ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

A FRAMEWORK FOR HUMAN FACTORS INFLUENCE ON INFORMATION SYSTEMS SECURITY AT COMMERCIAL BANKS IN ETHIOPIA

By: GIRMA ABEBE

JUNE, 2020

ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

A FRAMEWORK FOR HUMAN FACTORS INFLUENCE ON INFORMATION SYSTEMS SECURITY AT COMMERCIAL BANKS IN ETHIOPIA

A Thesis Submitted to Addis Ababa University in Partial Fulfillment of the Requirement of the Degree of Master of Science in Information Science (Information Systems Specialization)

By: **GIRMA ABEBE**

Advisor: **LEMMA LESSA (Ph.D.)**

JUNE, 2020

ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

A FRAMEWORK FOR HUMAN FACTORS INFLUENCE ON INFORMATION SYSTEMS SECURITY AT COMMERCIAL BANKS IN ETHIOPIA

A Thesis Submitted to Addis Ababa University in Partial Fulfillment of the Requirement of the Degree of Master of Science in Information Science (Information Systems Specialization)

By: **GIRMA ABEBE**

Name and Signature of Members of the Examining Board

Lemma Lessa (Ph.D)	_____	_____
Advisor	Signature	Date
Dereje Teferi (Ph.D)	_____	_____
Examiner	Signature	Date
Temtim Assefa (Ph.D)	_____	_____
Examiner	Signature	Date

Declaration

This thesis has not previously been accepted for any degree and is not being concurrently submitted in candidature for any degree in any university. I declare that the thesis entitled "A FRAMEWORK FOR HUMAN FACTORS INFLUENCE ON INFORMATION SYSTEMS SECURITY AT COMMERCIAL BANKS IN ETHIOPIA" 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.

Signature: _____

GIRMA ABEBE

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

Advisor's Signature: _____

LEMMA LESSA (PhD)

ACKNOWLEDGEMENTS

I am thrilled to express my appreciation to my advisor Dr. Lemma Lessa for his incredible advise without which this thesis could not have been completed.

I will also extend my appreciation and thanks to my brother Dr. Dawit Bullo (MD) and my son Abeselom Girma, second year Architecture student at Kotebe Metropolitan University, for their help to be successful in my life, and especially my son for his help to transcribe the interview.

Girma Abebe
June, 2020
Addis Ababa, Ethiopia

ABSTRACT

The importance of protecting information in banks and mitigating security breach is becoming more important than ever. Human factors represent essential issue in information systems security in organizations, since human factors determine the behavior of employees toward information systems security. This thesis researched 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. A case study research design was used, since case study research design helps to understand a situation in great depth. Purposive sampling was used by this thesis, since it is recommended for qualitative case researches. 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 front users. For this research both structured and unstructured interviews were used. For data analysis thematic analysis and pattern matching techniques were used. The findings were used to create comprehensive model which can assist in information systems security to secure information. The study investigated the impact of employees behaviour with regard to information systems security. The 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. 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 problems in banks by increasing theoretical and practical knowledge of the users. Since information systems has the human element as a fundamental component, information systems security process should include the users.

Key Words: Information Systems Security, Human Behavior, Information Policy, Organizational Culture, Training.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

BYOD	Bring Your Own Device
HRM	Human Resource Management
IS	Information Systems
IT	Information Technology
UK	United Kingdom
TPB	Theory of Planned Behaviour

CHAPTER ONE
INTRODUCTION

1.1. RESEARCH BACKGROUND

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). 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. It is hoped that the framework will be used by information security professionals in organizations toward better human related information security management (Alhogail et al. 2015).

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 (Pollock, 2017). 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 (Pollock, 2017).

Pollock (2017) revealed that information systems security violations and errors, however, are not only limited to users. Systems administrators are also at some fault. If there is no adequate level of information systems awareness, many of the information systems security techniques are likely to be misinterpreted or misused by the users that are rendering adequate information systems security mechanisms.

With technical protection constantly improving, attackers increasingly target vulnerabilities created by the human element in an organizational security implementation. Examining a number of attacks, IBM's Computer Security Incident Response team identified human error as a contributing factor to the occurrence of over 95% of identified security incidents (IBM, 2014). This highlights the inability of current information security approaches to correctly manage the human element of security implementations, also suggesting the need to radically rethink current information security management practices to better reflect challenges employees face in their work environment.

According to Kraemer & Carayon (2006) human factor refers to the environmental, organizational, job factors and human and individual characteristics that influence human behaviour. However, it is widely defined as referring to the science of ergonomic design. Human factors is the scientific field interested with the understanding of interactions amongst individuals and other elements of a system, and the declaration that applies theory, principles and methods to design in order to optimize human well being and performance and general system functions (Kraemer & Carayon, 2006).

1.2. RESEARCH MOTIVATION

There were two types of justifications that can justify the conducting of this research study. The justifications can be summarized as contextual justification and personal motivation as follows:

CONTEXTUAL JUSTIFICATION: According to Parsons et al. (2010), 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 .

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, 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.

PERSONAL MOTIVATION: This motivation relates to the educational and professional background of the researcher who has worked as an information technology auditor in an Internal Audit Department of a bank which has made me very much aware of the possible challenges of information systems security to banks in Ethiopia. In addition, being an information technology auditor allowed me to gain a knowledge in information systems security

which involves not only machines and technology but also the human behaviour within the industry. My interest has been focused more towards the human factors aspects because, as literature has reviewed,and from my practical experience, I found that an information systems security requires a human factors behaviour change in the industry in a day by day activities. Human behavioral factors are key factors that ensure information systems security. Therefore, these personal concerns helped me in the selection of this research area. Thus, in order to summarize what have been presented so far, the main factor of this study was that human factors behaviour in information systems security in banks in Ethiopia. As the literature was reviewed, the relationship between human factors behaviour and information systems security was identified. Such a relationship has not been investigated before in the Ethiopian banks context, hence, it appears vital to examine the relationship between human factors behaviour and information systems security to improve the practice of the existing information systems security.

1.3. STATEMENT OF THE PROBLEM

Gratian (2018) suggests that even though their study was tailored to a university population, it can be replicated for practical use in other environments, there may be different individual traits and security behaviors that are of interest i.e., researchers and security practitioners at other institutions will use the study as motivation to evaluate populations for correlations between individual differences and security behaviors in order to continue developing the security community's understanding of users. Gratian (2018), 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.

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, 2018) 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 will 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.

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.

Finally, the thesis will research 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.

1.4. RESEARCH QUESTIONS

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?

1.5. RESEARCH OBJECTIVE

1.5.1. GENERAL OBJECTIVE

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.

1.5.2. SPECIFIC OBJECTIVES

The specific objectives of the study are:

i. Identify the factors that influence the security behavior of employees

ii. Identify the perception of employees security countermeasures addressing internal threat

iii. Identify countermeasures to address internal threats and to acquire a deeper understanding of how employees perceive those countermeasures and how employees change their security behavior.

iv. Identify how the knowledge about employee perception and security behavior changes can help to identify whether there are countermeasures that influence the internal threat level.

v. Identify human factors model to secure information systems in commercial banks in Ethiopia.

1.6. SIGNIFICANCE OF THE STUDY

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 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 academicians can use the knowledge developed in this research for training and education.

1.7. SCOPE

In this study, how human factors are an essential part of overall security and how they affect commercial bank's information assets was addressed. It focused only on overcoming data breaches, resulting from human factors of employees in information systems of banks.

1.8. ORGANIZATION OF THE THESIS

Chapter One introduces the research background, research methodology, and research questions of the study. It also includes the scope of the study, the objectives, the research methodology, and its proposed contribution to knowledge. It also presents the scope and limitations of this research.

Chapter Two presents the literature review that provides an extensive background to the studied concepts, namely Introduction i.e., Chapter Introduction, Information Systems Security, System Security Goals, System Security Threats, Information Security Countermeasures, Role of Human Factors in Information Security, Human Factors Evaluation, Human Factors Program, Human Error Models and Concepts, Information Security in Banks, and Related Works.

Chapter Three provides the methodological understanding and the choices selected and employed in this research, in addition to a detailed description of the use of the case study and

the triangulation methods (semi structured interviews and structured interviews) utilized to collect the required data in order to support the development of the program.

Chapter Four provides details on the data analysis process starting with a summary of the background of each of the studied banks and the extracted data from the questionnaire. The analysis of the data gained from the close ended and open ended questions are presented. Furthermore, the interviews' findings are presented including the themes and the sub themes. These are discussed alongside supporting quotes from the interviewees who are working in the selected case banks. Furthermore, this chapter compares and discusses the findings summarized with the current literature.

Chapter Five presents the main conclusion and recommendations of this research, and also suggestions for further study are given.

CHAPTER TWO
LITERATURE REVIEW

Literature review provides an overview and analysis of the current state of research on a topic (Harvey, 2010). The objective of literature review is evaluating and comparing previous research on a topic and provides in depth information about what is known to reveal controversies, weaknesses, and gaps in current work, or synthesize the existing literature to a mature level, or facilitates the theory development work (Harvey, 2010).

2.1. INFORMATION SYSTEMS SECURITY

ISO/IEC 27000 (2016) defines information systems security as the preservation of integrity confidentiality and availability of information. Integrity, availability, and confidentiality (Known as 'CIA Triad') are depicted as three aspects of information that should be protected to achieve security goals. It can be explained that only authorized persons should gain access (availability) to the accurately represented information (integrity) without disclosure to unauthorized persons (confidentiality).

It is believed that human errors are likely to cause serious security breaches, rather than technical vulnerabilities (Parsons et al. 2014).

According to Solms (2010) securing information in an organization does not necessarily generate any income and is thus often neglected. Guo (2013) explains that security related behaviour in organizations can be broken down into the following areas; "...computer abuses or security contravention, emissive security behaviour, unethical use, information systems misuse, non-malicious security violation, violation of policy, information security policy abuse and information systems security policy compliance."

There are numerous threats which threaten an organization's information security. These threats can either be, accidental, caused unintentionally by an employee, or deliberate, which is an intentional breach of security by an employee (Guo 2013). According to Cheng et al. (2013) people play a vital role in information security governance. They could be the weakest link and therefore, the use of behavioural information security as a mechanism to combat this, is

increasing. Much of the focus on information security research is on technical issues however, a significant weakness in protecting information assets, are employees in an organization.

However, recent research has shown that information security cannot be achieved by use of technology tool alone, but can only be achieved by use of three components including people, processes, and technology (Ifinedo, 2014).

According to Siponen et al. (2014) the most significant threat to information security is the information system user, who lacks the security awareness necessary to comply with information security policies.

Pham, H-C et al. (2017) examined several behavioural theories have been employed as the underpinning framework in compliance studies, for example, (Ajzen, 1991) the Theory of Planned Behaviour (TPB), (Rogers, 1983) Protection Motivation Theory (PMT) , (Gibbs, 1975) General Deterrence Theory (GDT) , and (Becker, 1968) Rational Choice Theory (RCT) in terms of their effect on security compliance intention and behaviour.

Different theories have been used in different studies in order to determine factors that influence individuals to perform or not to perform certain security actions. This research reviews studies that have applied among the most used theories, which is Theory of Planned Behavior (TPB).

Theory of Planned Behavior which was developed by Ajzen in 1991 states that "a person's performance of a specified behavior is determined by his or her behavioral intention to perform the behavior, and behavioral intention is jointly determined by the person's attitude and subjective norm concerning the behavior in question".

TPB theorizes that individual behavior is determined by behavioral intentions. Behavioral intentions have three major determinants, which are attitude toward the behavior, the subjective norms surrounding the performance of the behavior, and perceived behavioral control. Lee, J. and Lee, Y. (2001) described these determinants as follows:

- Attitude: the degree to which the person has a favorable or unfavorable evaluation of the behavior in question.
- Perceived behavioral control: the perceived ease or difficulty of performing the behavior.

- Subjective norms: the influence of social pressure that is perceived by the individual to perform or not perform a certain behavior.

Siponen (2014) used a theoretical model that combined constructs from various theories, one of which was theory of planned behaviour. The study looked at employees' behavior toward compliance with the information system security policy. The results showed that attitude and normative beliefs had a significant effect on the intention to comply with security policy.

Foltz et al. (2008) investigated the reasons that caused individuals not to read computer usage policies. The results of this study suggested that attitude, apathy, and social trust contribute to the formation of the intention to read computer use policies, while perceived behavioral control and subjective norm do not.

Foltz et al. (2008) emphasize that perceived behavioral and subjective norms did not support the TPB theory due to the environment in which the study was carried out. If everyone is required to read (and abide by) the policies, this takes care of the individual's perceptions of their ability to perform. It also minimizes discussion among individuals and referring others to the merits of reading the policies.

The results from the reviewed studies show that attitude has a major influence on behavioral intentions, as Leonard and Cronan (2005) state: "Attitude has been found to significantly affect an individual's intention to behave ethically or unethically. Therefore, understanding the dimensions of attitude will lead to the further understanding of the influences on ethical behavior intention".

In order to find what factors influence an individual's attitude towards ethical behavior, Leonard and Cronan (2005) purposed a model to examine the formation of attitude toward the behavior. The proposed model suggests that an individual's attitude toward ethical behavior is influenced by society, by the professional, legal, and business environments and by one's belief system, personal values, personal environment, moral obligation and awareness of consequences. The results showed that these attitude influencers are not permanent. They suggested that organizations must continually assess their employees' ethics.

2.1.1. INFORMATION SECURITY POLICY

According to Hagen et al. (2013) an information systems security policy is a set of principles that an organizations' information systems security management consider critical for their employees to adhere to, and it is based on past organizational information security experience, identified information security risks, industry level good practice guidelines, national and international standards and regulatory requirements. Policies are foundations of any information security, hence, their existence is critical for the organization that information systems security practices are developed and clear understanding of objectives are important (Hagen et al. 2013). Hagen et al. (2013) explains that policies are usually materialized as documents on corporate intranets and they define the information security objectives of the organization, employees' responsibilities and the desired employees' behaviours to minimize organizational information security risk exposures.

Singh et al. (2014) identified some important factors in information systems security policy that organizations need to have. Organizations need to have a documented information systems security policy, the information systems security policy need to clearly define information systems security objectives of the organization, the information systems security policy need to clearly define responsibilities and roles of the employees, the information systems security policy need to clearly define responsibilities and roles of contractors or third party vendors, the information systems security policy need to be reviewed regularly or when the business environment changes, and the procedures to implement information systems security policy need to be clearly defined and documented. These activities indicate the importance of information systems security policy, contents of information systems security policy, and key issues.

Siponen et al. (2014) state that one of the most important threats to information systems security is from employees who did not comply with information systems security policies of their organization.

According to Siponen et al. (2014) recent studies on information security policy compliance can be separated into three categories which include; conceptual principles with no underlying theory or empirical evidence, theoretical models with no empirical evidence and empirical work

grounded in theory. Furthermore, they argue that the first two categories are merely guidelines and provide little insight or little evidence to support it.

If the users do not comply with policy, then the policy and all other security solutions lose its meaning (Siponen et al. 2014).

