to phishing attack links is poor. In "safely use of internet and computer" personal computers security precautions are not practiced good enough, password management is also poor and most of employees are unable how to distinguish whether a website is safe to surf or not. In "threats and preventive measures" respondent security practices are below average. For instance updating software, antivirus usage, security scanning and backup are not performed regularly in a timely manner. In "password management and security" respondents' password setting, changing and protection practices are unsatisfactory. In "information security terms and social engineering" section respondents' knowledge to information security responsibility and social engineering needs improvement.

In technical category “security standards, procedures and training” section the organization doesn’t use information security standards, doesn’t have well-organized procedures in case of cyber-attacks and employees are not being trained of information security. In “firewall, IPS, penetration and traffic control” the organization is not performing internal and external penetration testing. The implementation and usage of IPS/IDS and web filtering is unsatisfactory. In “wireless network security” the organization wireless network implementation and security management are not good. In the rest six sections multiple security features are not implemented enough to strengthen the organization security posture such as port-based filtering, enabling port security, disabling unused ports etc. Ignoring these important issues may cause vulnerabilities to multiple cyber-attacks such as denial of service attacks and a business down time which is unacceptable to a financial institution. Overall the employees’ information security awareness is not satisfactory and needs to be dealt with such kind of programs to protect its assets or even its business.

6.2 Recommendation

The findings may assist the organization to really consider the concerns and act responsibly. The proposed program can be used as-is or as a guideline with minor modification based on the organization decision makers interest. The program needs to be implemented and be practical so that to get solutions related to employees awareness to information security.

When it comes to Enat Bank contextual factors such as IT infrastructure and environmental factors influence the delivery techniques. As discussed, security awareness programs should be tailored based on the organization needs and functions. As a result of IT executives’ evaluation the lack of an isolated awareness and training room during the Bank facility assessment, the Bank needs to prepare a facility that is well-organized and equipped with resources. Since employees have overall unsatisfactory result towards information security awareness, all candidate topics have been decided to be provided to employees to create exposure. It is recommended that they shall be addressed in short term schedule with continuous frequency to create exposure towards security awareness. Awareness and training needs were also checked and some of the topics are identified as training is more feasible to address them. These are Data transmission security, Timely application of system patches, Backup and storage, Device security and Changes in system environment. Internal human resource and external party such as partners’ involvement to provide the program was also identified and topics such as Data backup and storage, Incident management, Changes in

system environment, Device security, Timely application of system patches and Data transmission security are identified to be provided by both in-house and outsourcing companies. While the rest topics are identified as to be addressed by internal human resources mainly by the Bank senior IT executives and IT security office.

Once implemented information security awareness programs can quickly become obsolete if sufficient attention is not paid to technology advancements (NIST, 2003). Therefore, senior and middle managements need to have a continuous follow up and improvements since change is constant. End-users should be supported with the awareness program to protect the organization information. They should get trainings on security incidents and what to do if occurred. Employees need to have knowledge about safely use of internet and computer including password management and personal computer security precautions. The organization should aware its employees regards threats and their preventive measures such as file sharing software and their risks, updating software, types of antivirus and security scanning intervals, taking backup on regular basis. Employees should also be informed about information security responsibilities. Phishing attacks and social engineering attacks should be taught in a continuous manner since the ways these kinds of attacks occurred are complex and dynamic. Technical staffs need to consider the implementation of security standards and technologies such as web application and database firewall, data loss protection etc… to protect and secure the organization webservers, application servers and have a standard in performing tasks. Technical staffs needs to have knowledge how to perform security hardening such as internal and external penetration testing, configuring, implementing and monitoring IPS/IDS, web filtering, port security to overcome attacks such as denial of service, MAC overflow and man-in-the-middle attacks which sometimes have a huge amount of destruction to the business.

Top and middle managements should monitor the proposed program and update it as the technology advances. A security awareness program that didn't get the management support will not survive a day. Managements are the one who influence and guide the staffs below them. In addition, technical staffs must take security trainings to get a better result in short term by configuring and implementing security hardenings. The program can be delivered annually, semiannually or even quarterly depending on the Bank interest, gap and budget to mention few.

6.3 Future works

This research paper proposed information security awareness program for Enat Bank using frequency analysis technique. However, for future researches analyzing the survey data using cross tabulation analysis will help to review the relationships and significance of the variables. In addition, researchers can wider the scope to incorporate all financial institutions to have a generic information security awareness program.

