Human Factors Influence in Information Systems Security: Towards a Conceptual Framework

Girma Abebe
Accounting and Finance Department
Rift Valley University, Ethiopia
Addis Ababa, Ethiopia
agirma747@gmail.com

Lemma Lessa
School of Information Science
Addis Ababa University
Addis Ababa, Ethiopia
lemma.lessa@aau.edu.et

Abstract

The importance of protecting information in banks and mitigating security breach is becoming more important than ever. Human factors represent essential issues in information systems security in organizations, since human factors determine the behavior of employees toward information systems security. Extant literature revealed that the human factor aspect is one of the emerging research areas in information security. Thus, this research tries to explore information systems security countermeasures that are used to reduce internal threat and how employees perceive them and create a human factors model to address human factor gaps in information systems security in commercial banks in Ethiopia. Accordingly, a conceptual human factor model is developed from literature. A qualitative case study research design is employed to validate the proposed conceptual framework in selected banks in Ethiopia. Purposive sampling is employed to select the sampled banks. The samples are selected based on eligibility criteria that the respondents should have experience and expertise in information systems security and the banking activities. The research contributes to the current knowledge of information security by demonstrating the importance and critical role of human factors in the development of an information systems security model. The main contribution would be the advancement of the theoretical and practical basis for information systems security in proposing a model framework for developing, assessing and modeling a human factor model. Furthermore, it improves the understanding of risks in the security incident stages in relation to human factors.

Keywords
Information Systems Security, Human Behavior, Information security Policy, Organizational Culture, Training

1. Introduction

Human factors represent essential issue in information systems security in organizations, since human factors determine the behavior of employees toward information systems security. The only application of information systems security technologies could not always result in the improved information systems security as security is largely associated with people. The interaction between human and information systems have always opened the chance for many security risks (Alhogail et al. 2015; Naidoo, 2020). To improve the security of information assets, an

understanding of the human factor is required. The framework by (Alhogail et al. 2015), provided a comprehensive view of the human issues that influence human behavior toward information security in organizations.

According to Pollock (2017) for many decades, researchers have identified that a human error is the significant cause of information systems security breaches, and also it still remains to be the major one issue today. The quantification of the effects of information systems security incidents is often the difficult task because the studies often overstate or understate the costs involved. A human error is always a cause of failure in many organizations and professions where it is ignored or overlooked as an inevitability. Moreover, there are so many causes of an information systems security breach related to human error such as poor awareness, boredom, lack of training, and lack of risk perception. But, human error might be unintentional because of some incorrect execution of a plan (slips/lapses) or of correctly following the inadequate plan (mistakes). Whether it is intentional or unintentional, errors could lead to the vulnerabilities and security breaches as stated in (Pollock, 2017). Hence, humans remain the weakest link in the process of interfacing with computers they operate and in keeping information systems secure.

The application of information systems security technologies do not always result in an improved information security. Human factors play significant role in the computer security, factors such as cognitive abilities, individual difference, and personality traits could impact behavior. Information systems security behaviors are also highly influenced by individual's perception of risk. All these factors are affected by the organization's information systems culture and security environment where they occur. These human factors interact with each other and they can result in human behaviors that are often detrimental to information security. Parsons et al. (2010), reveals the recommendations as to how the human and cultural factors could be influenced in more positive behaviors, and lead to more secured information systems environments (Parsons et al., 2010).

Dahlström (2008) states that the demand for increased security has escalated recently and comprehensive development of it as a field of operations, beyond potential technological progress, is needed. In spite of distinct differences in the nature of threats (intentional/unintentional), there are many areas (use of standardized procedures, human factors training, modeling for increased understanding of adverse events) where knowledge and experiences from safety operations can fruitfully spill over to security; to establish cooperation between these two fields, for example on regulatory and procedural development, training and simulation, as well as operational evaluation, would be to produce synergies not yet known today. From this conclusion, it is perceived to develop a model for human factors for organizations in general and banking industry in Ethiopia in particular in the research.