The willingness of an information system user to comply with security policy is impacted by both their level of information security knowledge and their intended security behavior (Ngoqo & Flowerday, 2015; Van Niekerk & Von Solms, 2013). Kaspersky and Furnell (2014) highlighted the fact cyber criminals are exploiting information system users because users of the technology lack basic security awareness.

Shay et al. (2010) showed that users often lack motivation to use strong passwords since they are not convinced about the importance of suggestions in the information systems security policy. It is proved that the users' awareness of information systems security problems is not adequate to restrain users from undesirable security practices such as sharing and reusing their passwords. Therefore, most effective approaches are important to make users behave in a secure manner in their password use and authentication domain Shay et al. (2010).

2.1.2. INFORMATION SECURITY AWARENESS

Information security awareness has been defined as having general information about the security objectives and security policies within a business (Bulgurcu et al. 2010). Researchers seem to agree security awareness is essential to improving information security behavior (Siponen et al. 2014). However, researchers have yet to agree on whether information security awareness pertains to knowing about threats, includes knowledge of protections, or extends to the behavior which results simply from gaining increased knowledge about a situation (Hansch et al. 2018).

According to Singh et al. (2014) the important factors for information systems security training for employees include the organization conducting regular information systems security training for employees, information systems security training programs given by the organization are useful for the business operation, and there would be an information systems security adviser to coordinate information systems security functions in the organization.

The important factors for information systems security awareness include employees need to be aware of information systems security policy and guidelines of their organization, the organization need to conduct programs to make its employees aware of the importance of information systems security, their roles and responsibilities for information systems security are properly communicated, employees need to be aware that information systems security incidents that would be reported to management, employees need to be well informed about the acceptable and unacceptable usage of information systems assets, and employees need be aware of the punishments or disciplinary actions for violating information systems security guidelines (Singh et al. 2014).

In addition, compliance training plays significant role in awareness improvement. Current research has proposed some sanction-based compliance solution (Siponen et al. 2014) but this theory betrayed. The purpose of security compliance is to make employee deeply understand the policy through training and education. Therefore, Siponen et al. (2014) proposed a two theories based training program and validated it. The program was practical, and effectiveness was positive. Since the employees are the users of information systems mostly, so they have the access of critical data. By educating and motivating them to follow the policy of using information systems will significantly help the organization to avoid the internal threats (Siponen et al. 2014).

To effectively increase the value of information systems security for employees, thinking about current information systems security awareness, training and education is required. An accurate understanding of organizational information systems security risks, and corresponding mitigating actions motivates employees to behave information security (Hagen et al. 2013). On the other hand, the understanding of threats accurately, make compliance less attractive (Sasse, 2010) to deliver effective employees' behavioral change.

For internal IT staff, enterprise should not rely upon "on the job training", however, an intensive and skill based training should be conducted constantly, and the training result should combine with the performance analysis (ISACA, 2016).

Given the rising level of breaches (Symantec, 2016), organizations depend upon their users as a key line of defense. It is thus more critical than ever for organizations to raise the level of

security awareness. To safeguard a company against all Information Technology (IT) threats requires adequate attention to many aspects of security. Among others, it is important to maintain a high level of employee awareness at all levels and not just among staff whose work is IT related (Kaspersky Lab, 2013).

Based on the International Standard ISO 27002 (2013) all personnel of the bank and contractors as well as the third party employees need to receive proper information system awareness training and updates in their organizational guidelines and measures the significant factor for their job purpose.

Increasing instructors/learners awareness by adopting socio cognitive and social computing approaches could raise the people's critical knowledge and prediction capacity on phishing attempts (Chaudhary et al. 2015).

According to Bulgurcu et al. (2010) employees may have been harmed directly or indirectly by any kind of information systems security incidents such as worms, or phishing attacks in private or working contexts or viruses. Information systems security awareness might be shaped by some experiences such as negative incidents raise the interest and future consciousness in how to prevent such incidents. Bulgurcu et al. (2010) accordingly explains life experiences "such as having once harmed by a virus attack or penalized for not adhering to information systems security rules and regulations" might increase the individual's information systems security awareness.

According to Kim (2014) the most important information systems security awareness topics that should be discussed during an information systems security awareness and training program are to understand:

- the need of antivirus program
- the need of updating the virus definitions
- install software patches
- use of pop-up blockers
- use of personal firewall

- the risk of downloading a program or file
- risks of peer-to-peer file sharing
- the risk of e-mail passwords
- risk of e-mail attachments
- regularly backup of important files
- risk of clicking on an e-mail link
- risk of smart phone viruses
- the need of anti virus program for smart phones
- use different passwords for different systems
- change of passwords regularly, and.
- the characteristics of the strong password.

Secure and insecure employees' information security behaviour emerge by employees' understanding of information systems security risks and awareness and appropriate mitigating actions. According to Alfawaz et al. (2010) four different employees knowledge - action states of information systems security behaviours are depicted below:

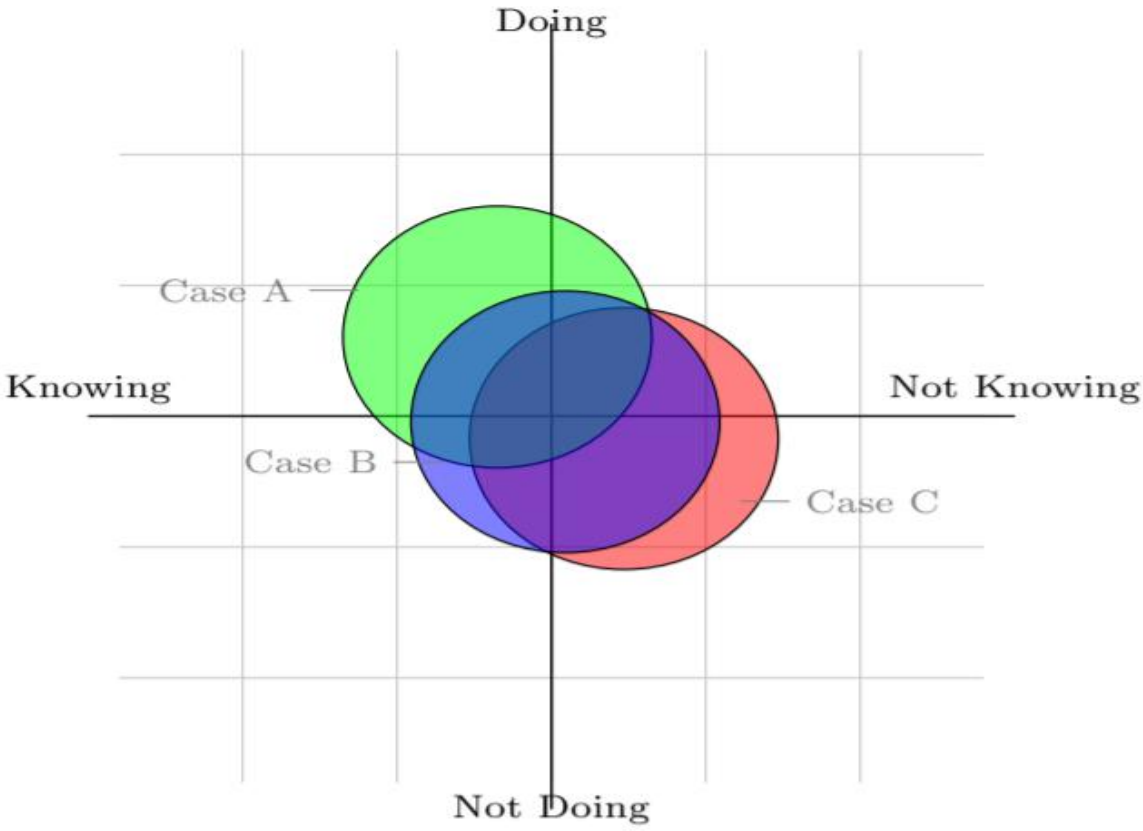

Figure 2.1 Alfawaz Information Systems Security Behaviour Model

Not Knowing – Not Doing: Employees are unaware of the information systems security policies and rules regarding their role and consequently do not comply with them.

Not Knowing - Doing: Employees are unaware of information systems security rules but are behaving in the secure way, and this usually might be due to the organizational norms and culture that influence their behaviour. For example, mimicking information systems security habit of a colleagues. Since employees are not able to make secure decisions in case they faced rare and new challenges, it is not a desired state.

Knowing - Not Doing: The employees know the rules which are defined in information systems security policy but they are not following them consciously or unconsciously in order to reduce the impact of information systems security on their abilities.

Knowing - Doing: The employees know policy rules that are defined in the information systems security policy and they are following them. This state is the desired state that comprehensive organizational information systems security program is aimed to be achieve.

2.1.3. INFORMATION SYSTEMS SECURITY CULTURE

As explained by Da Veiga and Eloff (2010) information systems security culture is defined "as a set of collective norms and values, developed through employee interaction with information security elements or by adjusting their behaviour to match that of their colleagues''. It is developed at an individual, group or higher organizational level, and it is not formalized, but it can highly affect employees' intention and behaviour to comply with information security policies. Therefore, many researchers argue that information security culture is very important to organizational information systems security as technical implementations (Knapp et al. 2009). Da Veiga and Eloff (2010) explain that the formation of organizational information security culture is based on the combination of tangible factors such as technical and procedural controls and other intangible factors such as assumptions, values, and norms of employees within the information systems security implementation. Any thing attempted to influence an employee information security culture and secure behaviour needs to target both an intangible and tangible factors that is procedural and technical controls that create friction need to be avoided, and assumptions, values and norms that lead to insecure information behaviour needs to be understood and addressed in order to deliver effective security (Knapp et al. 2009).

According to Cheng et al. (2013) employee's mind set where consequences are concerned for information security misuse, is for example, different in Korea than in the United States of America. This highlights the possibility that findings could differ from country to country, and generalizing results would not be accurate.

According to Singh et al. (2014) the important factor in an information security culture includes when the organization creates an information systems security focus among all the employees, the organization makes sure that the information systems security is the first important thing on the mind of all the employees, the organization makes information systems security the norm for all the employees, the organization dedicates its efforts to create an information systems security

focused workforce, the organization makes sure that all the employees are careful towards information systems security, and the organization has an information systems security discussions to give the management direction and support.

Various cultural aspects should be taken in to consideration when studying adverse behaviour of employees in organizational settings. Numerous national and organizational culture scholars have demonstrated the effect of cultural aspects on human behaviour. For example, Hofstede (2011) compares culture with an onion consisting of multiple layers; values are the inner layer of the onion and the core element of culture. They are invisible until they become evident in behaviour. Furthermore, Hofstede (2011) demonstrate a connection between national culture values and employees' compliance with authority and organizational policies and rules.

Veiga (2015) explains that an information security culture where training and awareness programs provided can positively influence it significantly. According to Veiga (2015) the information security culture of an organization can significantly improve the protection of information, reduce employee risk and compliance with regulatory requirements.

A weak information security culture could tighten the dilemma to security breaches. For example, when employees accept as being normal to share or divulge passwords, they believe meeting customer expectations, is paramount to rather comply to policies; they may even not use any secure means of transferring information (Veiga, 2015). These potential weak points outline potential risks that could have a negative impact on any organization as Veiga (2015) state, that information security controls has a significant impact on process, technology and information processing within an organization. Organizations should therefore, cultivate an effective culture towards protecting information in order for it to be effective. Vroom and Solms (2013) further argue that organizations can ensure that their employees adhere to prescribed rules and regulations by investigating the security compliance status of each individual.

The information systems security culture framework Tolah et al. (2017), as can be seen below, comprises eight constructs or factors that are identified and have a positive impact on the creation of the information systems security culture.

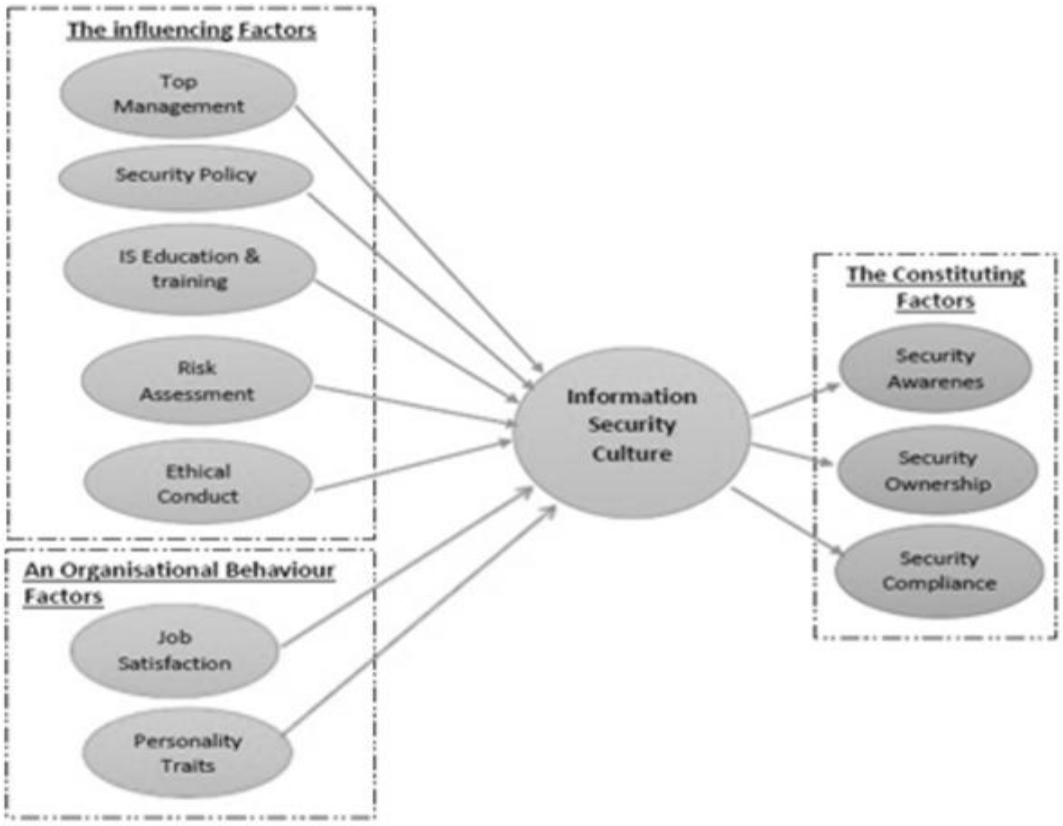

Figure 2.2 Alfawaz Information Systems Security Behaviour Model Tolah et al. (2017)

2.2. SYSTEM SECURITY GOALS

Organizations have been largely supported and accelerated by Information Systems (IS); on the other hand, protecting sensitive information, valuable assets and intellectual property in the organizations against external and internal attacks become more sophisticated and difficult than ever before (Solms & Niekerk, 2013).

Multiple surveys conducted found that many security breaches in organizations, occur due to the actions of employees within organizations; rather than that of external hackers, many of which would not have been possible without the intentional or unintentional actions of employees (Cheng et al. 2013; Crossler et al. 2016).