REFERENCES

Abdyli, F. (2014). *How Ready are Banks in The Republic of Kosovo to Implement an Information Security Policy?* Thesis work, University of Ljubljana, Ljubljana.

Alageel, S. M. (2003). *Development of an Information Security Awareness Training Program for The Royal Saudi Naval Forces (RSNF).* Thesis work, Naval Postgraduate School, Monterey, California.

Al-Alawi, A. I., Al-Kandari, S. M., & Abdel-Razek, R. H. (2016). Evaluation of Information Systems Security Awareness in Higher Education: An Empirical Study of Kuwait University. *Journal of Innovation and Business Best Practice, 2016*, 1-23. doi:10.5171/2016.329374

Alnatheer, M., & Nelson, K. (2009). A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context. *Proceedings of the 7th Australian Information Security Management Conference, 7*, pp. 6-17. Perth, Western Australia.

Amare, B. (2015). *Assessment of Insider Threat in Ethiopian Banking Industry.* Thesis work, Addis Ababa University, Addis Ababa.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If Someone is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security. *European Journal of Information Systems, 18*, 151–164. doi:10.1057/ejis.2009.8

Brodie, C., & Wanner, R. (2009). *The Importance of Security Awareness Training.* SANS Institute Reading Room Site.

Chang, A. J.-T., & Yeh, Q.-J. (2006). On security Preparations Against Possible IS Threats Across Industries. *Information Management and Computer Security, 14*(4), 343-360.

Chen, C. C., Shaw, R. S., & Yang, S. C. (2006). Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System. *Information Technology, Learning, and Performance Journal, 24*(1), 1-14.

Connolly, A. Y., Lang, M., & Tygar, D. J. (2017). The Impact of Procedural Security Countermeasures on Employee Security Behaviour: A Qualitative Study. *International Conference on Information Systems Development (ISD2017 Cyprus), 26*, pp. 1-12. Cyprus.

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

Creswell, J. W. (2013). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). California: SAGE Publications, Inc.

D'Aubeterre, F., Singh, R., & Iyer, L. (2008). Secure Activity Resource Coordination: Empirical Evidence of Enhanced Security Awareness in Designing Secure Business Processes. *European Journal of Information Systems, 17*(5), 528-543.

Da Veiga, A. (2015). The Influence of Information Security Policies on Information Security Culture: Illustrated through a Case Study. *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015), 9*, pp. 22-33.

Dawson, C. (2002). *Practical Research Methods.* Oxford, United Kingdom: How To Books Ltd.

Diver, S. (2007). *Information Security Policy – A Development Guide for Large and Small Companies.* SANS Institute.

Durmus, A. (2014). *The Observation of Information Security Awareness in Turkey.* Thesis work, Cankaya University, Ankara.

Enat Bank. (2017). *Enat Bank Annual Report.* Addis Ababa: Central Printing Press.

Gebrehawariat, D. (2017). *Assessment of The Effectiveness of Information Security Management in The Ethiopian Financial Sector: Card Banking Security in Focus.* Thesis work, Addis Ababa University, Addis Ababa.

Gundu, T., & Flowerday, S. (2013). Ignorance to Awareness Towards an Information Security Awareness Process. *SAIEE Africa Research Journal, 104*(2), 69-79.

Haeussinger, F. (2015). *Studies on Employees' Information Security Awareness.* Dissertation, Georg - August - University, Göttingen.

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and Effectiveness of Organizational Information Security Measures. *Information Management and Computer Security, 16*(4), 377-397.

Herath, T., & Rao, H. R. (2009). Protection Motivation and Deterrence: A framework for Security Policy Compliance in Organisations. *European Journal of Information Systems, 18*(2), 106-125.

InstantSecurityPolicy. (2008). The IT Security Policy Guide: Why you need one, what it should cover, and how to implement it. North Carolina, North Carolina, USA.

ISF. (2007). The Standard of Good Practice for Information Security. London, London, United Kingdom.

ISO/IEC . (2013). *NEN-ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems -.* Switzerland: ISO/IEC .

Jones, A. (2010). How do you make information security user friendly? *Information Security Technical Report, 14*(4), 213-216.

Kankanhalli, A., Teo, H., Tan, B., & Wei, K. (2003). An Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management, 23*(2), 139-154.

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information Security Threats and Practices in Small Business. *Information Systems Management, 22*(2), 7-19.