The findings from the study by Hadlington (2018), highlight the interplay between cyber security attitudes and behaviors of employees. Behaviors such as the use of the same password for multiple websites, sharing passwords with colleagues, and clicking on links in emails are all active parts of most information security policies, but are still evident in the sample. Aspects such as lack of skills, knowledge and awareness were seen as the key barriers for individuals engaging in active cyber security, presenting a pathway for further research in the area. The research and the tools presented within the study are intended to be used further in a practical manner and should be viewed as being reactive, not only in terms of the development of new technologies but also additional policies in the context of cyber security. Aiming to improve the existing employees' knowledge in banks about information systems security behaviour and to provide comprehensive guidance for effective information systems security management, this research answers the following research question: How human factors model be identified to address human factor gaps in information systems security? The general objective of the study is to identify human factors that guide the shaping of employees' information systems security behavior towards favourable information security culture.

2. Problem Statement

According to Calvin (2019) most business organizations lack a human factors program and remain inattentive to human centric issues and human related problems that are leading to cyber security incidents, significant financial losses, reputational damage, and lost production. The under appreciation and under exploration of human factors in cybersecurity threatens the existence of every business. (Nobles, 2019) cited in Calvin (2019) depicted cybersecurity attacks are mounting and intensifying; consequently, making most organizations vulnerable from a human factors viewpoint especially as cyber threat actors increasingly target human weaknesses and limitations. Even though organizations are investing substantially in cybersecurity technologies and services, most of them experience a cybersecurity incident due to the inattentiveness of human factors. Calvin (2019) also indicates that humans are the

weakest link and a critical vulnerability within cybersecurity; yet, most organizations fail to provide adequate human factors training so in truth this is an organizational induced vulnerability. The cybersecurity threat landscape is too hyperactive and perilous for businesses to continue to turn a blind eye to human factors in cybersecurity. Gratian (2018) on his part identified correlations between certain human traits and specific cyber security behavior intentions, which present a comprehensive study that examines how risk taking preferences, decision making styles, demographics, and personality traits influence the security behavior intentions of device security, password generation, proactive awareness, and updating. Therefore, the researcher believes similar scenario can be applied in the banking industry in Ethiopia.

Singh (2016) proves that the human factor is the major contributor to the data loss and data breach events. Many employees in the IT sector fall prey to the social engineering tactics of the attackers and end up compromising the confidentiality of the organizations' data. Negligence or minor wrong doing on part of the employees often leads to data breaches. However, the challenge is to devise new techniques that equip the employees against such wrong tactics. So there is clearly a need for further research in this area for improving cyber security. Pollock (2017) has also revealed that human error is complex and elusive information systems security problem that generally has resist the creation of a sound and standardized classification scheme. While human error can never be completely eliminated from the activities, they perform due to poor information systems awareness, or a lack of adequate information systems security training, the first step to make improvements over the status quo is to establish a unified scheme to classify such information systems security errors. The study also intended to develop the tool to gather data and apply the human factors analysis and classification system, a tool developed for the aviation accidents, to see if there is any latent organizational condition that led to the error. This analyzes historical data to find the common trends that can identify areas that should be addressed in an organization to reduce the frequency of errors (Pollock, 2017).

Aldawood (2019) examined factors that may contribute to overcoming the challenges posed by implementing training and awareness programs against social engineering. Staff social media access using such interconnected information systems can lead to increased threats of attack by malicious social engineers. The main objective of information security training and awareness programs is to enable employees to develop skills in identifying, disabling, and reporting any social engineering malicious attempts. The study further recommends strategies for addressing challenges from the point of view of security decision makers in organizations. Enhancing information security training and awareness programs can help organizations achieve better results against social engineering techniques Aldawood (2019). Metalidoua et al. (2014) acknowledged that employees of an organization are often a weak link in the protection of its information assets. Metalidoua et al. (2014) also noted that human factors do play a significant role in a computer security. The research, has also focused on the relationship between the human factor on information systems security presenting human weaknesses that might lead to the unintentional harm to organization and discuss how information systems security awareness can be a major tool in the overcoming of these weaknesses. Hence, the study also presented a framework of field research to identify human factors and major attacks that threat computer information security. Similarly, a framework can be presented for banks.

According to Soltanmohammadi (2013) human factors had a big portion among other factors, in information systems security in the health care industry of Malaysia. The research had tried to propose a new framework based on three factors: motivational factors, organizational factors and learning, and the research also suggest testing the proposed framework in other scopes to make highlight the importance of each variable. For future study, Soltanmohammadi (2013) recommends other researches emphasis on existing factors on human resource management, for example, the role of human resource management practices, job satisfaction and organizational commitment in improving information system security should be highlighted. Based on this finding the researcher perceives to propose a new framework based on the three factors: motivational factors, organizational factors and learning in commercial banks in Ethiopia.