Information security's goals are often in conflict with the business goals of the organization (Solms & Niekerk, 2013). Organizational goals are to improve productivity and to minimize cost.

Often information security goals do not take into account the organization's goals. The two goals can even be found to be in conflict (Solms & Niekerk, 2013).

2.3. SYSTEM SECURITY THREATS

Employees who lack knowledge and skill sets are seen as a susceptible threat vector for cyber attacks, and therefore, are being targeted with continually evolving threats (Jang-Jaccard & Nepal, 2014).

Malware is the leading tool used by cyber attackers to carry out malicious acts and is known to advance rapidly to capitalize on new approaches to exploit flaws in emerging technologies (Jang-Jaccard & Nepal, 2014). Furthermore, social engineering attacks are on the rise and are considered the greatest security threat to people and organizations (Algarni et al. 2014). Even the most technologically advanced IS security measures can be thwarted by social engineering, which utilizes tactics to trick victims into compromising personal or organizational security defenses through phishing, vishing (voice solicitations), and impersonation (Algarni et al. 2014). While employee awareness of social engineering techniques is important, (Kvedar et al. 2010), found that even those who classify themselves as aware of these tactics can be fooled. Likewise, an employee with IS knowledge does not necessarily possess the cyber security skills required to protect themselves and their organization from cyber threats (Choi et al. 2013).

2.4. INFORMATION SECURTY COUNTERMEASURES

Security education, training and awareness programs take many forms, but quality programs raise employee awareness of responsibilities in relation to their organizations' information assets, provide instruction on the consequences of abuse, and develop the necessary foundational cyber security skills to help fulfill these requirements (Carlton & Levy, 2015).

According to Aytes et al. (2003) information about computer security threats, vulnerabilities, and countermeasures comes from a variety of sources. Some of these sources are relatively formal, such as training programs and organizational policies and procedures. Other sources include the news media, friends and coworkers, and personal experience. These information sources provide the "facts" that form the user's knowledge. Some of these important facts include:

- Knowledge of threats and vulnerabilities: awareness and understanding of the various threats to security, such as computer viruses, hackers, etc., along with an understanding of how vulnerable their own systems may be.
- Awareness of countermeasures: awareness that there are means of reducing risk, such as using virus protection software, not sharing passwords, etc.
- Potential consequences to self: understanding the potential negative consequences if security is violated, including loss of data, compromised privacy, etc.
- Potential consequences to others: knowledge that while there may be little or no personal consequences, friends, coworkers, and the vast number of internet users may be negatively impacted when one's system is compromised.
- Ease of recovery: although data may be lost and files corrupted, a well planned, implemented, and tested backup and recovery procedure may mean that negative consequences are only temporary (Aytes et al. 2003).

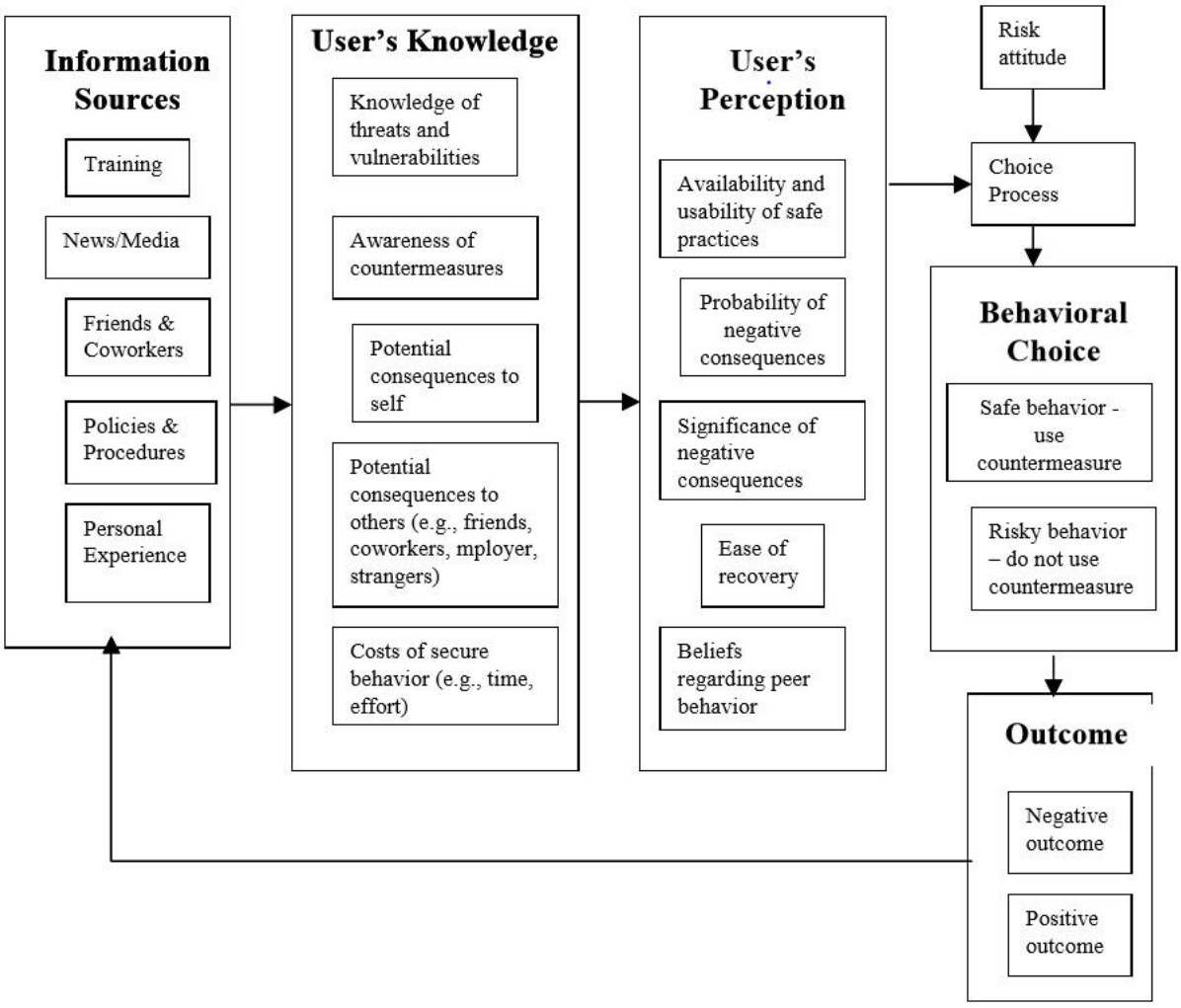

Figure 2.3 Decision Model adopted from Aytes and Conolly (2003).

The model for human behaviour related to computer security by Aytes et al. (2003) investigates different factors affecting user's perception such as tendentious media and former personal involvement and knowledge are considered to be important when it comes to the choice process in securing computer activity. The authors assume that the user's action will end up in either safe practice (certainty of no negative repercussions but with costs such as time or effort) or risky practice (no extra costs but with the probability of negative repercussions) (Aytes et al. 2004).

2.5. ROLE OF HUMAN FACTORS IN INFORMATION SECURITY

Although “no business is without risk”, human factor is always the weakest part in security reviews (Symantec, 2016). Therefore, Symantec report suggests that “every employee should be part of the effort to stay digitally healthy”. Besides, boardroom should understand what risks they face and proactively manage the situation in order to build a wall for customer data and customer loyalty before cyber criminal’s attack (Symantec, 2016).

According to (ISACA, 2016) report, although technical and administrative controls can support the prevention and detection of cyber attacks, insecure human behavior still remain weakest part in information security management. Training staffs to secure information systems and proper reaction when encountering potential threats are significant for achieving good security results.

According to Singh et al. (2014) the important factors that ensure proper top management support for information systems security are senior executives understanding of the significance of information security, senior executives attention to information systems security related meetings, involvement of senior executives in information systems security related decisions, and senior executives allocation of manpower and budget for information systems security functions.

2.6. HUMAN FACTORS EVALUATION

Aldawood H, and Geoffrey G. (2019), conducted a qualitative research on reviewing cyber security social engineering training and awareness programs. This study examines factors that may contribute to overcoming the challenges posed from implementing training and awareness programs against social engineering. This study 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.

2.7. HUMAN FACTORS PROGRAM

Knapp, K. J., & Ferrante, C. J. (2012) identified that information security policy is an essential element of an effective information security management program.

Knapp, K. J., & Ferrante, C. J. (2012) proposed a framework of information security policy that impacts the effectiveness of information security program. Each of these information security policy such as policy awareness, policy enforcement and policy maintenance have direct effect on information security program effectiveness Knapp, K. J., & Ferrante, C. J. (2012).

Tsohou et al. (2010) identified that information security training and awareness programs have a significant role in protecting the organization's assets. Information systems training and awareness enable employees comply with information security policy and procedures (Puhakainen et al. 2010). A significant proportion of security incidents are caused by employees' lack of awareness, which leads to the misuse or misinterpretation of technology or procedures which is a crucial part of information security management programs (Tsohou et al. 2010).

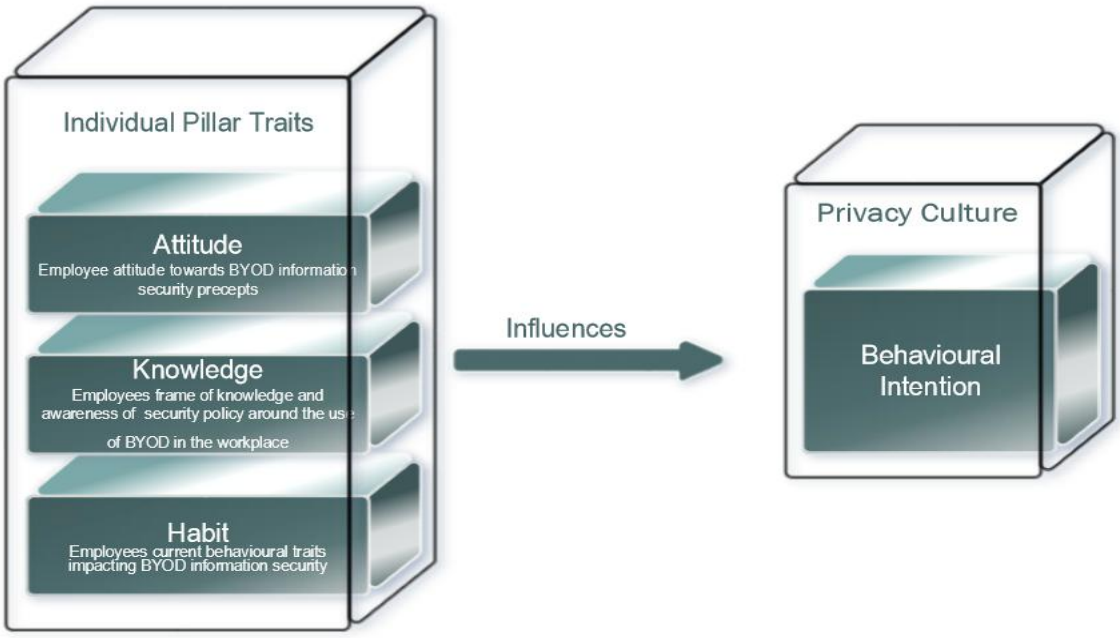

Figure 2.4 The BYOD IS Model on Individual Traits, Musarurwa & Flowerday,(2019).

According to Musarurwa et al. (2017) Figure 2.4 shows the relationship between the individual traits and the behavioural intention towards IS culture. It can be seen from the figure that the three individual traits all contribute to the IS culture formulation. The three traits of knowledge, attitude and habit have a significant bearing in the improvement of BYOD IS in banks. The figure shows that the behavioural intention of employees to improve BYOD IS rests in their

attitude towards the devices and polices, their knowledge of the security and repercussions of not observing it as well as their habits will collectively influence the culture Musarurwa et al. (2017).

Figure 2.5 adopted from Ngoqo et al. (2015) provides a graphic representation of identified associations between information security awareness, behavioural intent and actual behaviour. Behavioral intent influences actual information security behaviour.

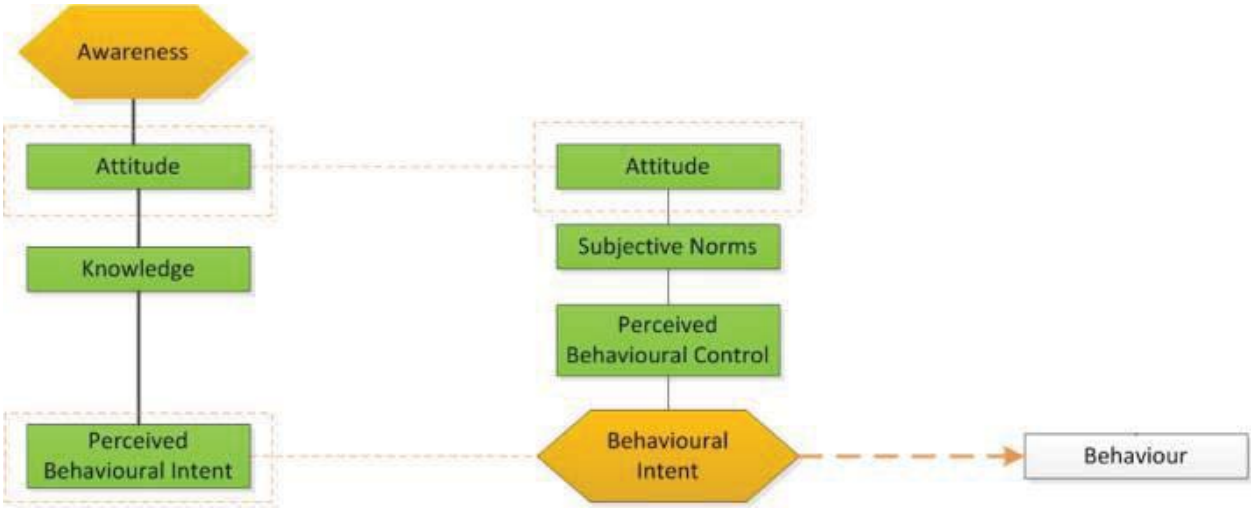

Figure 2.5 Mobile phone information security constructs adopted from Ngoqo et al. (2015).

According to Da Veiga (2015) employee behaviour would become an evident as guided by the vision, policies and strategy. Over time the organizational information systems culture emerges that encapsulates the strategy and vision and the experiences employees had at the time of implementing them. This information systems culture will incorporate the specific organizational behaviour (Hellriegel et al. 1998 cited in Da Veiga, 2015).