Kothari, C. (2004). *Research Methodology: Methods and Techniques* (2nd Revised ed.). New Delhi: New Age International (P) Ltd.

Kruger, H., Drevin, L., & Steyn, T. (2006). A Framework for Evaluating ICT Security Awareness. *ISSA,* (pp. 1-11). Potchefstroom.

Mahncke, R. J., McDermid, D. C., & Williams, P. A. (2009). Measuring Information Security Governance Within General Medical Practice. *Proceedings of the 7th Australian Information Security Management Conference, 7*, pp. 63-71. Perth, Western Australia.

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

Negussie, A. (2015). *Practices, Challenges And Prospects Of Information Security Policy In Ethiopian Banking Industry.* Thesis work, Addis Ababa University, Addis Ababa.

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). *National Institute of Standards and Technology Special Publication 800-12 Revision 1*. Gaithersburg: NIST.

NIST. (2003). *Building an Information Technology Security Awareness and Training Program.* Gaithersburg: U.S. Government Printing Office.

Payne, S. (2003). Developing Security Education and Awareness Programs. *Educause Quarterly, 26*(4), 49-53.

PCI Security Standards Council. (2014). *Information Supplement: Best Practices for Implementing a Security Awareness Program.* PCI Security Standards Council.

Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *Information Systems Security, 14*(2), 37-49.

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly, 34*(4), 757-778.

PwC. (2014). *Managing Cyber Risks in an Interconnected World: Key Findings from The Global State of Information Security Survey 2015.* PwC.

SANS Institute. (2018, May 15). *About Us: SANS Institute*. Retrieved from SANS Institute Web site: https://www.sans.org/

Siponen, M. (2000). A conceptual Foundation for Organizational Information Security Awareness. *Information Management & Computer Security, 8*(1), 31-41.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer, 43*(2), 64-71.

Son, J.-Y. (2011). Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to Follow IS Security Policies. *Information and Management, 48*(7), 296-302.

Sumner, M. (2009). Information Security Threats: A Comparative Analysis of Impact,Probability, and Preparedness. *Information Systems Management, 26*(1), 2-12.

Swartz, N. (2007). Protecting Information from Insiders. *Information Management, 41*(3), 20-24.

Symantec. (2016). *Internet Security Threat Report.* Mountain View, CA: Symantec Corporation.

Tebkew, K. (2013). *Information Security Management Framework For Banking Industry In Ethiopia.* Thesis work, Addis Ababa University, Addis Ababa.

Tse, W. D., Hui, M., Lam, S., Mok, Y., Oei, W., Tang, K., & Yau, X. (2013). Education in IT Security: A Case Study in Banking Industry. *GSTF Journal on Computing (JoC), 3*(3), 21-30.

Von Solms, B. (2006). Information Security – the fourth wave. *Computers and Security, 25*(3), 165-168.

Vroom, C., & Von Solms, R. (2004). Towards Information Security Behavioural Compliance. *Computers and Security, 23*(3), 191-198.

Woretaw, A., & Lessa, L. (2012). Information Security Culture in The Banking Sector in Ethiopia. *5th ICT 2012 Ethiopia Conference,* (p. 22 pages). Addis Ababa.

Xiong, P. (2011). *Building a Successful Information Security Awareness Programme for NLI.* Thesis work, Gjøvik University College, Gjøvik.

Yamane, T. (1973). *Statistics, An introductory analysis* (2nd ed.). New York: Harper and Row.

APPENDICES

Appendix A: General category questionnaire

Questionnaire on Designing Information Security
Awareness Program for Enat Bank in Ethiopia
General Questionnaire

Dear Respondent,

I am Milkyas Bogale, a postgraduate student. Currently, I am attending Master of Science in Information Science at Addis Ababa University, Ethiopia.

As part of my accomplishment for the program, my research lies on designing information security awareness program for Enat Bank S.C. Therefore, this is to kindly ask you to participate in the survey that needs data from your esteemed bank to assess the issues in relation to Information Security Awareness.

This survey is anonymous. No one, including the researcher, will associate your responses with your identity. Your participation is voluntary. You may choose not to take the survey, to stop responding at any time, or to skip any question that you do not want to answer. Your response is extremely important and valuable for the success of the research to achieve the objective of the study by indicating possible gaps, if any, and possible solutions that need to be taken by concerned parties.

Therefore, I appreciate if you spend few minutes from your valuable time according to the instruction for each part.