According to Pham, H-C et al. (2017) employees' unsafe security behaviour has been considered the weakest link in overall security programs. Safe security practice and complying with security guidelines are essential to minimize security risks caused by the users. Future study should investigate a complex interaction between personal and organizational characteristics so that the security program can be developed where it can effectively engage employees with information systems security tasks even in a demanding work environment (Pham, H-C et al. 2017). Milkyas et al. (2019) conducted a study that revealed the information systems security awareness level of the employees of Enat Bank is unsatisfactory and the researcher has proposed a program that would assist the banks to create information systems security awareness and best practices to its employees in order to strengthen its information systems security

posture by mitigating the vulnerabilities of computer attacks. Moreover, the researcher has proposed an implementation strategy program to help the organization to implement the program. This can be extended to other commercial banks by developing a human factors program that is applicable to all banks through research.

Abiy et al. (2019) studied the level of existing information systems security culture in the banking sector in Ethiopia. The study showed that the information systems security awareness in the banking industry in Ethiopia is not satisfactory, which according to the study possibly emanates from inadequate information security communication and training. The researchers also recommended banks in Ethiopia should invest in effective information security training and information security policy awareness programs.

The identified research gap of past research, suggest that the need for further research in organizational information systems security in order to improve current understanding of the employees insecure behaviour, and identify what constitutes employees' behaviour of information security that can be used to devise a model that aid more effective information systems security behaviour in organizations. Accordingly, this research deals with information systems security countermeasures that are used to reduce internal threat and how employees perceive them and creates human factors model to address human factor gaps in information systems security in commercial banks in Ethiopia.

3. Proposed Conceptual Model

On the basis of literature review of the research areas outlined, the researchers created a model which divided behaviors into three categories: information systems policy, information systems culture and information systems awareness, factors that constitute information systems policy, culture and awareness and information systems security.

The study improves the current understanding of information systems security in commercial banks in Ethiopia by synthesizing the findings of the study to the theoretical framework presented in this thesis as an information systems security model (Figure 1). The model aims to increase the awareness of employees in information systems security.This can be achieved through channeling awareness through the model's abstracted information systems security framework and focusing on information security policy and cultural compliance towards information security. The framework proposed is also to determine the model for information security that might exist in commercial banks in Ethiopia. The proposed model (Figure 1) is developed in a comprehensive way to ensure an information systems security in banks. Bearing this in mind, the researchers are using critical concepts from information security culture framework (Tolah et al. 2017), Decision model from Aytes and Connolly (2003), the BYOD IS model on individual traits, Musarurwa & Flowerday, (2019), and mobile phone information security constructs from Ngoqo et al. (2015).

The proposed comprehensive conceptual model results from empirical investigation of commercial banks in Ethiopia. Moreover, the developed model assessed the previous published peer reviewed articles in depth and tried to address particular information systems security gap in banks that is discussed by this research paper in higher depth.

The research model of this research is illustrated below.