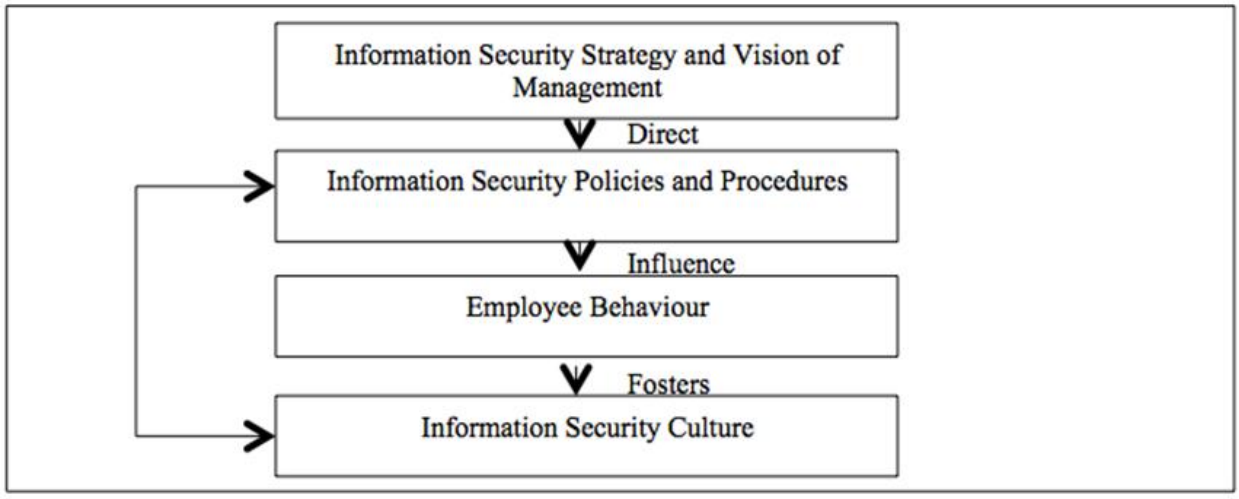

Figure 2.6. Development of an information security culture adopted from Da Veiga (2015).

Similarly, an information systems security culture develops in the organization in the same way the organizational information systems culture develops, Figure 2.6 Da Veiga (2015).

The information systems policy governs the employee behaviour. In turn, the employees will respond to the information systems policy as influenced by intrinsic and extrinsic factors. The information systems security culture that emerges can be conducive to the protection of information systems or hamper it. It is therefore crucial to assess the information security culture that has emerged and to determine whether it is in line with the initial information systems security strategy and vision of management (Da Veiga, 2015).

2.8. HUMAN ERROR MODELS AND CONCEPTS

Ifinedo (2013) proposes an integrated model, combining protection motivation theory and the theory of planned behaviour to better understand employee compliance behaviour. The findings of his research suggest that both coping appraisals and threat appraisals have a significant influence on information security policy compliance intentions.

According to Crossler et al. (2013) fear is an underlying motivating driver contained in the protection motivation theory, and these fear-relating models are becoming increasingly important to consider, being able to increase compliance in information security.

Glaspie and Karwowski (2018) conducted a research on information systems security programs and outlined the factors which contribute to the information systems security culture of the organization and developed framework from that synthesized research. Technology based safeguards alone won't achieve this goal. Humans, in the form of management, employees, and users, play a vital role in information systems security. An organization's information systems security program success depends on the appropriate user behavior. All human contributions to the effort are dependent on the factors that contribute to the information security culture. In order to have positive information systems security culture, organizations should ensure a mix of human behavioral aspects and technical systems of information systems security management (Glaspie & Karwowski, 2018).

The following model depicts the factors that affect information security. These factors are information systems security policy, attitudes and involvement, deterrence and incentives, training and awareness and management support (Figure 2.7).

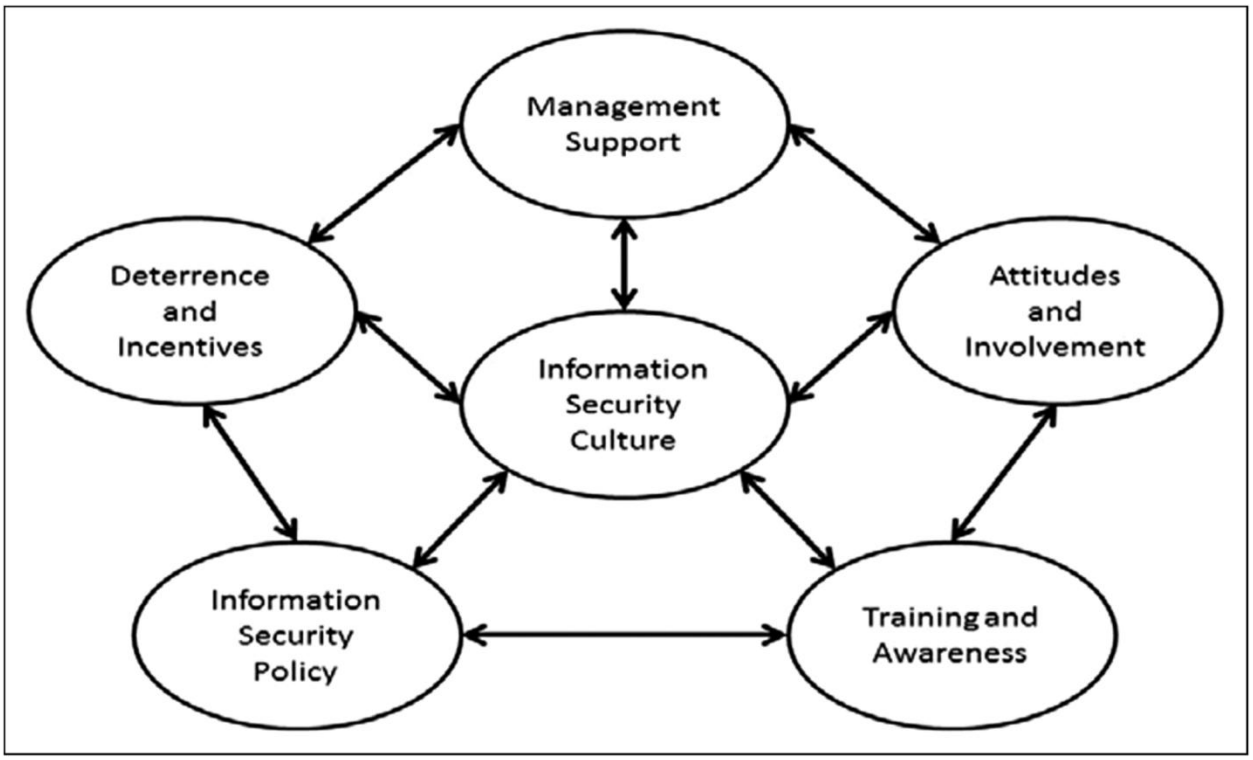

Figure 2.7 Model of the Factors that Influence and Cultivate an Information Systems Security Culture Adopted from Glaspie and Karwowski (2018).

2.9. INFORMATION SYSTEMS SECURITY IN BANKS

When business critical information is not properly protected, businesses can experience unnecessary expenses and hardships (Van Niekerk & Von Solms 2010).

Bank employees training and education in building a safe culture may influence and activate their rational manner for engaging with information security. Information security training are the highest accepted method to increase employee's information security performance and their activities (Siponen et al. 2014).

Jassal and Sehgal (2013) aimed to find various types of flaws in the security of online banking that result in loss of money for account holders and financial institutions. The research explained the reasons behind security breaches, and the participation of both customers and banks to enable hackers or crackers to access their networks. Bank clients log on to bank websites daily, through a Web-browser installed on client's personal computers, which open opportunities to cyber crimes to take place. The authors pointed to some flaws in security that could result in loss of money, along with leakage of information to unauthorized persons. Flaws could be on banking websites themselves, such as cross site scripting which happens when an attacker injects malicious scripts into a web page, and SQL injection vulnerability in which the hacker enters SQL statements into a field on a web form, in an attempt to get to the website to pass the command to the database (Jassal and Sehgal, 2013). Other Flaws could be in banking security policies, that they publish online in order to help users understand security measures that the bank follows, or could be in users' usability and customer awareness (Jassal and Sehgal, 2013).

Research tried to categorize and classify the various types of attacks against e-banking in different way. Vrincianu and Popa (2010), reported that the main threats or attacks to security of e-banking platforms are the following: denial of service, illegitimate use, disclosure of information, and repudiation. Other research presented a classification for the common attacks against online banking systems Peotta et al. (2011). Peotta et al. (2011), proposed a hierarchy of causes that includes three major categories: legitimate access, device control and credentials theft. The model (Attack Tree Model) represents the main efficient attacks and how they relate to each other and how to exploit vulnerabilities inherit in the people (social engineering and phishing attack), and gain control of device (malware), and credential theft of a legitimate user (fake web

pages and malware). Such classification is one of the simple and the most commonly used ones for the attacks performed over the online banking system.

2.10. RELATED WORKS

There exists broad empirical evidence that information security policy provision is positively associated with proper information systems security behavior (Waly et al. 2012).

Applying the theory of planned behavior, according to Anderson and Agarwal (2010), being aware of information systems security threats influence the employees' perception of the probability and severity of the threat, that are weighed against their beliefs in the efficacy of their action and ultimately influence their information systems security behavior.

Kruger et al. (2010) has aimed to test the feasibility of an information systems security vocabulary test as the assessment tool for information systems security awareness levels of specific topics. However, they also found a significant correlation of the respondents' information security awareness levels and their information security behavior.

Anderson and Agarwal (2010) explains that being aware of information systems security threats influences the employees' perception about the severity and probability of the threat, that are weighed against their beliefs in efficacy of their actions, ultimately influencing their information systems security behavior.

According to Bulgurcu et al. (2010) attitude, self efficacy and normative beliefs do positively affect employees' intention to comply with information systems security policies. Moreover, the benefits of compliance, and costs associated with both the compliance and non-compliance significantly influence the employees' attitude.

Kruger et. al. (2010) observed empirically the significant relationship between higher levels of information systems security awareness and information security behavior.

The under appreciation and under exploration of human factors in cyber security threatens the existence of every business (Nobles, 2019).

AlHogail (2015) states that neglecting the human factor could lead to security breaches as human factor determine behavior of employees toward information systems security.

According to Metalidou et al. (2014) information systems security awareness is key the to mitigate information systems security threats caused by the human weaknesses. Organizations must cultivate and maintain a culture where positive information systems security behaviors are valued. In addition, information systems security policies must be comprehensible and easy to locate. The employees' education about the importance of information systems security awareness should be a priority (Metalidou et al. 2014).

Abiy et al. (2019) studied the level of existing information security culture in the banking sector in Ethiopia. The study revealed that the information security awareness in the banking sector in Ethiopia is unsatisfactory.

2.11. CONCEPTUAL MODEL

On the basis of literature review of the research areas outlined, the researcher 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 2.8). 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 2.8) is developed in a comprehensive way to ensure an information systems security in banks. Bearing this in mind, the researcher is using critical concepts from information security culture framework (Tolah et al. 2017), Decision model from Aytes, and Conolly, (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 concept of the developed comprehensive research model is going to be discussed in detail below.

The research model of this thesis is illustrated below.

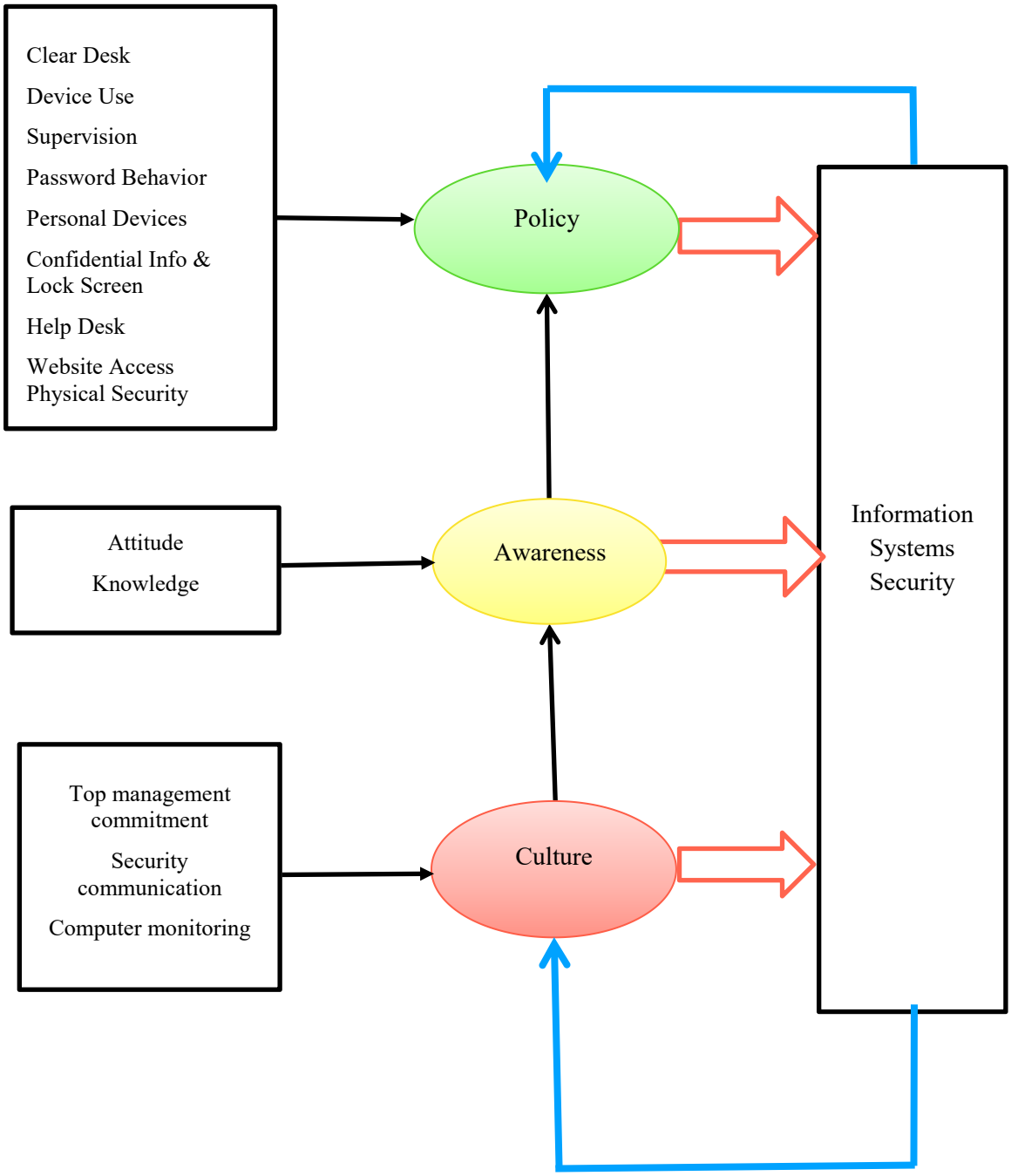

Figure 2.8 Source: Researcher's Own Model based on concepts of (Tolah et al. (2017) model, Decision model from Aytes, and Conolly (2003), the BYOD IS model on individual traits, Musarurwa & Flowerday (2019), and mobile phone information security constructs model Ngoqo et al. (2015).

