12-2019

INFORMATION SECURITY AWARENESS PROGRAMS IN CONGOLESE ORGANIZATIONS: CULTURAL INFLUENCE AND EFFECTIVE USE.

Arnold Nzailu

INFORMATION SECURITY AWARENESS PROGRAMS IN CONGOLESE ORGANIZATIONS: CULTURAL INFLUENCE AND EFFECTIVE USE.

A dissertation submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Doctor of Science

in

Information Systems

December 2019

By
Arnold Nzailu

Dissertation Committee:
Dr. Park, Insu
Dr. Meyer, Casualene
Dr. Liu, Jun

DAKOTA STATE UNIVERSITY

DISSERTATION APPROVAL FORM

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Science in Information Systems degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: Arnold Nzailu

Dissertation Title: INFORMATION SECURITY AWARNESS PROGRAMS IN CONGOLESE ORGANIZATIONS: CULTURAL INFLUENCE AND EFFECTIVE USE

Dissertation Chair: Dr. Park, Insu Insu Park Date: 9/27/2019

Committee member: Dr. Meyer, Casualene Casualene Meyer Date: 9/29/2019

Committee member: Dr. Liu, Jun Jun Liu Date: 9/30/2019

Committee member: _____ Date: _____

ACKNOWLEDGMENT

I would like to express my deepest gratitude to my dissertation chair, Dr. Insu Park, for his immeasurable support, patience, insights, and encouragement throughout my study.

My sincere appreciation is extended to Dr. Meyer Casualene for helping me proofreading my work and guiding me through the journey of becoming a better academic writer.

It would have been impossible to complete my dissertation without the support of family and friends. I am especially grateful to my parents, Marceline and Benjamin Nzailu, my brother and sister, Herbert, and Marline Nzailu for their moral support and their belief in my ability to complete this journey.

ABSTRACT

Motivated by a need to understand the underlying drivers of employee effective use behaviors as it relates to security awareness in Congolese organizations, this study examined extrinsic motivation, intrinsic motivation, attitude toward security, intention to comply with security, and cultural motivators as critical elements that have an influence on employee effective use of security awareness.

To our knowledge, this study is the first to develop a model to investigate the influence of employees' culture on the effective use of security awareness programs. This study contributes to behavioral aspects of the body of knowledge on information security by presenting empirical support that employees' culture, intrinsic motivation, extrinsic motivation, information quality, and attitude toward security awareness programs are essential factors to consider in order to predict employees' decisions on the effective use of security awareness program.

The results indicate that influencing employees' attitudes toward security is a better predictor of employees' effective use of security awareness programs than their intention to comply. Both intrinsic and extrinsic factors considered in this study are positively associated with the effective use of security awareness programs. The cultural effect has also proven to influence employees' effective use of security awareness programs. Collectivism and uncertainty avoidance are positively associated with the effective use of security awareness programs, while masculinity/femininity and power distance did not.

Furthermore, the study confirms that top management support is a decisive factor in helping increase the effective use of security awareness in the Congolese context. According to the findings, senior management must work on improving employees' intrinsic motivation and attitude concerning security awareness guidelines and must follow through with both reward and punishment. Finally, organizations should create a culture where each employee makes their peers accountable for following the security awareness guidelines.

DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

_____

Arnold Nzailu

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Background of the Problem

In today's highly connected world, the protection of digital assets has become a top priority for both organizations and nation-states. As organizations and countries are struggling to protect their assets, it becomes clear that information security is not just an IT problem but instead an organizational and national problem. Herath and Rao (2009) argued that the protection of assets within an organization is the responsibility of everyone within the organization. It does not limit itself to the IT department.

In the United States, like in many other countries, governments are demanding better cybersecurity protections for both the public and private sectors. The United States has passed and implemented initiatives, laws, and regulations such as the Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience, the Sarbanes–Oxley Act of 2002, and the Cybersecurity Act of 2015. The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience was aimed at advancing a national effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. The Sarbanes–Oxley Act of 2002 was passed to ensure an organization's board of directors discusses information security risks to the organization. The cybersecurity Act of 2015 was promulgated to provide that the Director of National Intelligence and the Departments of Homeland Security (DHS), Defense, and Justice develop procedures to share cybersecurity threat information with private entities, nonfederal government agencies, state, tribal, and local governments, the public, and entities under threats. While laws and regulations have shined a light on the issue of information security, organizations and nations are still struggling to protect their assets against cyber threats.