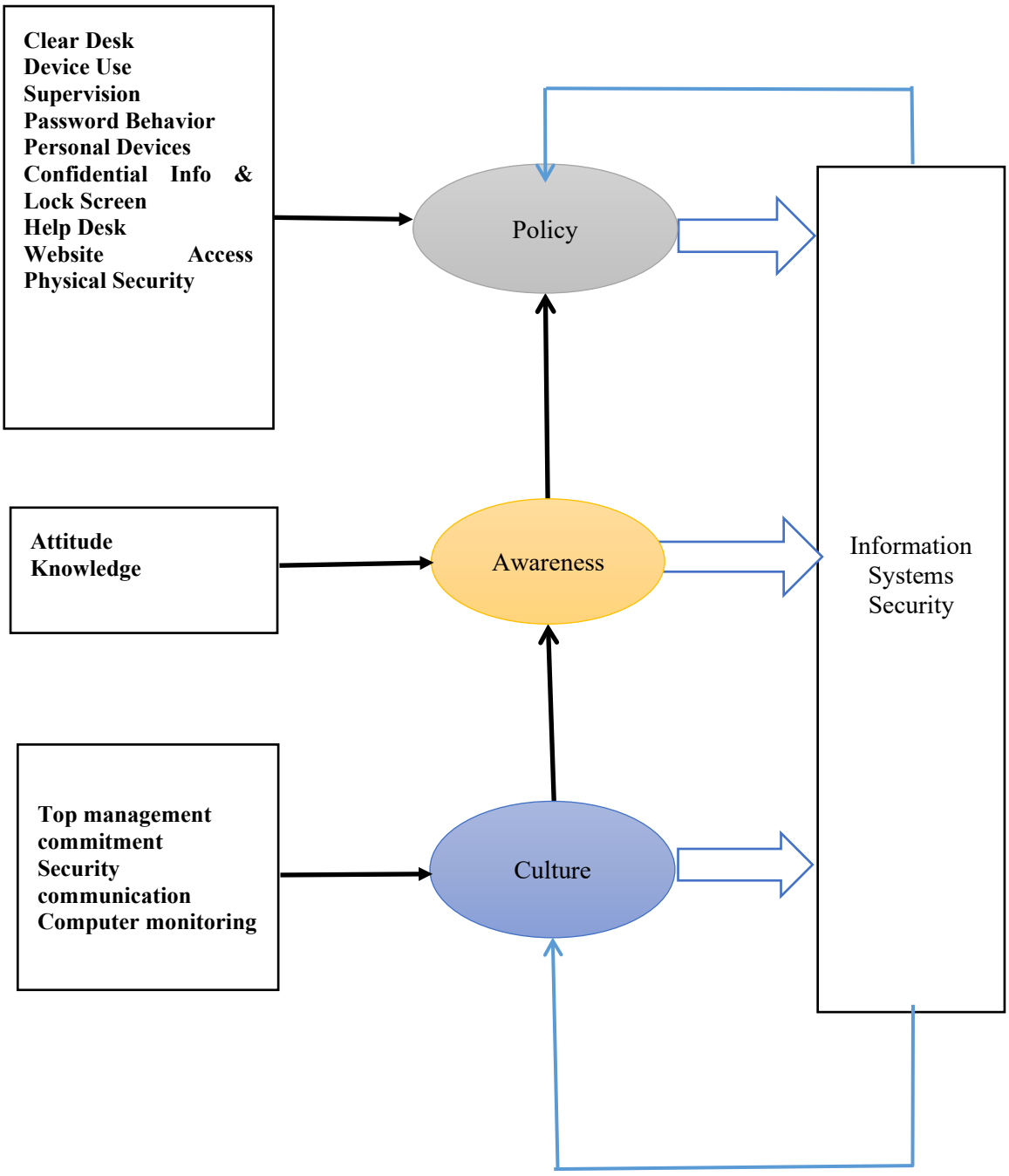

Figure 1: The proposed Conceptual Framework

The developed conceptual model (Figure 1), provides a holistic understanding of key elements that affect information systems security for banks. Information systems policy, culture and attitude are key issues that has to be understood

by the management of Commercial Bank of Ethiopia, Debub Global bank, Bank of Abyssinia, Nib bank, and Wegagen Bank. So that the information systems security gap can be clearly manifested. On the basis of the literature review the researchers have created the above comprehensive model which is divided in to four sections such as information systems security policy, information systems security awareness, information systems security culture and information systems security.

The following table shows the identified elements of the human behaviour areas and their relationship to information systems security:

Information Systems Policy	Information System Culture	Information Systems Awareness	
● Clear Desk Policy ● Device Use Policy ● Supervision ● Password Behavior ● Personal Devices ● Confidential Info & Lock Screen ● Help Desk ● Website Access ● Physical Security	● Password Sharing	● Attitude ● Knowledge	Information Systems Security

Table 1: Identified areas and their Relation Ship.

For each area pattern and relationship associated among the variables is depicted in Figure 1. For information systems security to be implemented in banks framework is used to interface with the sections across the bank. The three sections of he model briefly described as follows:

Policy Section: The policy section takes in to account Clear Desk Policy, Device Use Policy, Supervision, Password Behavior, Personal Devices, Confidential Info and Lock Screen, Help Desk, Website Access, and Physical Security of information security. This section ensures that information systems security is enabled through making employees understand the components of information systems policy issues.

Culture Section: The security culture is explained, for example, by password sharing. This is the application of information systems security policy.

Awareness Section: information systems security policy is affected by the employees' awareness, which is attitude and knowledge, of information systems security policy.

This model which is divided in to sections begins at policy section and is abstracted across the bank to be followed in the bank's day to day operations. The central goal of the model is to secure information and data through increasing employees' awareness and improving information security culture.