The developed conceptual model (Figure 2.8), 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. Finally, achieving information systems security will be tangible. Hence, commercial banks in Ethiopia can increase information systems security to achieve their business objectives.

Moreover, on the basis of the literature review the researcher has 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 relation ship 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 2.1 Identified areas and their Relation Ship.

For each area pattern and relationship associated among the variables is depicted in Figure 2.8. 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 to secure information and data through increasing employees awareness and improving information security culture.

2.12. CHAPTER SUMMARY

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 researches 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 chapter 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 researcher (Figure 2.8) which paves the way towards the further investigation and findings presented in the fourth chapter. However, the research design and methodology to complete the study will be presented in the third chapter.

CHAPTER THREE
RESEARCH DESIGN AND METHODOLOGY

According to Melnikovas (2018) a methodology is a general research strategy which delineates the way how research should be undertaken. It includes a system of beliefs and philosophical assumptions that shape the understanding of the research questions and underpin the choice of research methods. One of the ways of research methodology construction is based on the theoretical concept of "research onion" (Melnikovas, 2018). The research onion provides a rather exhausting description of the main layers or stages which are to be accomplished in order to formulate an effective methodology (Melnikovas, 2018). This chapter outlined the research design and methodology that was used to carry out the study and meet the objectives of the research.The chapter also discussed the data collection methods, target participants, sampling techniques used, data analysis and interpretation, and validity and reliability. Finally, the chapter ends with a brief summary.

3.1. RESEARCH DESIGN

Leedy et al. (2015), describes five commonly used qualitative research designs. It gives enough information to help determine whether one of these approaches might be suitable for the research question, and briefly describe the specific nature of each methodology. Qualitative research methods are the least prescriptive. There are no magic formulas, no cookbook recipes for conducting a qualitative study. In a qualitative study, the specific methods used will ultimately be constrained only by the limits of the researcher's imagination (Leedy et al. 2015).

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. Because of this, a case study seemed to be the most suitable method to use. Yin (2009) discusses that case study focused on investigating phenomenon in real life context by revealing "Not only what, but also why and how". Case study is the subject of inquiry, which is instance of class of phenomena that provides analytical frame within the study (Yin, 2009). The purpose of case study essentially is "not hoping to prove anything but learn something", on the existing problem where there is lack of

understanding the problem that prevents use of other methods (Leedy et al. 2015). Therefore, the research design is a case study; because case study research design helps to understand a situation in great depth.

3.1.1. RESEARCH APPROACH

According to Bryman (2012) it is important for the research to be based on a theory to be completed successfully. This importance of a theory is from its influences on the research design of a project. Saunders et al. (2009) also emphasized that deductive approach starts with a theory and it needs to be predictive since the researcher starts the collection of evidences. Therefore, this research relied on the deductive approach.

The two main research methods are quantitative and qualitative research methods. The distinction between qualitative and quantitative methods is made based on the question that is asked, and the precision which one requires (Pickard, 2007). In quantitative research mathematical modelling is applied and it connects the product of study with it. The outcome is also measured in relation to the quantity. Quantitative method is used in a research where measurable could be enumerated and the mathematical relationships can be known. Quantitative research is used when it comes to investigate different realities in a various depths Pickard (2007). The advantage of using quantitative research is for a more concrete framework and when the data are easier to analyze Pickard (2007).

According to Pickard (2007) qualitative research method involves measuring data that is usually related to the human actions. 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.

3.1.2. RESEARCH STRATEGY

Bryman (2012) states that a research strategy is a way by which researchers intend to tackle research in order to answer the research questions in a social context. In this section the

researcher depicts a research approach and research technique. Bryman (2012) further stated that it is vital for a researcher to base the research on a theory in order to complete a research study successfully. The value of the theory comes from its influences on the design of a research project. All qualitative researches have two things in common, they focus on "real world" phenomena and they are used to research that phenomenon in all its complexity (Leedy & Ormrod, 2015).

The research problem was 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 was gathered and analyzed as extensive data was necessary for case study research (Leedy and Ormrod, 2015).

3.1.3. CASE SELECTION

Yin (2014) explains cases could be selected based on the purpose of the study. This study developed a model that could help commercial banks maintain secured employees information systems security behaviour. Banks in Ethiopia were chosen based on their accessibility, technology adoption by the researcher for data collection. Accordingly, five cases were identified. According to Neuman (2014) different types of samples are identified as convenience sampling, quota sampling, purposive sampling, snowball sampling, sequential sampling, deviant case sampling, and theoretical sampling. Neuman (2014) defined purposive samples as samples that are selected from the fieldwork for the purpose of special issues. Neuman (2014) also gave the researcher a control over the sample selection that is to judge the samples that can meet the specific purposes of the study. So, this study investigated the impact of employees behaviour on information systems security in banks in Ethiopia.

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.

3.1.4. STUDY PARTICIPANTS

The five banks involved in the study, Commercial Bank of Ethiopia, Debub Global Bank, Bank of Abyssinia, Nib Bank and Wegagen Bank were commercial banks operating in Ethiopia. The study participants were information security managers, branch managers, audit managers, IT auditor, help desk officers and banking system users.

3.2. RESEARCH TECHNIQUES

According to Saunders et al. (2009), research philosophy has been classified into three main perspectives, namely ontology "assumption that the researcher makes about the nature of reality", epistemology "an assumption about how researchers acquire and accept knowledge about the world" and axiology "assumptions about the nature of values the researcher adds to the study" which all belongs to the same layer which differs from approaches which can be inductive, abductive or deductive.

3.2.1. DATA COLLECTION

Kumar (2011) stated that the selected size of the sample in qualitative research is less important than in quantitative research. Also, Kumar (2011) suggests that "In interviews studies, the sample size is often justified by interviewing participants until reaching data saturation". That means, that interviews will be conducted until no new ideas emerge, in other words, when data saturation is achieved. Interviews are an essential source of data within case study methodology especially if humans are investigated (Yin, 2011). For this research both structured and unstructured interviews was used.

Within the study, the data collection method was selected after a review of previous studies. Different data collection techniques including structured interviews were used to assure appropriate, rich and accurate information for the study.

The interviews conducted had covered many aspects of information systems security in the banks examined the experience of the employees to identify weak points between information systems security and employees behaviour that lead to insecure system. The interview questions comprised of closed questions (structured interviews) and open questions (unstructured interviews).

The researcher conducted the interviews in one-to-one in all the five banks, lasting approximately 30 minutes each, to elicit rich representation of the employees' experience of information systems security.

In the interview process, the interviewer followed up the responses, when the interviewees reported a problem with an information systems security mechanism, the interviewee was asked some more additional questions, to explain further, the implications of the problems.

Sampling or the selection of the interview participants was purposive aiming to the depth context of the matter as much as possible. The participants held various positions within the bank, including information systems security division manager, information technology auditor, audit manager, branch manager, help desk officer and banking system users.

In all the banks used as a sample ten respondents were scheduled for the interview in person. The participants gave their consent to be recorded and the interview was conducted.

The interviews were recorded using recorder and copied to external drive in audio format, and the transcription to text was manually done by the researcher. It was done on word-to-word basis to make sure that all interviewee responses were accurately captured in text format.

3.2.2. DATA ANALYSIS STRATEGY

According to Bryman (2012) the sequence in the main steps in qualitative research outlined below provides a representation of how the qualitative research process can be visualized.

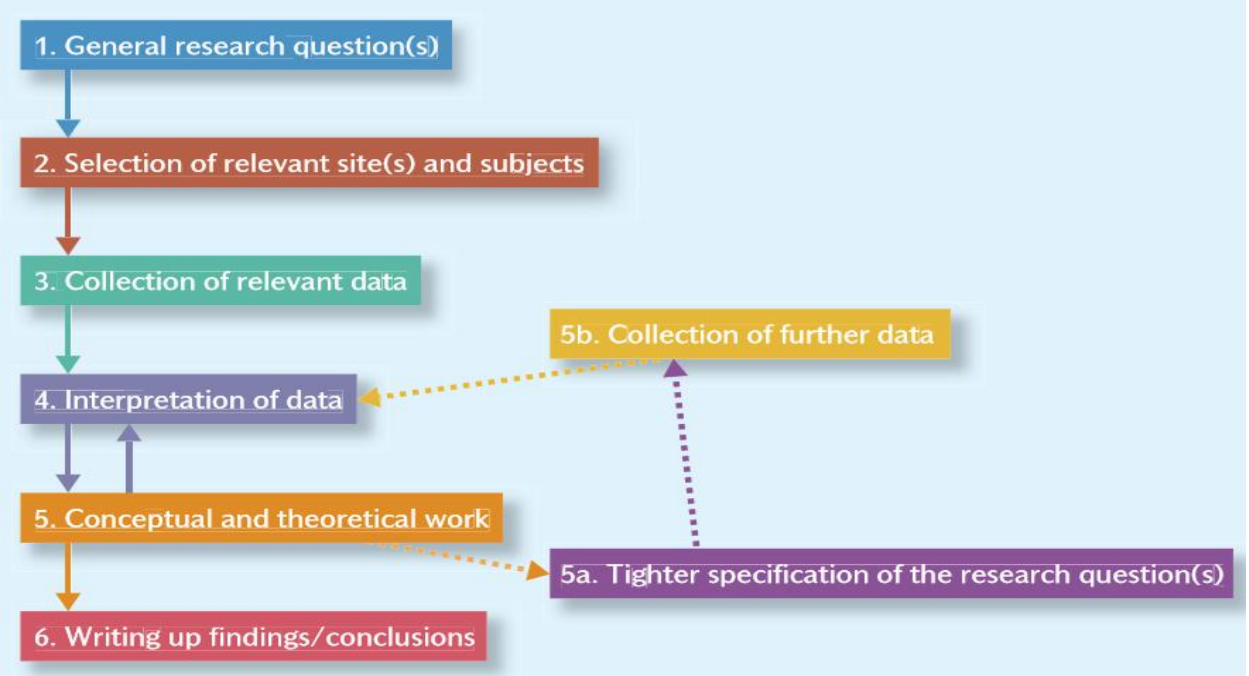

Figure 3.1: Sequence of Steps in Qualitative Research, Bryman (2012)

Leedy and Ormrod (2015) proposes data analysis based on Creswell (2014) spiral that describes how to treat raw data to get the result. The first step is to organize the collected data by filling, computerizing and breaking into smaller units. The second step is to peruse all the data to get an overall sense of data. Thirdly general categories should be identified and data must be classified. And finally, data should be integrated and summarized to be understood by readers.

This research was 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.

THEMATIC ANALYSIS

Thematic analysis is defined by Braun and Clarke (2006) as: "a method for identifying, analyzing and reporting patterns within data." It is is data driven analysis which offers flexible and accessible approach to a qualitative data analysis. Codes are assigned to text, identifying feature of a data i.e., semantic content that appears to the analyst interesting, referring to information that could be assessed in a way meaningful to the phenomenon of interest. Then codes are developed to themes, that are broader concepts, which are aiming to capture the

important properties of a data in relation to the asked research questions. Themes emerge represent responses, which are patterned or meanings within a data set, that provide interpretative analysis of data in relation to phenomena being examined (Braun and Clarke (2006).

The thematic analysis process followed for data analysis presented in discussion and analysis chapter was based on Braun and Clarke (2006), which consist of a set of six steps, for an effective thematic analysis as depicted in Figure 3.2 below:

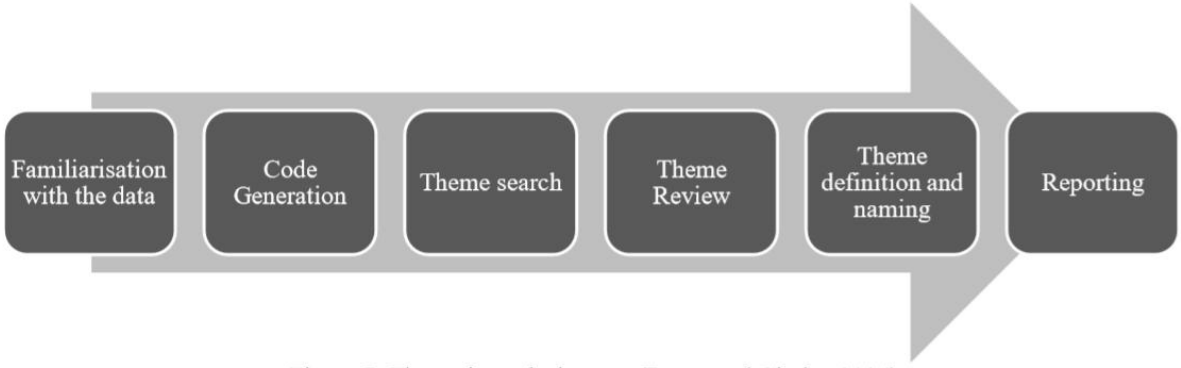

Figure 3.2: Steps of Thematic Analysis (Braun and Clarke, 2006).

The six steps can further be explained as follows:

Step 1: Familiarization with the Data

Reading and re reading the data to become familiar with what the data entails, paying due attention to the patterns that occur.This step presents preliminary start to codes and the detailed notes, and with the description of the code and the source.

Step 2: Code Generation

This step generates the initial codes, documents the codes and the patterns occur. Code generation happens through the reduction of data into labels to create categories for further efficient analysis. The data complication is completed here. Code generation involves the inferences what the codes mean. More over, the researcher also provides the detailed information how and why the codes are combined, questions are asked about the data, and finally how the codes can bring improvement to the researcher's ability in order to answer the questions.

Step 3: Searching for Themes

This step involves combining codes to overarching themes that can accurately show the data. Searching for themes is important in the development of themes that the researcher uses to describe exactly how the generated codes are interpreted and combined in order to form themes, that clearly define the themes and their meaning which is assigned to the themes, even though some theme might not seem fit the initial purpose, or contradict to each other. The researcher could also describe the missing themes from the analysis and can present a list of themes for further more analysis.

Step 4: Theme Review

In this step, the researcher sees how the themes devised support an overarching theoretical perspective and the data. If the analysis gets incomplete, the researcher would go back and investigate the available data to close any of the identified knowledge gaps. This step presents coherent recognition of the themes and how the themes are patterned to tell accurate story about the data, which is including the process how themes fit the given codes. Answers to research questions need to be well supported by the data.

Step 5: Theme Naming and Definition

The researcher has to define each theme, which data are captured, and the interesting issue about the themes, in relation to research questions. This step also provides comprehensive analysis of the contribution of the themes to the understanding of the data.

Step 6: Reporting

At the time of writing the report by researchers documenting the thematic analysis findings, the researchers must decide which themes are making meaningful contributions for the understanding of what is going on in the data. The researchers also should conduct a “member checking” for the themes by looking back to the data collected and at hand to see whether their description of phenomena is the accurate representation of what has been depicted in the data. In this step the researchers provide a description of the results by noting why the particular themes get more useful in making understanding and contributions that is going on in the data set.

Thematic analysis is chosen as for data analysis approach for this study to identify the phenomena in the banks related to the asked research questions.

