Building an Information Security Awareness Program for a Bank: Case from Ethiopia

Completed Research Paper

Milkyas Bogale
Addis Ababa university, Ethiopia
milkyasb@gmail.com

Lemma Lessa
Addis Ababa university, Ethiopia
lemma.lessa@gmail.com

Solomon Negash
Kennesaw State University, USA
snegash@kennesaw.edu

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. While huge amounts of money is invested in technical solutions, organizations often pay too little attention to 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 for Enat bank in Ethiopia. The research tried to answer 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? A quantitative research approach with case study method is used. Findings showed that the information security awareness level of Enat Bank employees is unsatisfactory. 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. Hence, the researchers 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 bank to smoothly implement the program. Recommendations are also forwarded in short and long-term basis to improve the information security awareness of its employees.

Keywords

Security Awareness Program, Information Systems Security, Information Security Policy

Introduction

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, 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.

Problem Statement

Information is crucial asset of organizations and the protection of these assets became one of the major aspects that organizations have to face 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 (PricewaterhouseCoopers) 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.

Review of Related Works

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.

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).

In order to let employees familiar with complicated information security issues, Payne (2003) suggested that organizations should 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 awareness and training, e.g. conducting classroom sessions, seminars and workshop, distributing information security handbooks, etc. Meanwhile, Chen et al., (2006) suggested that a training could be delivered using an e-learning platform. A 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, it would emphasize more on employee involvement and effective communication instead of one-way content delivery (Chen et al., 2006). 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).

Research Design and Method

Research Design

The researcher used quantitative research approach to express employees' awareness level in terms of quantity. 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. 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). 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. 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). 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. 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. Then 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, when we substitute the numbers in the formula the sample size for Addis Ababa stratum is 157 and for outlying branches stratum 44.

Method

During the study, primary data were collected using a closed-ended questionnaire. 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. 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. Then 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 tries to assess the end users awareness level and identify gaps that needs to be filled with the appropriate measures. The technical category as the name implies focuses on technical matters and was distributed to the Bank's IT technical staffs to assess their awareness and review their current practices related to information security.

The researcher of this study used descriptive analysis. 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 collected data was edited, coded and classified using IBM SPSS tool. Frequency analysis was used for data analysis and presented in table format including frequencies and percentage.

Key Findings

Based on the information collected from the sampled branches using questionnaire, the gap towards information security awareness were identified and analyzed. As a result, summary of the findings are 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 doesn'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.

Proposed Information Security Awareness Program

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.

Hence, as shown in Table 1, the key findings of the analysis are associated with the candidate topics that must be included in the ISAP (Information Security Awareness Program) for Enat Bank.

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 doesn'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	Desktop security

are not practiced well enough	
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 copy right

Table 1: Key findings

Delivery Techniques for the Awareness Program

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 organizations 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.

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 (NIST, 2003).

Conclusion and Recommendation

This paper tried to overcome issues that employees 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. 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.

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. 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 also 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.

Future Works

This research 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.

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.

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.

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.

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.

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

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.

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

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.

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.

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.

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.

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.