The protection of digital assets has become a priority for organizations and nation-states. The cost of circumventing security measures has increased exponentially, thus making it more difficult for hackers to penetrate organizations' information systems. In response,

hackers are adapting and taking advantage of "low-hanging fruit." Microsoft (Agrawal et al., 2019) explained that three of the low-hanging fruit routes most commonly employed by cyber attackers include social engineering, poorly secured cloud apps, and legitimate software platform features. Hackers are always looking for the path of least resistance in the security chain, and it is easier and less costly to social engineer a user into clicking a malicious link or opening a phishing email (Agrawal et al., 2019).

The identify theft resource center reported (Center, 2018) that the total number of breaches in 2018 was 1,244, which decreased by 23% from the total number reported in 2017, which was 1,632 breaches. However, the stated number of consumer records containing sensitive personally identifiable information (PII) jumped significantly, with a 126% increase from 2017 (197,612,748 records exposed) to 2018 (446,515,334 records exposed). A breakdown of the reported breaches shows that humans played a sizable role through either accidental exposure, employee error, negligence, improper disposal, unauthorized access, or insider theft.

In 2016, the Privacy Rights Clearinghouse, an organization that keeps tracks of data breaches made public, noted 501 breaches across all types of organizations in which approximately five million records were involved. Some of the breaches included Berks & Beyond Employment Services in which the file containing names, Social Security numbers, addresses, and other information were exposed at the City of Allentown Center for Recycling and Solid Waste. The files were placed in a public trash bin. Information on Crest Food employees was found in a dumpster at a recycling facility. Employment applications, direct deposit forms, Social Security numbers, and bank routing numbers were exposed (News9, 2016). Seagate employees fell for a phishing attack that exposed the W-2 information of all current and past employees (KrebSecurity, 2016). Mitchell International Inc's employees were victims of an individual impersonating an executive with the company who convinced one employee to provide information on current and former employees. The information compromised included first and last names, Social Security numbers, and salary information (Mitchell International, 2016). One employee from Advanced Auto Parts fell for a phishing attack in which an individual posing as an employee convinced the employee to provide a file containing information about individuals working for the company. The information compromised included names, Social Security numbers, 2015 gross wages, and the state(s) in

which the individuals paid income taxes (Advance Auto Parts, 2016). Democratic National Committee was hacked by Russian government hackers who accessed information about Democratic candidates as well as a database on opposition research against Donald Trump (Strauss, 2016). Hackers have breached databases for election systems in Illinois and Arizona. In Illinois, hackers accessed a database for the Illinois Board of Elections in which they compromised up to 200,000 personal voter records. The information compromised included names, addresses, sex, and birthdays, plus voters' social security number or drivers' license numbers(Wesley Bruer & Perez, 2016).

Bauer and Frysak (2014) supported the thought that insecure application and information systems are the sources of the many risks related to business operations in a ubiquitously connected world. Schlienger and Teufel (2003) argued that most organizations, while trying to secure their assets against threats in cyberspace, prioritize their security dollars and their effort on the technological aspect of the security equation. Although organizations are spending more money on security solutions, empirical data from surveys have shown that the respondents reported an increase in information security incidents over the years (Richardson, 2007). Sasse, Brostoff, and Weirich (2001) have shown in their research that organizations are spending large amounts of money on protective technology only to find out that they have been breached not because of inferior technology but because of the human factor of the security equation. A large number of breaches are because those organizations did not consider the human element while building their protective measures (Sasse et al., 2001).

Granger (2001) explained that focusing on technology alone while creating an enterprise security programs and ignoring the human factor of security is wrong as humans are considered the weakest link in the security chain. Werlinger, Hawkey, and Beznosov (2009) argued factors such as human, social, and organizational must be considered in addition to factors such as technology while building a security program. Zhang, Reithel, and Li (2009) believed that successful defense against cyber threats are directly related to understanding people involved in the security equation, arguing that it is of great importance that organizations understand their employees' attitude and behavior toward technology if they are to design and put in place adequate information security policies, processes, and technology (Zhang et al., 2009). Peltier (2005) argued that employees of an organization need

to be made aware of their rights and responsibilities when it comes to using the organization's information systems. He explained that the whole IT security architecture could be rendered ineffective if the employees using the technology are not aware of the risk related to the technology and do not know how they could avoid or mitigate the risk. Peltier (2005) explained that the implementation of employee awareness and training programs must address the people, the process, and the technology aspect of security in order to build an effective information security programs.