The findings from the thematic analysis process applied on five of the banks, such as Commercial Bank of Ethiopia, Debub Global bank, Bank of Abyssinia, Nib Bank and Wegagen Bank. The ten interviews provided the understanding of employees' information systems security behaviours and useful insights.

3.2.3. CASE SELECTION

Personal interviews were performed with information technology persons and end users. Interviews performed with employees and would help to understand their knowledge of information security and the way they understand and perceive the implemented security countermeasures. Interviews could help to gather data about employees attitude towards information security behavior. Therefore, interviews were used for the study. Interviews were recorded in audio format using recorder and copied on an external drive for further analysis. Transcription of the recorded audio to text was done manually on a word to word basis to ensure all the employees' responses were fully captured.

Yin (2011) defined a case study as "an empirical inquiry that investigates a contemporary phenomenon in depth and within its real life context, especially when the boundaries between phenomenon and context are not clearly evident". He added that such strategy has the strength to assist researchers in investigating an elaborate phenomenon in a natural setting. Yin (2011) also identified three different types of case studies, namely exploratory, descriptive and explanatory.

In this research, the aim was to investigate the relationship between employees' behavior and information systems security through the examination of actual experience by the employees who work in commercial banks in Ethiopia. Therefore, the researcher was adopted the case study research method. In addition, in order to address the research question of this study, the qualitative case study approach was identified as the most suitable research choice to be employed.

The most appropriate design for this study was the sequential explanatory methods' design. This is associated with collecting and analyzing qualitative data in the first phase, followed by the

collection and analysis of qualitative data in the second phase, based on the results of tests for close ended questions while using thematic analysis for open ended questions.

The five banks involved in the thesis, Commercial Bank of Ethiopia, Debub Global Bank, Bank of Abyssinia, Nib Bank and Wegagen Bank were commercial banks operating in Ethiopia. These banks were selected due to the fact that they are pioneer in adopting new technologies in the banking industry. In all the banks, information security management had recognized the importance to improve the understanding of employees information security behaviour in relation to their current information security implementations. As part of this, all banks agreed to provide the researcher access to their employees, and the additional data that is required for the thesis, to identify and characterize employees behaviour, identify the potential areas of improvement, and provide guidance and knowledge to drive the improvements.

3.3. VALIDITY AND RELIABILITY

Validity, reliability and trustworthiness are quality of a research that are considered in the literature. Validity and reliability are main criteria that should be considered while examining methodological appropriateness where as trustworthiness is about how can the researcher persuade the audiences whether the findings of the study are worth paying attention. According to Punch (2005) trustworthiness comprises of four criteria such as credibility, transferability, conformability and dependability . Bryman (2012) defines validity as a set of indicators devised to gauge or measure a concept. It refers to the appropriateness and accuracy of the gathered data (Denscombe, 2010). In qualitative research, reliability and validity are affected by the perspective of the researcher, that may be biased. Therefore, Lincoln and Guba (1985) proposed criteria to assess qualitative research, namely authenticity and trustworthiness . Authenticity is related to credibility and involves the portrayal of study that reflects the experiences and meanings that are perceived and lived by the participants. Yin (2011) indicated that in qualitative research, certain criteria need be undertaken to state quality of the study. The criteria are: internal validity, construct validity, external validity, and reliability. Miles and Huberman (1994) explained that construct validity is based on appropriateness of data collection instruments. In this study, data collection method was selected after review of the related previous literature such as previous studies, journal articles, and conference reports. Interviews

were used to make sure that appropriate, accurate and rich data was collected for this study.The researcher used different sources of evidences such as the data collected from different managers, senior experts and users working in different departments and compared them.

Moreover, related literature was reviewed comprehensively to make sure that the researcher was aware of current updates in selecting the appropriate data collection technique and the analysis process. By achieving the research objective the internal validity was addressed.

Yin (2011) defined external validity as to what extent research findings could be generalized. In this study case study replication can increase external validity of the findings.

Bryman (2012) states reliability means the process where the study can be repeated yielding the same results. In this research, appropriate research model has been selected which was keen to achieve this criterion. Credibility means to what extent the research findings could be acceptable and believable.

Once the analysis of the data was completed and presented, then it was compared with the literature, and the findings were used to create the framework to enhance secured employees' information systems security behaviour in banks. To validate the he framework, interview was conducted with the participants.

Finally, analysis and findings of this study was sent to interview participants of this study. All of the participants reviewed and returned it. Therefore, the researcher has taken the review of the respondents into consideration to validate the research findings.

3.4. CHAPTER SUMMARY

This chapter presented the detailed account of the research design in terms of the research strategy, the sample selection, the research techniques and procedures. Interview data collection tool was used to achieve the research objectives. Research methods such as structured and semi structured interviews were discussed. The research strategy and rationale for choosing the case study in the research was explained. This study used qualitative data collection methods which is face-to-face semi structured interviews and structured interviews. Moreover, this chapter discussed research quality that is research validity and reliability to ensure that the study was

conducted carefully in order to obtain reliable and consistent data. Finally, conceptual model was developed and discussed .

CHAPTER FOUR
DATA PRESENTATION, ANALYSIS AND DISCUSSION

4.1. INTRODUCTION

The literature review in chapter two identified a significant information systems security gap in the existing understanding of the employees information systems security behaviour and compliance to secure the banks information. This revealed the need for investigation and design of comprehensive information systems security model for employees' behaviour and their effect on banks security risk exposure. In order to improve the existing information systems security in banks, research questions were defined in the third chapter which the researcher attempted to provide answers.

In order to improve the information systems security of the existing knowledge in commercial banks, a research question was defined in section 1.4 to which this research attempts to provide preliminary answers:

- *How human factors model be developed to address human factor gaps in information systems security?*

To answer the research question, thematic analysis was chosen as the appropriate analysis method, because it allows enriching the understanding of unknown phenomena (Braun and Clarke, 2006). This analysis was aimed to understand the context of the employees behaviour in commercial banks with regard to information systems security. The analysis was based on the approach that was defined by Braun and Clarke (2006), as it is presented in section 3.2.2, with the interview transcripts analyzed to fit them into the preexisting coding frame.

This chapter presents thematic analysis process and discusses the emerging codes and themes and explains how it contributes to information systems security. This chapter also creates a model of employees' information systems security behaviour for employees, discusses the improved model of employees' behaviour of understanding the banks information systems security management and explains how the findings of this research were used to drive information systems security.

4.2. CHALLENGES OF DATA COLLECTION

Due to corona virus (COVID-19) pandemic the employees in the sample banks were reluctant to be interviewed. In the first place since the sampling technique was purposive ten respondents two from each bank were selected based on the knowledge and experience they have for interview. Among the ten interviewees one took long annual leave after promising to be interviewed the next day. Even some employees hesitated to accept a copy of the letter written by Addis Ababa University for cooperation of data collection. It was so difficult to convince the respondents to be willing for the interview. But after so many attempts nine of the ten interviewees became willing and interviewed.

The other challenge was some of the respondents were unwilling for the interview be recorded. One interviewee rejected recording and another one gave different responses when recorded from the response he gave previously.

4.3. DATA PRESENTATION

In this section data analysis, using thematic analysis, discussion and of findings of the study is presented.

4.3.1. FAMILIARIZATION WITH THE DATA

The first phase in the thematic analysis requires identification of the start code to initiate the analysis. An initial codes were devised based on the research questions of information systems security of the nine interviewees.

The start codes emerged were covered wide range of elements of bank information systems security implementation as depicted in the following table.

START CODE	MEANING	JUSTIFICATION
Clear Desk Policy	Employee behaviour in relation to banks' clear desk policy	Banks' policy that states the desks should be cleared of all equipment and documents at the end of the day
Device Use Policy	Employees' on handling of banks' devices such as laptops, tablets, information stored on them or external devises and information security precautions taken	Policy that states how laptops are used by employees in office and remotely Policy that states not to install any application or program software unless authorized to do so for the bank's business reasons
Supervision	Responsibility of an employee for the activities of anybody else	Policy that shows the responsibility of an employee for the activities of anybody else
Password Behavior	Selection of password strategies to deal with different multiple passwords for bank systems and need to change them on regular intervals	Policy that states employees should not write their passwords down or they should not share passwords and if not they will be held accountable for the actions attributed to the conditions that led to the policy violation
Confidential Info & Lock Screen	The behaviour of employees in relation to the banks' screen lock	Policy that states how the employees behave to lock the screen of their computers in the banks' when they leave their offices
Help Desk	Supporting bank's employees for information systems security	Policy that states how to support employees information systems security
Website Access	Experience of the bank of filtering website content and of emails	Policy that states how the bank filters website content and of emails
Physical Security	The willingness of the employees to challenge strangers to protect the devises present in the office	Policy that states any body should not access any device in which he/she is not allowed
Awareness	Employees understanding of information systems security risks in the banks	Policy that states how employees understanding of information systems security risks in the banks is managed
Attitude	Employees' perception towards information systems in their bank	Policy that states how employees' need to perceive information systems in their bank
Information Sharing	Methods of sharing information	Policy that states how information should be shared in the bank

Table 4.1 Start Codes for Thematic Analysis

THEME CREATION

The following table depicts how theme is created.

THEME CATEGORY	THEME	DEFINITION
Information Systems Policy	Clear desk policy	Employees should not leave any document on their desk when they leave office
	Device use policy	Employees' should follow the banks' policy how to handle & use devices such as laptops, tablets, information stored or external devises & security precautions taken
	Supervision policy	Employees should be supervised while they are discharging their responsibilities
	Confidential information & lock screen policy	Employees should share information or data through a secure means provided by the bank & they have not to leave any document on their desk and they should lock their computers while leaving offices
	Help desk policy	Employees need to be supported by bank's security experts when they need help with regard to security
	Web site policy	Website content and of emails with potential information systems security risk should be filtered
	Physical security policy	Unauthorized person should not access any device in which he/she is not allowed
Information Systems Awareness	Awareness about information security	Employees need to have adequate understanding of information systems security risks in the banks
	Information systems security training	Training employees to boost their understanding of information systems security risks in the banks
Information Systems Culture	Information systems security concern	The employees' general perception of information systems security in their bank
	Confidential information sharing	Information should be shared in the bank through secured means that is created by the bank
	Use of storage devices such as	The practices & use of USB or any other hard disk drives by employees to store and transfer data or information
	Taking data home	Taking the banks' data using any storage device home

Table 4.2. Themes emerged from analysis

4.3.2. THEME CATEGORY CREATION AND GROUPING

The themes were grouped in to three distinct categories as themed in Table 4.2 above:

1. Information Systems Security Policy: Themes related to elements of the existing information systems security implementation policy for bank's employees in the bank to behave securely (Example of theme include: general security issues, clear desk policy, device use policy, supervision policy, password policy, personal devises policy, confidential information & lock screen policy, help desk policy, web site policy, and physical security policy).

2. Information Systems Security Awareness: Themes related to employees' information systems security awareness provided by the bank and over all the banks employees' information systems security awareness (Example of the theme includes: Knowledge about information systems security, information systems security training, reporting information systems security concerns, and vetting or checking employees or colleagues).

3. Information Systems Security Culture: Employees security culture emerging from the presence of habits, perceptions or security mechanisms (Example of the theme includes information systems security concern, confidential information sharing, use of unencrypted storage devices such as USB flash derives, taking data home, working from home, and employee security precautions).

4.3.3. THEME RELATIONSHIP

Causal relationships among the themes were identified. Cause and effect relationship between information systems security and corresponding low employees' information systems policy awareness and culture are increasing security risks. This chapter presents themes that emerge from the use and analysis of how elements of the bank information systems security was influenced by employees' behaviour. It presents also the categorization of insecure behaviours that were identified together with information systems security risks and ways to alleviate the risks.

4.3.4. RESULTS OF THE INTERVIEW ANALYSIS

This section presents the impacts of employees' information systems security behaviour with corresponding information systems security risks.

INFORMATION SYSTEMS SECURITY POLICY

CLEAR DESK POLICY

For the question raised by the researcher saying is there a policy that states what you need do with your desk when you leave in the evening the following answer was given by the information security manager. He mentioned that there is a policy regarding clear desk policy in his bank. The clear desk policy is for PC, laptop and so on so depending on the specific bank and there must be a policy to protect the assets and data of the bank. And he thinks that the employees should be abide by the policy. Employees must lock their PCs and the laptops when ever they leave their office even during the lunch time and tea breaks. But he is not quite sure that every employee that means all users are aware of it. He emphasized in having the policy by stating as:

> "[…] every e*mployee should lock his or her computer when ever he leaves office, at the lunch time or break time, even when he go to another office, so there should be a policy to protect his or her data from the desktop change".*
>
> [Information Security Manager]

The same question was responded by banking system users as follows:

> *"[…] since many of us use one computer in common we do not lock the computer when we leave office. But our passwords are different."*
>
> [Banking System Users]

For the same question raised above that was raised to an information systems auditor and the following response was obtained.When you go for lunch do you leave your laptop on the desk? Is your laptop locked physically? Is your laptop password protected?

"... as a computer science student or employee I just follow what the regulation within the bank ststes and I will take care of my assets, then I will just log of my PC not only me but I just also recommend others to do. But there are other employees who do not follow this rule."

[Information Technology Auditor]

The above same question was also forwarded for a branch manager as a user and he responded saying yes of course. But there are some other individuals who do not follow this, that means there are employees who do not lock the screen of their computers or who do not clear their desk from any file while leaving office. He also said:

"[...] in fact in our bank there is one person who is assigned to check and lock all the unlocked computers after working hours and there is no problem as such in our office."

[Banking System Users]

DEVICE USE POLICY

To understand and evaluate the employees device use policy interviewees were asked similar interview questions. The following question was for warded and responded as follows, do you ever take your laptop home? The information technology auditor confirmed that he take the lap top home by saying absolutely yes I take it home.

The information systems security manager answered the question saying under device use policy, employees who are using their laptops do could take their laptops home. The response was explained as follows:

"Personally it depends on my job sometimes if have not finished my job in the office I will take my laptop to home to finish my job but company say there are different kinds of device use policy for some companies there is a policy for the BYOD which is bring your own device policy for those companies they may allow their own device by the BYOD policy. But companies try to filter their devices when join to the network from the other

company they don't allow their personal computers to the company's network. So there should be a policy to protect each device in the system."

[Information Security Manager]

The following questions were also forwarded. When you take a laptop home do you go straight home or go somewhere else like cafe or gym? Is this a general practice for your other colleagues also?Do you have a concern that the laptop might be stolen or lost? When you take your laptop home do you afraid that your laptop might be stolen.

"For that matter its beyond stolen lap top, you may have if you may get into trouble it may not only your laptop you may lose your life by considering so as a general you may think about to not to lose your laptop but as far as I can am trying to protect my laptop when I go from the office as much as possible directly to home as much as possible."

[Information Security Manager]

Therefore, taking lap tops home is common among the employees of the banks despite the fact that there is a chance of losing the computer on the way to home.

The interviewees are asked whether confidential data are stored locally on the laptop and answered as follows:

"There should be it is not my personal laptop it is the company's laptop so I should put this for the companies things."