If you require any assistance or clarification, please don't hesitate to contact me through either of the following methods. Tel: 0913-01-93-92 or Email: milkyasb@gmail.com

Thank you for your kind contributions in advance.

Please choose the appropriate answer and circle the letter of your choice.

CHAPTER 1 – DEMOGRAPHIC FEATURES	
Q1.Your gender?	a. Male b. Female
Q2.Your age?	a. 18 – 24 b. 25 – 34 c. 35 – 44 d. 45 – 54 e. >55
Q3. What is your professional qualification?	a. Diploma/Level IV b. BA/BSc c. MBA/MA/MSc d. PhD
Q4. Which of the following job categories indicate your current position?	a. Management level b. Senior level c. Officer level d. Junior level
Q5.Your working experience?	a. 0-1 year b. 1-3 years c. 3-5 years d. 5-10years e. Above 10 years

CHAPTER 2 – SECURITY INCIDENT AND REPORTING	
Q6.Do you use internet?	a. Yes b. No
If you chose option 'b' in previous question, skip to 10th question. Go ahead otherwise.	
Q7.How much time do you spend on the Internet?	a. Very Little b. Little c. Average d. Much e. Very Much
Q8.Do you have a membership for any social media platform like Facebook, Twitter, Instagram and so on?	a. Yes b. No
If you chose option 'b' in previous question, skip to 10th question. Go ahead otherwise.	

Q9.Which personal information that you mostly share in social media? (You can select more than one option)	a. Picture b. Video c. Name, surname d. Birthdate e. Name, surname of family members f. Identification number g. Phone number h. E-mail address i. Researches/studies j. Emotions k. Thoughts l. Hobbies
Q10.Have you ever faced with incident about information security?	a. Yes b. No
Q11.Do you think that you will probably face with such incidents in the future?	a. Yes b. No
Q12.You faced with a content or post in a social media or a website that violate your personal rights[1]. Where do you report?	a. My family and/or friend b. The nearest police department c. Relative website admin d. Internet Service Provider e. Cyber Security Office (Information Network Security Agency-INSA) f. Prosecution Office g. I do not know where to report h. I do not report
Q13.When you faced with unwanted content or post (encourage/help suicide and prostitution, harmful drugs, gambling, nudity, sexual harassment and crimes against Ethiopia etc.). Where do you report?	a. My family and/or friend b. The nearest police department c. Relative website admin d. Internet Service Provider e. Cyber Security Branch Office (Information Network Security Agency-INSA) f. Prosecution Office g. I do not know where to report h. I do not report
CHAPTER 3 – E-MAIL SECURITY	
Q14.Do you use e-mail address?	a. Yes b. No
If you chose option 'b' in previous question, skip to 19th question. Go ahead otherwise.	
Q15.What is Email Spam?	a. Spam is an antivirus solution b. Spam is a firewall c. Spam is an unwanted and mass e-mails d. Spam is an e-mail attachment

[1] Personal rights – According to Merriam-Webster dictionary "rights (as of personal security, personal liberty, and private property) appertaining or belonging to the person".

Q16.What do you do when you got an e-mail asking to update your personal info by clicking the link in the e-mail body?	a. I click the link if logo and address of the bank is right b. I do the same if my close friends update their info c. I make a call to bank to get information about the e-mail d. I do not have any idea
Q17.What do you do when you got an e-mail saying that a little girl is lost for a while and ask you to forward the e-mail as many people as you can?	a. I forward to all of my contacts b. I forward to closest contacts c. I create a new post to ask sender not to forward chain e- mail d. I do not have any idea
Q18.What do you do when you got an e-mail from your friend but file extension of the attachment and domain name of the address (the section after '@' sign) is weird?	a. It is safe to open up attach as the sender is friend of mine. b. I reply to e-mail to confirm if it is really sent by my friend c. I create new post to send to my friend's address in my contact to for confirmation d. I do not have any idea