Both information security practitioners and researchers have noted the existing gaps in the security posture of organizations that did not consider the human aspect while building their information security programs. Therefore, there is a need to educate users about information security and their roles and responsibilities in the protection of the organization's assets. Form this was born the idea of the security awareness programs with the objective of effectively train users on how to defend themselves against human hacking (Chen, Shaw, & Yang, 2006).

Martinez-Moyano, Conrad, and Andersen (2011) are proponents of the idea that effective security awareness programs are the best way to reduce risk related to security breaches in an organization. Despite the implementation of security awareness programs, organizations are still finding themselves at the losing end of the fight against human hacking (Richardson & Director, 2008).

Straub Jr and Nance (1990) argued that information security policies must be structured in a way that helps the users with concrete guidelines on how to address the confidentiality, integrity, and availability of resources at their disposal while performing their job responsibilities. Additionally, both researchers and practitioners have concluded that management involvement is imperative in designing effective security policies that motivate user compliance with guidance in the security awareness programs (Dutta & McCrohan, 2002).

Information Security Awareness Programs

As the risk associated with information technology has increasingly become significant, so is the need for effective management of security. Kruger and Kearney (2006) expressed the need for information security to be a combination of both technical and

procedural controls in order to manage information security risks. Kruger and Kearney (2006) argued that a positive environment where everyone is aware of security risks related to information technology and behaves as expected is essential for the implementation of effective security controls. Additionally, they explained the difference between information security and information security awareness. They argued that while information security focuses on the protection of the confidentiality, integrity, and availability of assets, information security awareness focuses on maintaining and building positive security behaviors within an environment.

M. T. Siponen (2000) argued the importance of security awareness as information security techniques, and the procedure can be misinterpreted or bypass by end-users, therefore not reaching its goal of increasing the importance of information systems security and reducing the possibility of security breaches. Al-Omari, El-Gayar, and Deokar (2012) argue that there are two critical dimensions to information security awareness: General Information Security Awareness (GSA) and Technology Awareness (TA). D'Arcy, Hovav, and Galletta (2009) defined General Information Security Awareness (GSA) as " an employee's self-learning knowledge obtained by personal effort from the Internet, magazines, experience and other sources and understanding of potential issues related to information security and their ramifications." Dinev and Hu (2007) defined Technology Awareness (TA) as, "A user's raised self-consciousness of and interest in knowing about technological issues and strategies to deal with them obtained by personal effort from the Internet, magazines, and other resources.". The Information Security Forum (ISF) workshop participant defines information security awareness as " the degree or extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organization, their individual security responsibilities, and acts accordingly " (ISF, 2003).

Mitnick and Simon (2009, 2011) explained that human hacking is best defeated by implementing ongoing information security awareness programs. Mitnick and Simon believed that the security awareness goal is to modify people's behavior and attitude as they relate to protecting their organization's digital assets. They also preached a top-down approach to security awareness programs. They argued that for security awareness programs to be successful, senior management of the organization must show committed to the program, and the program must be customized to specific groups within the organization.

Wilson and Hash (2003) argued that just informing users of security breaches is not enough to improve the level of security awareness. They proposed the implementation of security awareness programs with interactive material that presented the learners with possible security issues scenarios. Wilson and Hash argued that this would help improve the security awareness of users and give them the ability to respond to a potential security incident.

Kruger and Kearney (2006) argued that the continual change in the risks spectrum requires information security awareness to be a dynamic process, reasoning that an awareness program needs to be continuously measured, managed and refreshed to ensure that is aligned with the organization's culture and the risks face by the organization. They concluded that keeping the information security material relevant and consistent, and varying the delivery mechanisms are the keys to a successful security awareness programs.

Statement of the problem

For a little more than two-decade now, information system researchers have noticed and argued that a good number of information systems implemented in organizations are not used at their full capability or are not used at all (Landauer, 1995). The number of failures in information system developments and implementations caught the attention of both organizations and researchers; the two groups want to understand the causes of the high number of failures and find solutions to avoid failure in future IT projects. IS researchers (Bulgurcu, Cavusoglu, & Benbasat, 2010; Gefen, Karahanna, & Straub, 2003; Pavlou & Chai, 2002; M. Siponen, Pahnila, & Mahmood, 2010) understood the need not only to understand the information system project at hand, but also to understand the individuals' inherent behaviors which are different across the cultures, ranging from individuals to organization, and organizations to a nation and/or across personal and demographic characteristics (Agarwal & Prasad, 1999; Venkatesh, Morris, Davis, & Davis, 2003).