[Information Security Manager]

For the use of regular backups the respondent answered he does not take regular back up. Storing files or documents locally on PCs means that the potential loss of the laptop results in the loss of the data also. It enables also somebody who gets the PC to recover the document and hard drive contents, even the encrypted drives are insecure if physical access of a computer is secured by somebody (Halderman et al., 2009). More over, if the drive is not backed up, or if the data is deleted accidentally, or if the PC is lost or corrupted there is no way to recover a data that exists on it .

Other interview questions forwarded to the interviewees were do you use to store your file somewhere else? Can you install any of your own software on the laptops or is it managed by the bank? Have you ever installed any other software other than that provided by the bank? Do you take any precaution when you are doing so?

The respondents answered as:

> *"For the question can you install software on the laptop? My answer is previously we install soft wares, but currently its abide by the new policy, it is restricted we don't use USB we don't use or install any software or download anything. Now? Yeah, [...] Yes previously we have done it."*

[Information Technology Auditor]

If USB drives are lost, forgot to be wiped off, stolen or passed on to some body else who is not authorized to access the data stored on the drive, confidentiality of the data on it can be compromised. Even the deleted information can be recovered.

SUPERVISION OF OTHERSS

With regard to supervision the following questions were asked and responded as follows. Are you responsible for the activities of anybody else? Do you supervise others? Are you responsible for making them that they are aware of general information systems security policies and procedures? Are you supervised what you are doing, are employees supervised by another supervisor?

> *" No. […] Why do you think there is no supervision to employees to what they are doing what the sites they are visiting what they are downloading and so on? I don't think they are capable of doing that . […] Employees. No our supervisor is not capable of doing that. Ok, do you supervise others? No."*

[Information Technology Auditor]

The other to the above same question was as follows:

> *" Ok by this side also depends on the company so like vertical hierarchy things they have too also on their data or in their system there are a security guys. They should give what you called supervision for those smaller companies they might*

use supervision but they trying aware of how the things are smooth in working place."

[Information Security Manager]

PASSWORD BEHAVIOUR

To understand and evaluate employees password behaviour interviewees are asked the following questions and their response is captured. Are you sure that you are the only one who uses your password? Do you have password policy?

> *"Yes we do have. […] Yeah, as a bank we do have password security policy. But majority of the employees either they donot know it or they donot follow it appropriately."*

[Information Technology Auditor]

Are there peoples who wright there password on a piece of paper?

"Yeah."

[Information Technology Auditor]

Banking system users also reacted to this question saying:

> *"Password is very critical and we use it. But there are some conditions which force us to share it with colleagues especially when we are not in our office. We are humans and we encounter problem and we may be absent from office. At that time the activities can not be stopped. So, we share it."*

[Banking System Users]

Some employees write their passwords down on a piece of paper.This increases information systems security risk. To gain access to the banks systems, any attacker needs gain access electronic or physical to the document on which the passwords are stored.

PERSONAL DEVICES

Do you connect your personal devices to the bank's network? Are you using your own device your own computer or personal computer other than the banks computer? These and other similar questions were raised and the following responses are secured from the interviewees.

" Yeah, I can use but I cannot plugin bank's network."

[Information Technology Auditor]

For the question do you charge your phone by using the bank's computer, the information technology auditor responded saying:

"No that is restricted."

[Information Technology Auditor]

The same question was responded by information security division manager as follows:

"As I said personal device is depending on the policy of the companies if the personal device is allowed to some companies for those you may connect your personal things to your laptop. […] Right now the kind of mobile is some what more sophisticated and not smarter just like a laptop or a PC so you may get infected with your laptop from your mobile phone so am not advice to somebody to charge his mobile phone using the laptop.[…] Some of the employees may charge from their PC I can see that but it should not to be even if its not prohibited or from the policies side but it should be prohibited."

[Information Security Manager]

CONFIDENTIAL INFORMATION AND LOCK SCREEN

With regard to confidential information and lock screen the following questions were forwarded. Do you lock your work station when you leave your desk, even if it is just for a short period? Is there any confidential information that perhaps somebody can see on your screen that while they are walking through office? Within the office, are there people whom you don't know who could be able to see over your shoulder? Can you do anything to prevent this from happening personally?

" Actually I do have comfortable place I have a distance with others so I am comfortable to use my password comfortably no problem with that."

The information technology auditor answered.

HELP DESK POLICY

To analyze help desk policy effectiveness and its impact on banks information systems security the following questions are raised and responded as presented below. Have you ever forgot your password and had reset it? What is the process for reset it? Is it automated or you need to talk to a help desk or the IS department? Do you think they are able to see your password?

> *"There are different kinds of help risk type for the help desk for those some kind of smaller kind of help the help desk can be fix it but for those critical one like system password or critical things only the admin should change his password so the admin is may be the infrastructure admin from the operating system side or the system admin from the system side. […] I think just contact the support department. […] I have seen it will took two or three days. No, so far I haven't seen it."*

[Help Desk Officer]

WEBSITE ACCESS POLICY

To understand and to evaluate web site access policy and its impact on information systems security in banks the following questions are asked and responded by the interviewees as follows. Do you have an access to your own personal space or shared area? What else do you also have access to? Are some emails or sites blocked, for example pornographic sites or social media or if it is too big? Are there any restrictions or any rules around the emails use?

> *" Yeah, actually social media sites for example face book, you tube, instagram, twitter, and so on are restricted. […] Also they are blocked. Yeah blocked, in fact actually they are open on lunch time and before 2 o'clock."*

[Information Technology Auditor]

The same question raised above raised for other respondent and responded as follows:

> *"There are sites that are prohibited by security not to be opened by employees. There should be. But it also depends on the company and depends on the infrastructure the company has and with different devising tools you can protect or deny prohibited the different sites from the employees."*

[Help Desk Officer]

The other fundamental question to evaluate information systems policy enforcement in banks was asked and responded as follows. Have you observed some body reprimanded for his/her inappropriate email use? If someone bypass the restriction and found using the restricted site or if he violates the rule and regulations policy what is the consequence?

> *" From my entire life experience I didn't get such punishment but in the companies policies document there is a written that if somebody gets in this thing he will be punished. […] Actually there are number of listed consequences as a procedure. […] As a procedure, Yeah. But, I have not seen someone punished due to this mis behaviour. The regulations are set I think it's before a month so far no one is in-charged."*

[Information Technology Auditor]

The inability of the banks to enforce their information systems security policy and not responding to reported risks is clearly evidenced from the response of the interviewees.

The banks are filtering email system and block some websites to prevent employees from visiting high risk websites.

PHYSICAL SECURITY POLICY

In order to understand physical security policy and evaluate it the following questions are asked and the responses are captured as follows. What do you know about information systems physical security? How did you enter information systems infrastructure site? Can you see how someone could get into the building or sites without authorization? How easy it is for some one to walk in from street? Have you seen some one tailgating to the building? How often does that happen? Would you try to stop them if you noticed it to happen? Is there any other physical information security to prevent people moving between different blocks? How often it happens?

> *"Yeah, now in one room there are a lot of PCs, if somebody during lunch time or whatever access some PCs, I think it's secured by password. Yeah, physically they can access it. Physically it can happen."*

[Banking System Users]

The other respondent responded as saying:

"Its also depending on the company some of the companies may allow different kinds of different departments can share their devices to work in collaboration for the others even the same employee should not touch the other peoples PC or laptop so specially for the financial service like the IT department the others they may not allow to access their PC even to physically tries to login or tries to access somebodies laptop or somebodies PC."

[Information Security Manager]

The other respondent answered the questions: Have you bypassed any of the building's information systems physical security? If you notice some one that you did not recognize without pass card come and sit down in one of your coworker's desks would you try challenge them? The other Password issue is another issue but if they physically access it can accessible what will you say if somebody come to your office and access others PCs what will you say?

"If I see him? I will tell him. […] don't touch others PC I will tell. […] Yeah. […] Yeah, I have got someone using my mouse. And you told him not to access your PC. Yeah".

[Information Technology Auditor]

For the question that says, but what if the PC is others not yours, would you tell them? He answered saying:

"I don't think." […] Yeah, because I am a new employee they might know each other so it's not comfortable to me not to do that, I am not responsible for that."

[Information Technology Auditor]

Also, the question was extended as if somebody enter the compound some stranger to your compound data center what will you say? And he answered saying:

"I am not working in data center. […] I am stranger too to the data center. […] Yeah."

[Information Technology Auditor]

INFORMATION SYSTEMS SECURITY POLICY AWARENESS

According to Alfawaz et al. (2010) information systems security behaviour model information systems security awareness and employees behaviour presented in the literature review section 2.2.2 non compliance with policies and rules is attributed to the lack of awareness.

Question regarding the awareness of employees information systems security policy was fore warded to the interviewees and they responded as follows:

Are employees are aware of information systems security policies?

> *"I don't think they are aware of it. Others non IT employees are not aware of it. The main concern of security in my opinion is just sustaining the business in secured way. …. I think the challenge is a knowledge gap among employees, managers or IT guys in every aspect, in all cases……. Yeah, training is mandatory to tackle this problem……. Yeah to fill the gap basic IT training or security training will be mandatory…….So awareness has to be created through training in every employee……The awareness created by the training is not adequate. Not sufficient.*
>
> [Information Technology Auditor]

The other interviewee answered the same interview question saying:

> *"It is a very good question right now. It is the cyber security issue in our global world, so this cyber security issue is a very sensitive thing so it should be clearly done by different kinds of methods of the awareness as far as I know. I think it should be done in different ways the first thing is by giving the employees a training for an awareness to be more important about the information security the second one is by giving like an information tips to their by sending an email to different employees so the should be try to be aware of the third one on job like when they are using their device a laptop or PC and they get difficulties to take to use their systems so at that time the IT guys should give an awareness to any points for the employee for the system so with this three different kinds of methods the awareness should be done by each company."*
>
> [Information Security Division Manager]

Based on the response of the conducted interview, the overall bank information systems security training for security experts and users seen as dysfunctional. There is a very limited information systems security awareness among employees about the existence of information security

policies and procedures that help to mitigate bank information security risks. The employees also lack the knowledge of information security risks, and also they perceive information included in information systems security and training are not useful to them. The employees are not also aware of how to identify and protect the banks' sensitive and confidential information.

INFORMATION SECURITY CULTURE

The banks have clear policy that prohibits password sharing. But employees are sharing their passwords they needed to access the banks' systems. By the time the interviewees are asked the question that says What is your main information systems security concern? Is there any other concern that you can think of? one of the respondent answered as follows:

> *"Yeah, They (employees) share different things even they share passwords[…]. Yes of course, actually in branches they share passwords during lunch time or if they are busy they share passwords and doing their jobs."*
>
> [Information Technology Auditor]

The sharing of passwords among employees increases risks for the misuse of the system, and also leads to reduced accountability if security bridges happen, and in case the employees behaviour requires follow up. The risks also might be significant when password sharing is across many systems.

For the question that states is your work be misused by individuals who are malicious? Do you share confidential information to someone inside the bank or to someone outside the bank? Do you share information critical information with your colleague? With your colleague?

One of the respondent which is the security manager of the bank responded as follows:

> *" It depends on your colleague type." […] Yeah my colleague I am working for the company specific with the colleague with me we are trying to analyse researching or making to know about that information to be secured we may discuss about sharing that information for the other departments or the other guys we shouldn't do that."*
>
> [Information Security Division Manager]

According to a research conducted by Bartsch and Sasse (2012), sharing information through USB drives or informal channels are security inadequate and employees need to take actions that is considered mitigate security risks.

So, the following question was raised to the interviewee as:

Do you use removable storage devices such as USB? Is it your own one or is it given to you by the bank? Is it just for your own use or is it shared by the bank? How far it is important to you to use storage devices at your work place?

The respondent answered as follows:

> *"Actually using USB is restricted by the bank when you plug in, but it is not in all PCs. The new ones are restricted actually. But there are PCs that can accept USBs and peoples can restore information on that".*
>
> [Banking System Users]

The other interviewee also answered the same question stating that:

> "*There is a companies USB or external hard disk so we are putting or store the companies data on that hard disk only for the purpose of the job may be its for the purpose of backup or may be the purpose of to analyse a data in a different ways".*
>
> [Help Desk Officer]

The banks provided different means for employees to share files in a secured information sharing using group document repositories. But some employees rather use USB or external hard disk for document sharing.

In connection with this question, the same respondent i.e., information systems security manager is asked to give his opinion and responded saying the main information system concern is from the beginning is the security which is the confidentiality of the the bank information. Since what is dealt with in banks is money any breach of information in banks results in heavy loss in terms of money. The integrity of the information, the availability of the information and confidentiality of the information of the bank data must be secured. The integrity of the the information must be

kept or the data should not be changed or altered by some one from the original type of data to some other data. But, employees for different reason not in a position to keep the integrity, confidentiality and availability of the the banks data. This is mainly due to lack of awareness. And, this lack of awareness is from their lack of knowledge and skill.

4.4. DISCUSSION

The research question that is stated as:

- *How human factors model be identified to address human factor gaps in information systems security?* is revisited.

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 researcher has 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, now a 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 will 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.

4.5. CHAPTER SUMMARY

In this chapter, the interview collected from the nine interviewees regarding the employees behaviour that affects information systems security in banks were identified and discussed. The summary of the findings were as follows:

- Even though the information security policy of the banks states that when workers leave office in the evening they should clear their desk from any document and they should lock their computers there are some workers who do not do so.
- Some employees even do not know whether information systems security policy exists in the bank.
- By the time some employees take laptop home, they use any mode of transport, go somewhere else, and they do have a concern that the laptop might be stolen or lost.
- There is a trend that some employees in some cases can install any application or program software on the laptop that is provided to them by the bank.
- There is no supervision to employees to what they are doing, what sites they are visiting what they are downloading and so on.
- The banks have password security policy. But, password sharing among themselves and writing passwords on a piece paper are common among employees.
- It is common for employees to connect their own personal devices like smart phones and tablets to the bank's network and they are also using their own device like laptop other than the banks computer.
- No body is reprimanded for his/her inappropriate email use or violation of information systems security policy in the history of the banks under research.
- In some instances the banks' computers might be accessed by unauthorized personnel.
- Employees are not aware of information systems security policies due to lack of training.
- Employees share information, store information or take back ups using removable storage devices such as USB or external hard disk .The storage devises are either provided by the bank or belongs to the workers. They also share information through email.
- Employees information systems security behaviour was deviating from the banks' information systems security policies, that can create security risks for the banks. The insecure practices identified were due to lack of employees' awareness related to information systems security policy.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

This chapter presents, the conclusion and recommendations of the study. This chapter explains how the objectives of the research have been accomplished. It also addresses the implications and recommendations for further work and recommendations to enhance the employees behavior in banks in Ethiopia to secure information systems security.