CHAPTER 4 – SAFELY USE OF INTERNET AND COMPUTER	
Q19.Which precautions do you take in case your laptop is stolen?	a. Keep its physical (MAC) address b. Keep its serial number c. Backup my sensitive data d. Encrypt my sensitive data e. Install an alarm software f. Set passwords for my user accounts g. Mark a sign to unrecognizable place on my laptop h. Install a GPS software to trace remotely
Q20.Do you lock your user account with password when you took a little break from work or leave your seat?	a. I only lock in my business laptop b. I only lock in my personal computer c. I use it in both d. I do not lock as I go back to work in short time e. I do not lock as my data is not that critical
Q21.How do you distinguish if a website is a safe to surf or not?	a. Websites that offer freeware are safe b. Online casinos are safe c. It is safe if a security logo exists d. It is safe if the web browser shows small gold lockpad e. It is safe if its address starts with "https://" instead of "http://" f. It is safe if it appears to be popular g. I am having difficulty in distinguishing
CHAPTER 5 - THREATS AND PREVENTIVE MEASURES	
Q22.Have you ever used file sharing software like uTorrent, BitTorrent, eMule and so on?	a. Yes b. No
If you chose option 'b' in previous question, skip to 24th question. Go ahead otherwise.	

Q23.Which ones are the threats originated by file sharing software?	a. I may violate copyright of music, video or any other software b. The program I downloaded may include malicious software c. I may allow bad guys with bad intentions to see my personal data
Q24.What do you think about updates of your types of software installed in your computer?	a. I install at once if there is available update b. I install few days later after I take care of my other tasks c. I get help from my closest friends d. I do not have any idea
Q25.What type of antivirus software do you use in your computer?	a. I use free antivirus software b. I use cracked antivirus software c. I use license paid antivirus software d. I do not use antivirus software e. I do not have any idea
If you chose option 'd' in previous question, skip to 27th question. Go ahead otherwise.	
Q26.How often do you make security scanning in your computer?	a. Never b. Rare c. Average d. Often e. Very often
Q27.How often do you backup your data in your computer?	a. Never b. Rare c. Average d. Often e. Very often
Q28.Which one of the statements below is true?	a. Only firewall is sufficient in a computer b. Only antivirus software is sufficient in a computer c. Both antivirus software and firewall perform same functionalities d. Both antivirus software and firewall need to be used updated in a computer
CHAPTER 6 - PASSWORD MANAGEMENT AND SECURITY	
Q29.What do you think about changing your passwords?	a. I change my password only if I doubt that somebody stole it b. Changing process is boring c. I change my password regularly d. I change my password only if I have to give it to my friend
Q30.How do you set your password?	a. I use the password preset by the system b. I set short password not to forget c. I set all of my passwords same not to forget d. I set my password including upper, lower letters, numbers and special characters e. I set my passwords with 8 characters at least if the system allows f. I use password generator tool

Q31.With whom do you share your computer's authentication password?	a. I share with my trusted friend b. I share with my trusted relative c. I share with IT division in my corporate d. I don't share with anyone
CHAPTER 7 - IS TERMS AND SOCIAL ENGINEERING	
Q32.Who is responsible for Information Security?	a. Information owner b. Information user c. Information manager
Q33. "A chain is as strong as its weakest link." What does this motto mean to you?	a. It could cause security vulnerability if an IT personnel walk out b. An information security awareness level in a place is as much as a person who has least information security knowledge in place c. Information security is provided only if you have skilled technical team d. A corporate can be exposed to vulnerability if an untrusted employee is recruited
Q34.What does "social engineering" mean?	a. It is a security add-on checking if a website is safe b. It is an art of deception that makes use of getting information that need to be kept secret in normal circumstances by using convincing and influencing abilities c. To be exposed to insultation by an entity you have just met on social media

***

Appendix B: Technical category questionnaire

Questionnaire on Designing Information Security
Awareness Program for Enat Bank in Ethiopia
Technical Questionnaire

Dear Respondent,

I am Milkyas Bogale, a postgraduate student. Currently, I am attending Master of Science in Information Science at Addis Ababa University, Ethiopia.

As part of my accomplishment for the program, my research lies on designing information security awareness program for Enat Bank S.C. Therefore, this is to kindly ask you to participate in the survey that needs data from your esteemed bank to assess the issues in relation to Information Security Awareness.

This survey is anonymous. No one, including the researcher, will associate your responses with your identity. Your participation is voluntary. You may choose not to take the survey, to stop responding at any time, or to skip any question that you do not want to answer. Your response is extremely important and valuable for the success of the research to achieve the objective of the study by indicating possible gaps, if any, and possible solutions that need to be taken by concerned parties.

Therefore, I appreciate if you spend few minutes from your valuable time according to the instruction for each part.