Venkatesh et al. (2003) suggested that for successful IT implementation, organization leaders must prioritize individuals' needs and expectations over and above those of the system designers. Following the same trajectory as prior information security researchers (Aytes & Connolly, 2004; Harrington, Anderson, & Agarwal, 2006; Workman, Bommer, & Straub,

2008) argued that technology alone is insufficient to ensure information security within an organization, they explained that both information security researchers and practitioners need to pay attention to the human aspect of security. Following the call for an inclusion of the human character in IT projects, several intention-based theoretical models have been developed to predict behavior. The following IS theoretical models have predicted individuals 'acceptance behavior to adopt information systems.

- The technology acceptance model (TAM) (F. D. Davis, 1989; F. D. Davis, Bagozzi, & Warshaw, 1989) and the TAM2 (F. D. Davis & Venkatesh, 2004),
- The theory of reasoned action (TRA) (Fishbein & Ajzen, 1975),
- The diffusion of innovation theory (DOI) (Rogers Everett, 1995),
- The theory of planned behavior (TPB) (Ajzen, 1985) and;
- the unified theory of acceptance and use of technology (UTAUT) (Venkatesh & Zhang, 2010).

From all the theoretical models, the TAM has emerged as a robust conceptual model. TAM theorizes that behavioral beliefs such perceived usefulness (PU) and perceived ease of use (PEOU) affect acceptance intention (BI) and usage behavior (BU) (F. D. Davis, 1989; F. D. Davis et al., 1989). While the TAM has gained a wide recognition throughout the research community as a robust model, it has also been noted that the TAM has failed to take into account individual factors such as culture (Bagozzi, 2007; Karahanna, Evaristo, & Srite, 2006; Sharif Abbasi, Hussain Chandio, Fatah Soomro, & Shah, 2011; D. Straub, Keil, & Brenner, 1997).

Human behavior and attitude differ from one side of the globe to the other, hence the need for the regional study of issues related to information security in general and security awareness in particular. Straub tested TAM in three different countries, namely the United States, Swaziland, and Japan (D. Straub et al., 1997). The results did confirm that cultural bias is an essential factor that needs to be taken into account when trying to predict individual behavior. The results of Straub's study did find a similar variance explained in behavioral usage in the U.S. and Swiss samples but a very different variance in the Japanese sample context.

Leidner and Kayworth (2006) argued that an understanding of culture is vital to the study of information technologies because it can influence the successful implementation and use of information technology and because it can also play a role in managerial processes that may directly, or indirectly, influence IT. When an organization fails, culture is often and partially the cause of the failure. Helmreich (1994) argued that culture was partly to blame when Avianca Airlines had twice experienced crashes. The crashes were blamed in part on the national culture of the crew, whereby their national culture made them uncomfortable expressing disagreement with superiors or conveying bad news. In the first case, a crash occurred in Madrid even though warnings from the Ground Proximity Warning System to the captain was clear, but the captain continued to maintain the belief that his situational perception was better even when the copilot quietly asked questions hinting at his disagreement with the captain while complying with the captain's interpretation. In the second case, an Avianca flight crashed upon landing after circling several times in bad weather and eventually running out of fuel. The investigation revealed that the first and second officers, who came from national cultures where subordinates tend to withhold bad information from superiors to maintain harmony, failed to provide the captain with continual information on the worsening fuel situation.

The example above illustrate that culture has a subtle and yet powerful influence on people and organizations, and that information flows and information technologies are often closely intertwined with culture. Culture theory has been used to explain an extensive range of social behaviors, including job attitudes (Birnbaum & Sommers, 1988) and technology transfer practices (Hussain, 1998). Carmel and Agarwal (2002) and Kaiser and Hawk (2008) argued that given the increasing use of offshore development practices, it is increasingly important to understand how value differences in culturally diverse software development teams may influence the systems development process and subsequent development outcomes.

In today's global economy, the need to adopt technological advancement from western countries is growing in fast-developing countries. Researchers understand that a simple "copy & paste" of the different solutions will not produce the same results; therefore, regional research in technology adoption, user behaviors, and effective use are necessary, essential, and much needed. Most of the studies based on the TAM in the body of knowledge are

restricted to North America and Western countries and, more specifically, to the United States. Therefore, the results of these studies limit their generalizability and reliability across different cultures.