4. Research Design and Methodology

The nature of this research problem required an exploratory approach which allowed improving the current understanding of how employees' information systems security behaviour in banks affected the existing information systems security implementation. The advantage of qualitative research method is its ability to examine a given phenomena in relation to multiple human perspectives. The free nature of the qualitative research allows more rich

input that may contribute to a more specific outcome Pickard (2007). Pickard (2007) also states that qualitative research method is more appropriate for a human oriented study and allows freedom of choice for both questions and answers, and this in turn offers a great input to the study. The research problem is studied using qualitative data analysis methodology. One of the strengths of the case studies is that they involve a full variety of evidence such as documents, artifacts, interviews, and observations (Yin, 2003). For this research, qualitative data is gathered as extensive data was necessary for case study research (Leedy and Ormrod, 2015).

Yin (2011) explained that in qualitative research, samples are selected deliberately which is known as purposive sampling. In this study, purposive sampling was used to select the sample. Purposive sampling is used by this thesis, since Neuman (2014) highly recommends purposive sampling for qualitative case researches to identify key participants. The samples were selected based on eligibility criteria that the respondents should have experience and expertise in information systems security and the banking activities. The sample consists of information systems security manager, branch manager, information systems auditor, audit division manager, information systems support officer and banking system users. Within the study, the data collection method is selected after a review of previous studies. Different data collection techniques including structured interviews is used to assure appropriate, rich and accurate information for the study. This research has used general analytic strategy and pattern matching technique that is recommended by Yin (2011), as the most desirable technique that compares the empirically based pattern with predicted one. The thematic analysis process followed for data analysis presented in discussion and analysis is based on Braun and Clarke (2006), which consist of a set of six steps.

5. Findings and Discussion

Human factors have huge impact in information systems security. This study investigated the impact of employees' behaviour with regard to information systems insecure behaviour. In conclusion, this research findings prove that users engaged into risky actions that could make the bank system subject to attack. Employees' behaviour has been shown in relation to technology interaction, perception and information systems security training. The answer to employees' behaviour on human factor in information systems security can be improved by supplying information security training. Information systems security oriented training can address human factor problem in banks by increasing theoretical and practical knowledge of the users. So long as the information system has the human element as a fundamental component, information systems security process should include the users. Since information systems security consists of both technology and the people, employees would still are subject to error and, hence, potential point of an intrusion.

The analyzed interview revealed the culture, awareness and understanding among employees and the need to protect banks information. However, they appeared to ignore the information systems security policy and procedures to act to achieve the information systems security. The findings suggest that the reason for the insecure information systems behaviour was the ineffectiveness of the banks information systems security training. The researchers have observed that banks under the case study are aware that information technology is responsible for ensuring the core business functions as well as providing uninterrupted services. Information technology may not perform as expected because of different technical problems such as information systems security breach which results in failure of the bank core function that extends to customer dissatisfaction.

Banks, these days, have become increasingly dependent on the use of information technology to carry out their day to day activities. In this context, they envisaged that success in achieving their mission and the goals stipulated in their strategy depends on well designed and managed information technology. For this purpose, the banks have developed information security policy to guide their information security operations. Based on their policy, the banks have customized and developed their information technology policies and procedures which contain information security policy and procedures. The information systems security policies and procedures of the banks, as observed from their documents, sets out the principles and standards, which determine acceptable and secure use of the information technology. The banks information systems policies are mostly intended to implementation of information systems security to ensure the proper use of the banks' information technology facilities, applications and systems by their

employees and guests in an appropriate, responsible and ethical manner. Their policy were also applied to the use of privately owned computers, notebooks and smart phones that were connected to the bank network.

With regard to training, the banks under investigation have included in their policy that IT department is responsible to develop and provide training to business users with the skills they need to correctly use business applications, computer equipment, portable storage media, networking technologies and mobile devices in a secure way. The banks procedure also states that failure to comply with the policies and procedures of the information systems security of the banks may result in an employee to face administrative action ranging from counseling to removal from the bank as well as any criminal penalties or financial liabilities depending on the severity of of the misuse. But, practically there was no time for the banks under investigation this had occurred. However, the findings of the study suggested two concepts of information systems security in banks. These are: firstly, the current culture of the employees in banks does not promote information systems security. Secondly, the awareness of the employees towards information systems security is poor due to lack or adequate information systems training and skill. From the findings of the study there is a relationship among the first concept, the second concept and information systems security. Accordingly, information systems security involves training employees and enhancing their knowledge and skill and promote a culture that help secure information systems security. This in turn help achieve the business goals and objectives.