5.1. SUMMARY OF KEY FINDINFS

Summary of the findings of the research was presented in chapter four. The findings were used to create comprehensive model presented in section 2.11. The study puts forward more findings which can assist in initiating further recommendations. Therefore, the aim of the conclusion section is to address the main findings of the study and to make the related recommendations. In order to fulfil the purpose of the study the researcher classified the different concepts involved in this study as information systems policy, information systems awareness, and information systems culture, and their relation ship with information systems security to secure information.

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.

5.2. CONCLUSION

The main objective of this study was to explore human factors that affect information systems security practices in commercial banks. Human factors that affect current practices of information systems security have been identified and discussed for improving information security practices.

It was found that information systems security in banks was affected by information systems security policy, culture, and level of awareness of the employees.

Currently the employees awareness and training towards information systems security policy in banks were not sufficient in light of current information systems security, thus banks were not able to secure their data and information. Moreover, no body is reprimanded for wrong doing or not following the banks information systems policy.

Banks need to learn how to secure data and information by taking advantage of employees training and creating awareness and thereby improve their information systems security practices.

This thesis has demonstrated the impact of human behaviour to information systems security. Information systems policy, awareness and culture have been discussed in particular. More research on information systems security with regard to human behavioral issues should be carried out in order to increase the understanding of information systems security and enable improved security practices.

5.3. RECOMMENDATIONS

The following recommendations were forwarded in line with the above findings:

1. The lack of information systems security policy awareness among employees identified should be alleviated through information systems security training and effectively need to be communicated.

2. The management should strengthen its follow up of policies and take corrective actions when there is violation of policies.

3. The findings of this study were used to create comprehensive model presented in section 2.11. Therefore, the aim of the study was to address the main findings of the research. In order to fulfil the purpose of the study the researcher classified the different concepts involved in this study as information systems policy, information systems awareness and information systems culture and their relation ship with information systems security to secure information. Therefore, by adopting the model developed in this study, it is possible to have secured employees behaviour which in turn can result in secured information system resources in banks.

4. Human factors have huge impact in information systems security as identified in the study. 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 banks, would therefore, recommended to focus on human factors to have secured information behaviour.

5.4. LIMITATION

The following challenges were the limitations encountered by the researcher during data collection:

- Due to corona virus (COVID-19) pandemic the respondents do not want to be interviewed.
- The unwillingness of some respondents not to be recorded or their reluctance to give genuine answer to the questions raised by the researcher.
- Some interviewees do not want to disclose the condition of information systems security of their banks.

5.5. FUTURE WORKS

This section provides some potential directions for further future study to expand scope of the study and to assess effectiveness of the current information systems security behaviour. The remarkable issue recommended by the researcher is to test this case study on other different industries other than banks. It might be interesting to explore how information systems security depends on information systems policy, culture and awareness in different industries.

The following specific topics are not addressed by this research and they are recommended for future studies by other researcher:

- what kind of training can be given to secure information systems security in banks
- what damage is experienced due to human insecure behaviour in information systems security
- what does human behaviour with regard to information systems security looks like in other industries other than banks.

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*

Alfawaz S, et al., (2010). Information Security Culture: A Behaviour Compliance Conceptual Framework. *Conferences in Research and Practice in Information Technology Series 105: 47–55.*

Algarni, A. et al., (2014). Social engineering in social networking sites: How good becomes evil. *Proceedings of the Pacific Asia Conference on Information Systems*, 1-10.

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.

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50(2), 179-211.*

Anderson, C., and Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly, Vol. 34, No. 3, pp. 613–643.*

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

Bartsch, S, and Sasse A. (2012). Guiding Decisions on Authorization Policies. *In Proceedings of the 27th Annual ACM Symposium on Applied Computing. SAC '12, 1502*. New York, USA: ACM Press.

Bryman A., (2012). Social Research Methods, 4th ed. Oxford University Press, Oxford, UK .

Carlton, M., & Levy, Y. (2015). Expert Assessment of the Top Platform Independent Cybersecurity Skills of non-IT Professionals. *Proceedings of the IEEE SoutheastCon Conference*, 1-6.

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

Chaudhary, S. et al., (2015). Time up for Phishing with Effective Anti-phishing Research Strategies. International Journal of Human Capital and IT Professionals (IJHCITP), 6(2), pp.49-64.

Choi, M. S., et al., (2013). The Role of User Computer Self-efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills Influence on Computer Misuse. *Proceedings of the Pre-International Conference of Information Systems on Information Security & Privacy*, 1-19.

Cheng, L. et al., (2013). Understanding the Violation of IS Security Policy in Organizations: An Integrated Model Based on Social Control and Deterrence Theory. Computers & Security, 39:447–459.

Creswell, J., (2014), *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches,* 4th ed. SAGE Publications Ltd.

Crossler, R., et. al., (2013). Future Directions for Behavioral Information Security Research. *Computers & Security*, 32:90–101.

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

Denscombe, M. (2010). *The Good Research Guide: For Small Scale Social Research Projects,* (4th ed.). McGraw Hill, England

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention Toward Protective Information Technologies. *Journal of the Association for Information Systems, 8*(7), 23.

Foltz C. B, Schwager, et al., (2008). Why Users Fail to Read Computer Usage Policies. *Industrial Management and Data Systems*, 108(6), 701-713.

Glaspie H. and Karwowski W. (2018). Human Factors in Information Security Culture: A Literature Review, *Department of Industrial Engineering and Management Systems, University of Central Florida,* Orlando, FL 32816-2993, USA.

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

Guo, K.H. (2013). Security Related Behavior in Using Information Systems in the Workplace: A Review and Synthesis. Computers & Security, 32(1):242–251.

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.*

Hagen J et al., (2013). Implementation & Effectiveness of Organizational Information Security Measures. *Information Management & Computer Security, Emerald* Vol 16 (4). pp 377–97.

Hansch, N., & Benenson, Z. (2014). Specifying IT Security Awareness. 25th *IEEE International Workshop on Database and Expert Systems Applications Proceedings.*

Hofstede, G. (2011). Dimenionalizing Cultures: The Hofstede Model in Context. *Online Readings in Psychology and Culture,* 2(1).

Harvey, M. (2010), What is Literature Review. pp 1-2

Ifinedo, P. (2013). Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialization, Influence, and Cognition. *Information & Management*, http://dx.doi.org/10.1016/j.im.2013.10.001.

ISACA (2016). State of Cybersecurity: Implications for 2016. An ISACA and RSA Conference Survey.

Jang-Jaccard, J., & Nepal, S. (2014). A Survey of Emerging Threats in Cybersecurity. *Journal of Computer & System Sciences, 80*(5), pp. 973-993.

Jassal, R. & Sehgal, R. (2013). Online Banking Security Flaws: A Study. *International Journal of Advanced Research in Computer Science and Software Engineering,* 3(8), 1016 – 1021.

Kaspersky, E., & Furnell, S. (2014). A Security Education Q&A. *Information Management & Computer Security, 22* (2), 130-133.

Kaspersky Lab (2013). Global Corporate IT Security Risks.

Knapp, K. J., & Ferrante, C. J. (2012). Policy Awareness, Enforcement and Maintenance Critical to Information Security Effectiveness in Organizations. *Journal of Management Policy and Practice,* 13(5), 66-80.

Kraemer, S. & Carayon, P. (2006). An Adversarial Viewpoint of Human and Organizational Factors in Computer and Information Security: Final Report. Wisconsin, Madison: *University of Wisconsin-Madison & Information Design Assurance Red Team (IDART)*, Sandia National Laboratories.

Kim, E.B. (2014). Recommendations for Information Security Awareness Training for College Students. I*nformation Management & Computer Security*, Vol 22(1), pp.115-126.

Kruger, H., et. al., (2010). A Vocabulary Test to Assess Information Security Awareness. *Information Management & Computer Security*, Vol. 18 No. 5, pp. 316–327.

Kumar R., (2011). *Research Methodology: A Step-by-Step Guide for Beginners, 3rd* ed, SAGE Publications, London.

Leonard, L. N., & Cronan, T. P. (2005). Attitude Toward Ethical Behavior in Computer Use: A Shifting Model. *Industrial Management & Data Systems*, 105(9), pp. 1150-1171.

Lee, J., & Lee, Y. (2002). A Holistic Model of Computer Abuse within Organizations. *Information Management & Network Security*, 10(2), 57-63.

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

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic Inquiry. Vol. 75. Sage.

Luo X. et al., (2011). *Social Engineering: The Neglected Human Factor for Information Security Management,* Information Resources Management Journal, 24 (3), The University of New Mexico, USA.

Melnikovas A. (2018). *Towards an Explicit Research Methodology: Adapting Research Onion Model for Futures Studies,* The General Jonas Zemaitis Military Academy of Lithuania.

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

Miles, M. B., & Huberman, M. (1994). *Qualitative Data Analysis: An Expanded Sourcebook.* (2nd ed.). Thousand Oaks, Calif. Sage.London

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

Musarurwa A., Flowerday S. (2019). Information Privacy in the BYOD, *Information Institute Conferences,* Las Vegas, NV, April 29 – May 1.

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.

Peotta, L., et. al., (2011). A Formal Classification of Interest Banking Attacks and Vulnerabilities. *International Journal of Computer Science & Information Technology (IJCSIT),* 3(1), 186 – 197.

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

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

Punch, K. F. (2005). *Introduction to Social Research: Quantitative and Qualitative Approaches.* 2nd ed.. SAGE.London.

Saunders M, et al, (2009). *Research Methods for Business Students,* 5th ed, Pearson Professional Limited, UK.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information Security Policy Compliance Model in Organizations. *Computers & Security, 56*, 70-82.

Shay, et. al., (2010). Encountering Stronger Password Requirements: User Attitudes & Behaviour, *In Proceedings of Symposium on Usable Privacy & Security, ACM*, pp. 14-34.

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

Singh A., (2016). Analysis of the Human Factor Behind Cyber Attacks, *International Research Journal of Engineering and Technology (IRJET)*, Vol 03, Delhi, India

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

Solms, V, R., & Niekerk, V, J (2013). From Information Security to Cyber Security, Computers & Security, Volume 38, pp 97-102

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

Symantec (2016). Internet Security Threat Report. Symantec Corporation. 21.

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*.

Tsohou, A., et al., (2010). Aligning Security Awareness with Information Systems Security Management. *Journal of Information System Security, 6*(1), (pp. 36–54).

Vrincianu, M. & Popa, L. (2010). Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests. 12(28), 388 – 403.

Waly, N., et. al., (2012). Measures for Improving Information Security Management in Organizations: The Impact of Training and Awareness Programs. Proceedings of the 17th UK *Academy for Information Systems Conference (UKAIS)*, UK, Oxford, Vol. 8.

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.

APPENDICES

APPENDIX A

ADDIS ABABA UNIVERSITY
COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES
SCHOOL OF INFORMATION SCIENCE

INTERVIEW QUESTIONS

Dear contributor: Firstly, I would like to say thank you for your participation in this thesis, which aims to study "**A FRAMEWORK FOR HUMAN FACTORS INFLUENCE ON INFORMATION SYSTEMS SECURITY AT COMMERCIAL BANKS IN ETHIOPIA''.** Your participation has very important significance to me and it has positive impact on the quality of this study i.e., it is very commendable and valuable.

Secondly, I would like to assure you that there is no negative future consequence of your participation in this study, no personal information is communicated or sought and you can not answer any question you do not want to answer and you can withdraw any time. You can also communicate me personally or on my email agirma747@gmail.com.

Moreover, all responses given as part of the interviews would be treated with the highest confidentiality and would be available only to the researcher and the adviser of the thesis. Excerpts from the interviews would be used for thesis publications, under no circumstances your name or any thing that is identifying characteristics of your identity be disclosed in such publications.

Thank you!

I. INFORMATION SYSTEMS SECURITY POLICY

1. GENERAL SESCURITY POLICY ISSUES

What do you think in general about information systems policies? Do you think the information systems policies are well known by employees and do they follow all policies procedures and rules all times in terms of security? If not why? Is there any policy or procedure that you routinely do not comply with? If so, why or why not? What would be done when some body does not follow the information systems security policy?

2. CLEAR DESK POLICY

Is there a policy that states what you need do with your desk when you leave in the evening?

3. DEVICE USE POLICY

What is your general view of employees device use policy such as installing software, taking laptop home, working from home, confidential data sharing, regular backups and so on.

4. SUPERVISION OF OTHERS

Are supervisors responsible for making employees aware of general information systems security policies and procedures? When some body leaves the bank, is access right revoked? Is the supervisor concerned whether employees comply with information systems security processes or not?

5. PASSWORD BEHAVIOUR

Have you ever shared your password with anybody else? Does any of your systems is using shared passwords? When a change is needed, do you change all the passwords at the same time, even though, they don't need at the same time to be changed? Without being prompted to, do you change the passwords? Is there any restriction, such as must have capital letters, numbers or characters?

6. **PERSONAL DEVISES**

Do you connect your personal devices to the bank's network? Are there any other particular properties or features that your device has to be used on the bank's network? Is it common practice among employees to bring their own devices to the bank?

7. **CONFIDENTIAL INFORMATION AND LOCK SCREEN**

Do you lock your work station when you leave your desk, even if it is just for a short period? Is there any confidential information that perhaps somebody can see on your screen that while they are walking through office? Do people in your office around you tend to lock screens when leaving desks?

8. HELP DESK POLICY

Have you ever forgot your password and had reset it? What is the process for reset it? Is it automated or you need to talk to a help desk or the IS department? Do you think they are able to see your password? What are the procedures they ask you to go through to check who you are to reset the password?

9. WEBSITE ACCESS

Are some emails or sites blocked, for example pornographic sites or social media or if it is too big? Are there any restrictions or any rules around the emails use? Have you observed some body reprimanded for his/her inappropriate email use? Are there some web pages that you cannot access?

10. PHYSICAL SECURITY POLICY

What do you know about information systems physical security? How did you enter information systems infrastructure site?

II. INFORMATION SYSTEMS SECURITY AWARENESS

How far employees know about the information systems security policies in general? Do you take any information systems security training? Has everybody in your team given that? Are you aware of something being done to keep employees aware of information systems security?

III. INFORMATION SYSTEMS SECURITY CULTURE

What is your main information systems security concern? Do you share confidential information to someone inside the bank or to someone outside the bank? Do you use removable storage devices such as USB?

Is any of the data confidential? What security precautions do you take in order to protect that data? In general what do you think about the information systems security culture in your bank?

APPENDIX B

አዲስ አበባ ዩኒቨርሲቲ
የተፈጥሮ ሳይንስ ኮሌጅ
የኢንፎርሜሽን ሳይንስ ት/ቤት

ADDIS ABABA UNIVERSITY
College of Natural Science
School of Information Science

Date:- March 18, 2020
Ref: - SIS/68/2020/12

To whom it may Concern

Dear Sir/Madam,

Student Girma Abebe (ID.No GSE/7956/10) 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 a Comprehensive Human Factors Model for Information Systems Security at Commercial Banks in Ethiopia".

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

With Regards,

Tibebe Beshah (PhD)
Head, School of Information Science

✉: 1176 ☎: +251-(11)-122-91-91