The following are a few adoption studies that have been carried out outside of the United States: Internet banking (Alsajjan & Dennis, 2010; Shih & Fang, 2004), broadband Internet use and adoption (Choudrie & Lee, 2004; Dwivedi, Khoumbati, Williams, & Lal, 2007) and academic, and email use (McCoy, Galletta, & King, 2007; D. Straub et al., 1997).

Prior research has mostly focused on end-user behaviors in the context of western countries and has attempted to generalize those behaviors across the globe. Robey (1979) argued that information systems implementation and usage can and do fail in situations where culture is ignored by the system designer. A similar line of research (Bourdieu, 1984; Choudrie & Lee, 2004; Loch, Straub, & Kamel, 2003; Rhee, Uleman, & Lee, 1996; Harry Charalambos Triandis, 1995) argued that culture-specific beliefs and social norms, as well as technological acculturation along with national policies and infrastructure, all have some degree of impact on systems adoption and usage.

Objectives of the project

Through its maturity as an art and science, Information Security and especially Security Awareness Training programs have proven to be invaluable tools in the fight against cyber threats. According to DeLone and McLean (1992, 2003) and D. W. Straub and Welke (1998), researchers and practitioners agree on the relevancy of security awareness programs in the fight again human hacking. While previous studies have looked at the effect of security awareness on user behavior in the context of western countries, we argue that western security awareness models do not universally hold across cultures and especially not in post-war developing countries such as the Democratic Republic of Congo (DRC).

The aim of this study is to develop and test a conceptual model of effective use of a security awareness programs that explains how motivation factors (intrinsic and extrinsic), cultural factors (power distance, masculinity/femininity, uncertainty avoidance, and individualism-collectivism) and information quality factors affect the effective use of a security awareness programs by employees in organizations in the DRC. This research aims

to contribute to the IS body of knowledge on security awareness, technology acceptance, and culture. Furthermore, we believe that this research will help policymakers and practitioners understand the reasons for the effective and ineffective use of security awareness programs in their cultural environment.

This research aims to answer the following questions:

- To what extent do motivation (intrinsic and extrinsic) factors affect employee engagement to use their organization's security awareness programs effectively?
- To what extent do individual-level cultural dimensions (power distance, masculinity\femininity, uncertainty avoidance, and individualism-collectivism) influence the relationship between the motivating factors, attitude toward security, intention to comply with security guidelines, and effective use of a security awareness programs?
- To what extent do information quality factors affect an effective employee use of security awareness programs?

Scope of the Research

It is crucial to define the scope of this study while taking into consideration the main aims and objectives of the research and the availability of resources such as time and money. This study investigates the factors that affect the effective use of security awareness programs by employees in organizations in the Congolese context. The scope of this research is summarized as follow:

- The area under investigation is the effective use of security awareness programs by employees in organizations in the DRC, particularly in the banking and telecommunication sectors. However, the results of this research could be generalized to other information-system-heavy industries.
- This study focused only on employees who use information systems to accomplish their daily work obligations in their respective organizations. Although other end-users such as contractors and consultants are considered to be necessary, the proposed conceptual model will only consider factors and

studies that are relevant to the effective use of security awareness programs from the employee's perspective.

- The investigation into the effective use of a security awareness program's behavior is limited to the geographical area of the Democratic Republic of Congo. Therefore, the applicability and the generalizability of the proposed conceptual model can become a problematic issue when applied in a different context or geographical area.
- This study is also limited by applying only Hofstede and Hofstede (1991)'s cultural dimensions at the individual level, as this study's primary concern is not the cultural models by itself. While other dimensions and cultural models are discussed in the literature review, they will not be part of our research plan.

The Significance of the research

Given the importance of information security awareness programs in contemporary organizations, this research provides useful and insightful information not only about the factors influencing the effective use of security awareness programs but also their impact on employees in Congolese cultural settings. The findings will help information security practitioners and researchers in the concerned cultural contexts to be better armed with knowledge about the specific motivation and cultural-related variables while working to improve the effective use of security guidelines in their organization or research study. Employee variables, such as behaviors and attitudes, cultural backgrounds, and other demographic characteristics, are essential variables that influence employee effective use of information systems. Understanding these variables is now helpful for information security practitioners to design meaningful security awareness programs to promote employee knowledge construction and make learning more effective and appealing.

M. T. Siponen (2000) called on Information Systems researchers to investigate security awareness in the realm offered by both motivation and behavioral theories. From an academic perspective, this research developed a model that combines both motivation factors and cultural theories at the micro-level (individual level) rather than the national level within different cultural contexts.