If you require any assistance or clarification, please don't hesitate to contact me through either of the following methods. Tel: 0913-01-93-92 or Email: milkyasb@gmail.com

Thank you for your kind contributions in advance.

Please choose the appropriate answer and circle the letter of your choice.

CHAPTER 1 – DEMOGRAPHIC FEATURES	
Q1.Your gender?	a. Male b. Female
Q2.Your age?	a. 18 - 24 b. 25 - 34 c. 35 - 44 d. 45 - 54 e. > 55
Q3.What is your professional qualification?	a. Diploma/Level IV b. BA/BSc c. MBA/MA/MSc d. PhD
Q4. Which of the following job categories indicate your current position?	a. Management level b. Senior level c. Officer level d. Junior level
Q5.Your work experience?	a. 0-1 year b. 1-3 years c. 3-5 years d. 5-10 years e. Above 10 years
CHAPTER 2– SECURITY STANDARDS, PROCEDURES AND TRAINING	
Q6.Which security technologies do you use in your organization? (You can select more than one option)	a. Antivirus software b. Firewall appliance c. Web Application Firewall d. Database Firewall e. Data Leakage Prevention f. Antispyware software g. Virtual Private Network h. Vulnerability/Patch Management i. Data encryption on storage units j. Web / URL filtering k. Application Firewall l. Log management software m. End point security / NAC (Network Admission Control) n. Data loss prevention / content monitoring o. Server-based ACLs (Access Control Lists) p. Information Forensic Tools q. Public Key Infrastructure (PKI) r. Smart cards and keys s. Wireless security t. Virtualization specific tools u. Static accounts user name and passwords v. Biometric w. Information Security Management System x. Other

Q7.Do you follow a standard for network and information security in your organization? (You can select more than one option)	a. ISO/IEC 27001/2 b. PCI DSS (Payment Card Industry Data Security Standard) c. COBIT (Control Objectives for Information Technology) d. NIST (National Institute of Standards and Technology) e. Another information security standard f. None g. I do not have any idea
Q8. Do you have any procedure in case your systems are being exposed to cyber-attack?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q9. Which information security policies do you put into practice in your organization?	a. Network policies b. User policies c. Laptop policies d. Intrusion Detection/Prevention policies e. Patch/Updating policies f. Another policy g. None of them h. I do not have any idea
Q10. Are your employees being trained about information security awareness?	a. Yes b. Sometimes c. No d. Another
If you chose option 'c' in previous question, please skip to 12th question. Go ahead Otherwise	
Q11. How often do you train your employees about information security?	a. Once a year b. Once a week c. Few times a year d. Once a month
Q12. Do you follow any resources, materials for oncoming technologic news and developments?	a. I follow some resources at home b. I subscribe to news bulletins and get e-mail regularly c. I benefit from the organization web portal d. I sometimes follow magazines e. Organization training is enough for me f. I do not follow any resource g. Another
Q13.Have you ever experienced any security incident in your organization network? (e.g. threat, attack, malicious software) If any, how many times did you face?	a. 1- 5 times b. 6-10 times c. More than 10 d. Never experienced
Q14. How long does it take to close the security breaches?	a. Between 0- 3 months b. Between 3-6 months c. Between 6-9 months d. Between 9-12 months
CHAPTER 3- FIREWALL, IPS, MANAGEMENT, PENETRATION AND TRAFFIC CONTROL	

Q15. Do you use SSL encryption?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q16. Do you use Virtual Private Network (VPN) on your network?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q17. Do you perform daily logging on your wired network?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q18. Do you use xflow protocols on your network? (e.g. Netflow, netstream, sflow)	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q19.Do you use authentication protocol in your network structure? (You can select more than one option)	a. TACACS/TACACS+ b. We do not use c. RADIUS d. Smart Card e. Biometric f. We use another authentication protocol g. I do not have any idea
Q20. Do you make penetration test for web environment?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q21. Do you make necessary filtering for web software?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q22. Do you apply CoPP (Control Plane Policy)/CPU on your network appliances?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q23. Is your network infrastructure wired or both wired and wireless?	a. Only wired b. Both wired and wireless
Q24. Do you have IPS or IDS appliance on your wired network?	a. We do not use any of them b. We have IPS appliance but IDS c. We have IDS appliance but IPS d. We use both appliances e. I do not have any idea
CHAPTER 4- WIRELESS NETWORK SECURITY	