6. Conclusion and Way Forward

The main reason of writing the literature review is to present theoretical basis as an input for the research. This chapter consists of two main parts. The first part is a theoretical literature and the second part is literature about related work. It is assumed that 50 - 70 % of overall information systems security incidents in organizations result from the employees' misuse that is ranging from naïve mistakes to an intentional harm (Siponen & Vance 2010). Therefore, improving the information systems security needs both investments in the technical, social and organizational resources (Bulgurcu et al. 2010). Therefore, recent studies need to be shifted the focus to organizational, environmental, and individual factors that influence employees' behavior, as they are regarded as the weakest link in information systems security (Siponen 2010, Bulgurcu et al. 2010). The prior researchers have found that increasing employees' information systems awareness has a strong positive effect on their information systems policy compliant behavior (Bulgurcu et al. 2010).

This research is, therefore, designed to investigate the literature relating mainly to policy, culture and training to information systems security. There is a need to address issues relating to policy, culture and training in order to design information systems security model for commercial banks in Ethiopia. The reviewed literature includes some very recent studies conducted in 2019 and some studies conducted in not more than ten years. From the literature, it is found that the relationship between policy, culture and awareness to information systems security has been examined and investigated by different scholars in different contexts. Furthermore, this relationship is articulated in a model created by the researchers (Figure 1).

The research contributes to the current knowledge of information security by demonstrating the importance and critical role of human factors in the development of an information systems security model. The main contribution would be the advancement of the theoretical and practical basis for information systems security in proposing a model framework for developing, assessing and modeling a human factor model. Furthermore, it improves the understanding of risks in the security incident stages in relation to human factors. The research examines the role of human factors in information systems security processes. The findings emphasize the importance of human factors in today's information security context and provide guidance on addressing the risk to and return on security investments. This could perhaps serve to improve the commercial banks performance, competitiveness and effectiveness of their security policies and guidelines.

This research can also benefit the government and National Bank of Ethiopia in their effort and mission to make policy for commercial banks since they are policy makers and regulatory agents to maintain healthy economy. Furthermore, managers or decision makers in banks can be benefited from the outcome of this research by understanding the employees' behaviour that can affect information systems security to improve data security. Also practitioners can use the knowledge developed in this research for training and education.

7. References

Abiy W., et. al., (2019). Factors Hindering Full Fledged Information Security in Banking Sector in Ethiopia: Emphasis on Information Security Culture. Twenty-fifth Americas Conference on Information Systems, Cancun.

Aldawood H., & Skinner G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs - Pitfalls and Ongoing Issues, Future Internet, Newcastle, Australia.

Alhogail A., et al., (2015). Comprehensive Human Factor Framework for Information Security in Organizations, Journal of Theoretical and Applied Information Technology, Vol.78. No.2, King Saud University, Riyadh, Saudi Arabia.

Aytes, K., & Conolly, T., (2003). "A Research Model for Investigating Human Behavior Related to Computer Security", AMCIS Proceedings, Paper 260.

Calvin N., (2019). "Establishing Human Factors Programs to Mitigate Blind Spots in Cybersecurity". MWAIS 2019 Proceedings. 22.

Dahlström N. and Dekker S, (2008). Security and Safety Synergy: Advancing Security with Human Factors Knowledge, John Wiley & Sons, Inc, Sweden.

Gratian M, et. al., (2018). Correlating Human Traits and Cyber Security Behavior Intentions, ELSEVIER, USA, V 73

Hadlington L., (2018). Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom, De Montfort University, United Kingdom, International Journal of Cyber Criminology Vol 12 Issue 1.

Hadlington L., (2018). The Human Factor" in Cybersecurity: Exploring the Accidental Insider, IGI Global, UK

Halderman, J.,et al., (2009). Lest We Remember: Cold Boot Attacks on Encryption Keys. Communications of the ACM Vol 52 Issue 5.

Leedy D. and Jeanne E., (2015). Planning and Design, 11th ed. University of Northern Colorado, Pearson Education Limited .