To our knowledge, no existing research has measured the impact of cultural factors at the individual level in the DRC as it related to information security. Therefore, this study can be considered a useful guide for other researchers to understand whether the motivation factors are mainly affected by individuals' cultural background or whether the motivation factors are primarily based on the fundamental determinants of the technology itself.

The research Contribution

The current research will primarily contribute to the literature on security awareness, adoption, motivations, and cultural studies. This research aims to make theoretical and practical contributions to knowledge as follows:

- From a broad perspective, this research will provide an overall picture of employees' views and usage of security awareness program guidelines in organizations in the DRC. The findings will help understand whether additional research is needed to address the needs of employees in efforts to close the gap that potentially exists between employees from various socioeconomic backgrounds.
- From a practitioner perspective, given the importance of information security awareness in contemporary organizations, the findings of this study will empower managers and policy-makers to formulate policies that appropriately target organizations to effectively use and improve the security awareness programs in place in their organization and to create security awareness programs that will be effectively used in the organization.
- Form an academic perspective; this research will provide a theoretical basis and empirical evidence of factors needed for employees in small and medium-sized organizations to effectively use the security awareness programs at their disposal. Also, it will provide elements required to build effective security awareness programs for small and medium organizations. Additionally, the result of this research will help develop fundamental and regional information security theories in the Democratic Republic of Congo.

CHAPTER 2

LITERATURE REVIEW

The Evolution of Information Security

Information Security has been around for as long as people have needed to keep secrets. The Caesar cipher is just one example of the ancient world practicing information security. Per the National Institute of Standards and Technology, it is unfortunate that developers and sometimes researchers are rediscovering problems and solutions since they have not taken the time to review many of the seminal papers. Therefore, it is crucial while studying information security to examine the original work in the field. In additional to seminal documents, we will also investigate pertinent laws, regulations, and directives related to information security.

The Summary of Seminal Papers in Computer Security

In early 1970, computer security had become a relevant topic, especially in the military, which was trying not only to provide a multilevel resource to its users but also to secure those shared systems against the threat from a malicious user. Several studies were performed, including:

- James P. Anderson's Computer Security Technology Planning Study Volume I and II; James P. Anderson's Computer Security Threat Monitoring and Surveillance;
- David E. Bell and Leonard J. LaPadula's Secure Computer System: Unified Exposition and Multics Interpretation;
- Richard Bisbey II and Dennis Hollingsworth's Protection Analysis: Final Report; Department of Defense's Trusted Computer System Evaluation Criteria;
- Ford Aerospace and Communications Corporation's Secure Minicomputer Operating System (KSOS) Executive Summary: Phase I: Design of the Department of Defense Kernelized Secure Operating System;

- Theodore Linden's Operating System Structures to Support Security and Reliable Software;
- Philip A. Myers's Subversion: The Neglected Aspect of Computer Security;
- Peter G. Neumann, L. Robinson, Karl N. Levitt, R. S. Boyer, and A. R. Saxena's A Provably Secure Operating System;
- Grace H. Nibaldi's Proposed Technical Evaluation Criteria for Trusted Computer Systems,
- J. M. Schacht's Job stream Separator System Design;
- Roger R. Schell, Peter J. Downey, and Gerald J. Popek's Preliminary Notes on the Design of Secure Military Computer Systems;
- W. L. Schiller's The Design and Specification of a Security Kernel for the PDP-11/45; Willis H. Ware's Security Controls for Computer Systems (U): Report of Defense Science Board Task Force on Computer Security; and
- Jerold Whitmore, Andre Bensoussan, Paul Green, Douglas Hunt, Andrew Kobziar, and Jerry Stern's Design for Multics Security Enhancements.

These studies had a tremendous influence on the development of many earlier systems such as the Atlas system and MULTICS, which was a time-sharing operating system, based around the concept of a single-level memory. The table 1 below, borrowed from Professor Matt Bishop at the University of California Davis, provides a summary of some of the studies.