Q25. Do you have wireless IPS or IDS appliance on your wireless network?	a. We do not use any of them b. We have IPS appliance but IDS c. We have IDS appliance but IPS d. We use both appliances e. I do not have any idea
If you did not chose options 'b' or 'd' in both 24th and 25th questions, please skip to 27th question	
Q26. Are your wired and wireless IPS appliances integrated each other?	a. Yes b. No
Q27. Do you use guest portal on your wireless network?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q28. Do you perform daily logging on your wireless network?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q29. Do you use WEP on your wireless network security?	a. Yes b. No c. We use another technology/method d. I do not have any idea
CHAPTER 5- OSI APPLICATION LAYER SECURITY (LAYER 7)	
Q30. Do you use voice applications?	a. Yes b. No c. We use another technology/method d. I do not have any idea
If you chose option 'b' in previous question, please skip to 32nd question	
Q31. Are they encrypted?	a. Yes b. No c. We use another technology/method d. I do not have any idea
CHAPTER 6- OSI TRANSPORT LAYER SECURITY (LAYER 4)	
Q32. Do you find port-based filtering enough?	a. Yes b. No c. We use another technology/method d. I do not have any idea
CHAPTER 7- OSI NETWORK LAYER SECURITY (LAYER 3)	

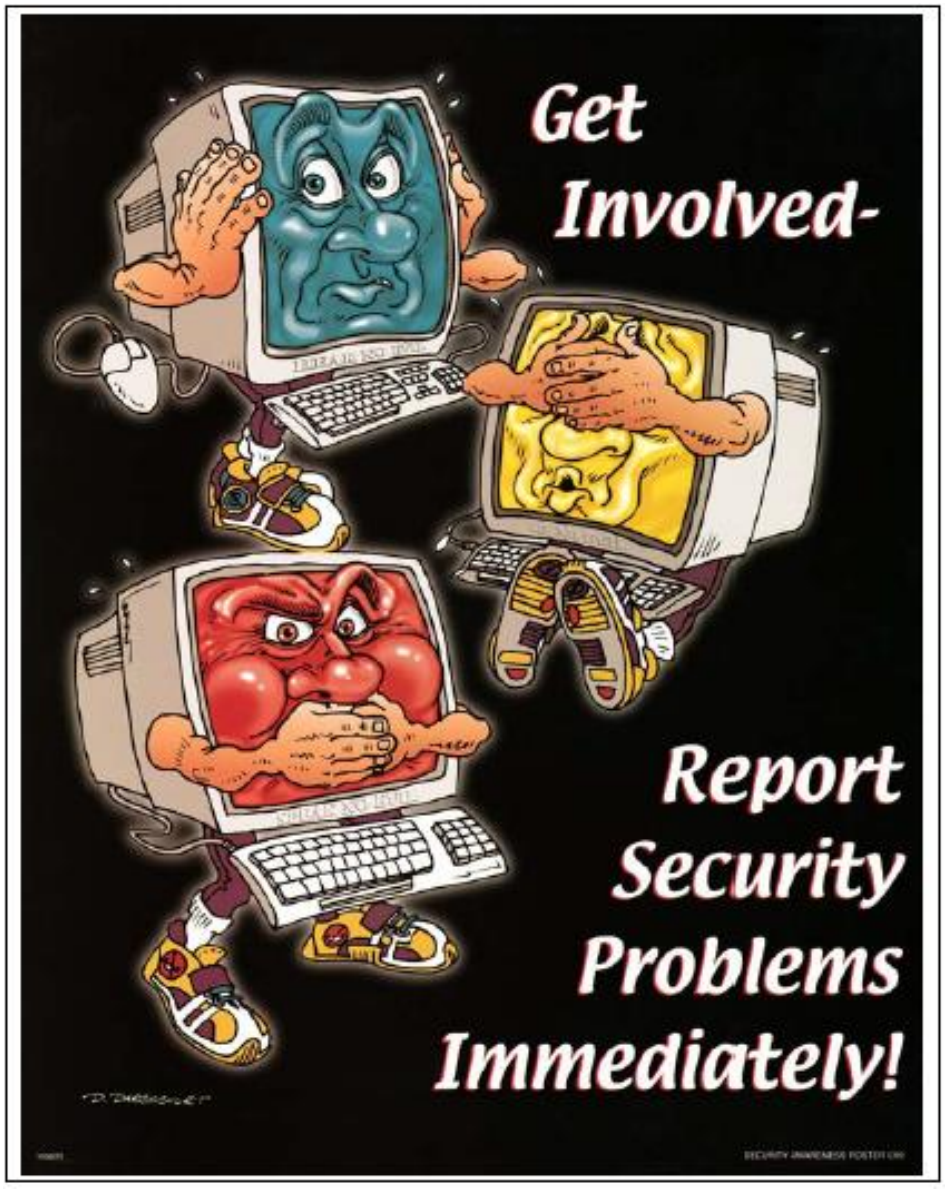
Q33. Which security feature is configured on your Layer 3 Switches or routers?	a. uRPF (Unicast Reverse Path Forwarding) b. ICMP redirection c. ACL (Access Control List) d. Fragmentation attack prevention e. Teardrop prevention f. We do not use these g. Another technology
Q34. Is authentication configured on your routers?	a. Yes (MD5) b. Yes (Clear text) c. No d. We do not use router
CHAPTER 8- OSI DATA LINK LAYER SECURITY (LAYER 2)	
Q35. Are unused ports disabled?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q36. Is port security enabled on your network?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q37. Do you use only one VLAN on your network?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q38. Do you use Private VLAN (PVLAN) on your network?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q39. Do you use 802.1x protocol on your network?	a. Only in wired network b. Only in wireless network c. In both of them d. None of them e. We use another protocol f. I do not have any idea
Q40. Do you use protected port?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q41. Is DHCP Snooping enabled on your network?	a. Yes b. No c. We use another technology/method d. I do not have any idea