Metalidoua E, et.al., (2014). The Human Factor of Information Security: Unintentional Damage Perspective, Procedia-Social and Behavioral Sciences, 147, ELSEVIER, Athens, GREECE

Milkyas B, et al., (2019). Building an Information Security Awareness Program for a Bank: Case from Ethiopia, Conference Paper, Research Gate, July 2019 https://www.researchgate.net/publication/336133212

Naidoo, R., 2020. A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, pp.1-16.

Neuman, W. L. (2014). Social Research Methods: Qualitative and Quantitative Approaches. (7th ed.). Pearson Education, UK.

Ngoqo, B., & Flowerday, V. (2015). Exploring the Relationship between Student Mobile Information Security Awareness and Behavioural Intent. Information & Computer Security 23(4), 406-420.

Nobles, C, (2019). Establishing Human Factors Programs to Mitigate Blind Spots in Cybersecurity. MWAIS 2019 Proceedings. 22.

Parsons, K., et. al., (2014). Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, Vol 42, pp. 165–176.

Parsons K., (2010). Human Factors and Information Security: Individual, Culture and Security Environment, Command, Control, Communications and Intelligence Division Defense Science and Technology Organization, Edinburgh South Australia, Australia

Pham, H-C. et al., (2017). Review of Behavioural Theories in Security Compliance and Research Challenges. Proceedings of the Informing Science and Information Technology Education Conference, Vietnam, pp. 65-76.

Pickard A, J. (2007), Research Methods in Information. Facet Publishing, UK.

Pollock T., (2017). Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS), KSU Proceedings on Cybersecurity Education, Research and Practice, Kennesaw State University

Singh, N, et al., (2014). Identifying Factors of Organizational Information Security Management. Journal of Enterprise Information Management, Vol 27(5) pp. 644-667.

Siponen, M. T., et. al., (2014). Employees' Adherence to Information Security Policies: An Exploratory Field Study. Information &Management, 51(2), 217-224.

Soltanmohammadi S., et. al., (2013). Main Human Factors Affecting Information System Security, Interdisciplinary Journal of Contemporary Research in Business, Institute of Interdisciplinary Business Research, Vol 5, No 7

Tolah A. et. al., (2017), A Comprehensive Framework for Cultivating and Assessing Information Security Culture. Proceedings of the 11th International Symposium on Human Aspects of Information Security and Assurance.

Yin R., (2011). Qualitative Research from Start to Finish, A Division of Guilford Publications, Inc., New York, USA.

Yin, R. K. (2014). Case Study Research Design and Methods, 5th edition, SAGE. Los Angeles. pp. 282 - 285.

Biographies

Girma Abebe is a lecturer of Accounting and Finance at Rift Valley University, Ethiopia. He received his Master of Science Degree in Information Sciences and Systems (specializing in Information Systems) in 2020, Master of Science Degree in Accounting and Finance in 2016, B.Sc. Degree in Information Systems in 2011 both from Addis Ababa University, Ethiopia. He has also received BA Degree in Accounting from Ethiopian Civil Service College in 2000 and B.Sc. Degree in Public Health from Medco Bio Medical College in 2012. Over the years, he has taught numerous undergraduate courses. He is also working as Senior Information Technology Auditor at Debeb Global Bank, a private Bank in Ethiopia. His research interest is in the area of Information Security.

Lemma Lessa is an assistant professor of Information Systems at School of Information Science, Addis Ababa University (AAU), Ethiopia. He received his doctorate in Information Technology (specializing in Information Systems) in 2016, Master of Science degree in Information Science in 2003, and BSc degree in Library Science (Computer Science minor) in 1995 from AAU, Ethiopia. Dr. Lemma has completed research projects in ICT for Sustainable Development and Application of Blockchain Technology for e-Government services. His teaching interest is on the social and management aspects of Information Systems. His postgraduate teaching includes Information Systems Security Management, Information Systems Strategy & Management, Enterprise Systems, Information Systems Project Management among others. His research interest is on behavioral, socio-cultural, and organizational aspects of Information Systems in general and the adoption and evaluation of e-Government in particular. He is member of Association for Information Systems (AIS) and current president for the Ethiopian chapter of AIS. He is serving as editor and reviewer for African Journal of Information Systems, reviewer for reputable conferences such as the International Conference on eDemocracy & e-Government, International Conference on Digital Transformations and Global Society, Hawaii International Conference on System Sciences, and International Conference on Electronic Governance and Open Society.