Table 1. Early Information Assurance Research

Title	Authors	Summary
A Provably Secure Operating System	(Neumann, Robinson, Levitt, Boyer, & Saxena, 1975)	Summarizes work to date on the development of a design for a general-purpose computing system intended for secure operations.
Computer Security Technology Planning Study	(J. P. Anderson, 1972)	Volume II report of the work of the Computer Security Technology Planning Study

		Panel. Presents details supporting the recommended development plan.
Computer Security Threat Monitoring and Surveillance	(J. P. Anderson, 1980)	This is a final report of a study, the purpose of which was to improve the computer security auditing and surveillance capability of the customer's system.
DoD Trusted Computer System Evaluation Criteria	(Latham, 1986)	The trusted computer system evaluation criteria defined in this document classify systems into four broad hierarchical divisions of enhanced security protection.
Job stream Separator System Design	(Schacht, 1975)	Presents a technical and economic assessment of the Job stream Separator (JSS).
Multics Security Evaluation: Vulnerability Analysis	(Karger & Schell, 1974)	A security evaluation of Multics for potential use as a two-level (Secret/Top Secret) system in the Air Force Data Services Center (AFDSC).

An Overview of Information Related Laws and Regulations

Since information security is a relatively new field, it is essential to look at prominent laws and regulations. The laws and regulations in place today have been put in place for different reasons. The table 2 below presents the laws and regulations related to information security.

Table 2. Overview of Information Security Laws and Regulations

Regulations / Laws	Description
Privacy Act of 1974	The Privacy Act of 1974's objective was to establish a code of fair information practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.
Computer Security Act of 1987	The Computer Security Act of 1987 was passed to improve the security and privacy of sensitive information in federal computer systems and to establish minimum acceptable security practices for such systems. It requires the creation of computer security plans and the appropriate training of system users or owners where the systems house sensitive information.
Health Insurance Portability and Accountability Act of 1996	The Health Insurance Portability and Accountability Act of 1996 Title II was enacted to establish a national standard for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.
Presidential Decision Directive 63: Critical Infrastructure Protection	The American Presidential Directive PDD-63 of May 1998 set up national programs of "Critical Infrastructure Protection." The directive describes the United States as having some critical infrastructure that is "so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety."
Gramm-Leach-Bliley Act – Title – V	Title V, Subtitle A of the Gramm-Leach-Bliley Act ("GLBA") was established to govern the treatment of nonpublic personal information about consumers by financial institutions. Section 502 of the Subtitle, subject to certain exceptions, prohibits a financial institution from disclosing nonpublic

	personal information about a consumer to nonaffiliated third parties.
Sarbanes-Oxley Act	The Sarbanes-Oxley Act of 2002 was enacted to address corporate governance, financial reporting, and internal control issues in the aftermath of public company collapses, such as Enron and WorldCom. Section 404 of the Act mandates, among other reporting and audit requirements, that companies establish a system of internal controls to ensure adequate financial reporting.
Homeland Security Act of 2002	In response to the terrorist attacks on the United States, the Homeland Security Act of 2002 established the Department of Homeland Security, which enabled a massive restructuring of the federal agencies that perform security functions. At the same time, the government published its "National Strategy to Secure Cyberspace," which outlined several programs that later translated into specific regulations.
E-Government Act of 2002 (Title III – FISMA)	The Federal Information Security Management Act (FISMA) was approved in December 2002 as Title III of the broad-based E-Government Act of 2002. Under FISMA, which supersedes the Government Information Security Reform Act of 2000 (GISRA), federal agencies are required to assess the state of their security before being approved for budget items by the OMB. This is the first federal law to tie security assessments with budget approval. FISMA requires federal agencies to assess the security of both classified and non-classified systems and to include risk assessment and security needs with each new budget request.
NERC 1200 Urgent Action Cyber Security Standard	Commonly called NERC 1200 UAS, the purpose of this standard is to reduce the overall vulnerability of the bulk electric systems to cyber threats. The cybersecurity standard defines requirements in 14 control areas.

California Individual Privacy Senate Bill – SB 1386	California SB1386 is another example of states setting privacy standards that are greater than those at the federal level. Among other requirements, organizations experiencing a security breach that may have revealed the "private information" of California residents must notify each of these individuals.
National Security Presidential Directive 54	This directive establishes the United States policy strategy, guidelines, and implementation actions to secure cyberspace. It strengthens and augments existing policies for protecting the security and privacy of information entrusted to the Federal Government and clarifies the roles and responsibilities of Federal agencies relating to cybersecurity. It requires the federal government to integrate many of its technical and organizational capabilities to better address sophisticated cybersecurity threats and vulnerabilities.
Presidential Policy Directive/Ppd-21	Presidential Policy Directive-21: Critical Infrastructure Security and Resilience replaces Homeland Security. Presidential Directive-7 and directs the Executive Branch to develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real-time, understand the cascading consequences of infrastructure failures, evaluate and mature the public-private partnership, update the National Infrastructure Protection Plan, develop comprehensive research and development plan.