Q42. Is ARP Inspection enabled on your network?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q43. Is IP Source Guard enabled on your network?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q44. Is Root Guard enabled on your network?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q45. Is Loop Guard enabled on your network?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q46. Do you use Storm Control feature on your network?	a. Yes b. No c. We use another technology/method d. I do not have any idea
CHAPTER 9- OSI PHYSICAL LAYER SECURITY (LAYER 1)	
Q47. Is MAC Security configured on your network?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q48. Do you perform user id authentication in all of the gates of your organization?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q49. Do you have any user authentication mechanism at the entrance of system rooms?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q50. Do you use shredder to destroy your institution documents?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q51. Do you have fire sensors in system rooms?	a. Yes b. No c. We use another technology/method d. I do not have any idea

Q52. Do you have cooling sensors in system rooms?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q53. Do you have power redundancy in system rooms?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q54. Do you have cameras in system rooms?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q55. Are the cabinets locked in system rooms?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q56. Do you label the cables plugged in to network devices?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q57. Do you have disaster recovery center?	a. Yes b. No c. We use another technology/method d. I do not have any idea
CHAPTER 10- END POINT SECURITY	
Q58. Do you use a technique that prevents passwords from holding in RAM?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q59. Do you use BIOS password in end point stations?	a. Yes b. No c. We use another technology/method d. I do not have any idea
Q60. Do you get WHOIS service?	a. Yes b. No c. We use another technology/method d. I do not have any idea

***

Appendix C: Examples of security awareness posters



Source: *(NIST, 2003)*

PinKEY Doesn't Open E-Mail From STRANGERS.

She Also Does NOT Send Files Ending In:
.VBS, .SHS, .SCR, .EXE, .BAT, .COM, .PIF, .LNK, .SHB, .VB, .WSH, .WSF, .WSC, .SCT, OR .HTA,
As Attachments to Her Emails.

http://www.ihs.gov/cio/itsecurity/posters/index.cfm

ITS Information Technology Security
Sponsored by Indian Health Service

Appendix D: Support request letter

አዲስ አበባ ዩኒቨርሲቲ
የተፈጥሮ ሳይንስ ኮሌጅ
የኢንፎርሜሽን ሳይንስ ት/ቤት

ADDIS ABABA UNIVERSITY
College of Natural Science
School of Information Science

Date March 20, 2018
Ref:-SIS/21 /2010

March 21, 2018

To: Enat Bank S.C
Addis Ababa

Dear Sir / Madam

Student Milkyas Bogale (ID. No. GSE/0392/08) is a graduate student at the School of Information Science, Addis Ababa University. He is currently conducting a MSc. thesis research under the title "Designing Information Security Awareness Program for Enat Bank in Ethiopia".

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

With Regards,

Martha Yifiru (PhD)
Head, School of Information Science

✉: 1176 ☎: +251-(11)-122-91-91 ☎:2122- 91-92