A review of the objective of each of the above security regulations has brought to light the fact that no new security concepts are introduced through the years. The different regulations are presenting the same security concepts using different words and contexts. They are all aiming at the same goals that we believe can be achieved by putting in place

security policies, procedures, education, and training that consider not only the organizational structure but also the national and individual culture.

In the next section, we reviewed the literature to understand the concept of security awareness and how prior researchers and practitioners have defined it through the years.

Information Security Awareness Definition

Häußinger (2015) analyzed 131 articles from the IS literature related to information security awareness and could not find a standard definition of the term "security awareness." Even more surprising, he noted that few of the articles discussing the topic of security awareness did not define what the concept was. From the 131 articles analyzed, 21 articles attempt to define what information security awareness is. Based on the open coding work performed on the different definitions of information security awareness from the literature by Häußinger (Häußinger, 2015), three major groupings of the definition were namely "cognitive," "behavioral," and "process." From a cognitive point of view, information security awareness (ISA) is mapped to the employees' state of mind. From a behavioral aspect, ISA focuses on the employees' actions as they relate to the organization information security policies. From a process perspective, ISA focuses on the procedural aspect of an organization used to raise awareness. The information security awareness definition presented in this dissertation will follow the three main groupings proposed by Häußinger (Häußinger, 2015). From a cognitive aspect, Banerjee and Pandey (2010) defined security awareness as the knowledge that members of an organization possess regarding the protection of the physical and information assets of that organization. Bulgurcu, Cavusoglu, and Benbasat (2009) defined information security awareness (ISA) as an employee's general knowledge about information security and his cognizance of the ISP of his organization. Additionally, they define General information security awareness as an employee's overall knowledge and understanding of potential issues related to information security and their ramifications. Choi, Kim, and Goo (2006) defined information security awareness as the mental aspect of users being aware of the significance of information security.

From a behavioral aspect, ISF (2007) defined security awareness as the extent to which staff understand the importance of information security, the level of security required

by the organization and their individual security responsibilities, and act accordingly. Galvez and Guzman (2009) defined information security awareness as a user's increased consciousness of and interest in knowing about security issues and the strategies to deal with those issues when they arise.

From a process aspect, Peltier (2005) defined information security awareness as a process that is used to stimulate, motivate, and remind the audience what is expected of them. Kritzinger and Smith (2008) defined information security awareness as a process that ensures that all employees in an organization are aware of their role and responsibility toward securing the information they use.

Information Security Awareness Literature

M. T. Siponen (2000) explained that an organizational state in which users in an organization are aware of the information security responsibility could be referred to as an information security awareness state. Mitnick and Simon (2009) explained that human hacking is best defeated by implementing ongoing information security awareness programs. They pushed forward the idea that an information security awareness goal is to modify people's behavior and attitude as they related to protecting their organization's digital assets. They also promote a top-down approach to security awareness programs. They argued that for a program to be successful, management of the organization must show commitment to the programs and that the programs must be customized to specific groups within the organization. Wilson and Hash (2003) argued that just informing the user of security breaches is not enough to improve the level of security awareness. They proposed the implementation of security awareness programs with interactive material that presented the learners with possible security issues scenarios. They argued that this would help the improve security awareness of users and give them the ability to respond to a potential security incident.

As early as 2005, the CIS/FBI report on computer crime predicted that information security awareness would be one of the most critical issues in information security (Gordon, Loeb, Lucyshyn, & Richardson, 2005). Mackenzie (2006) analyzed the information security breaches for the past years and noted that more than half of the breaches were linked to a social engineering attack.

A little bit more than fifteen years later, CIS/FBI prediction remains accurate regarding the number of successful social engineering attacks across multiple industries. The SANS Security Awareness Report 2018 revealed that security awareness field is still very immature because the majority of security awareness professionals report their program activity as being only a portion of their job responsibilities; many have reported that they either have no budget or don't know what their budget is; and most lack the skills or background to effectively communicate to and engage with their workforce. Report also revealed that 67 % Awareness professionals report they have the leadership support they need to run and maintain their awareness programs effectively; 71 % Organizations identify themselves in the Behavior stage or greater in the Security Awareness Maturity Model, and 85% Awareness professionals report their work has a positive impact on the security of their organization.

Although the technology to protect security breaches has gotten better, it seems that security breaches are still on the rise due to human hacking. Western organizations are struggling with this problem even when they have spent millions to educate their employees against social engineering attacks. Figure 1 below presents the benchmarking Maturity By Industry.

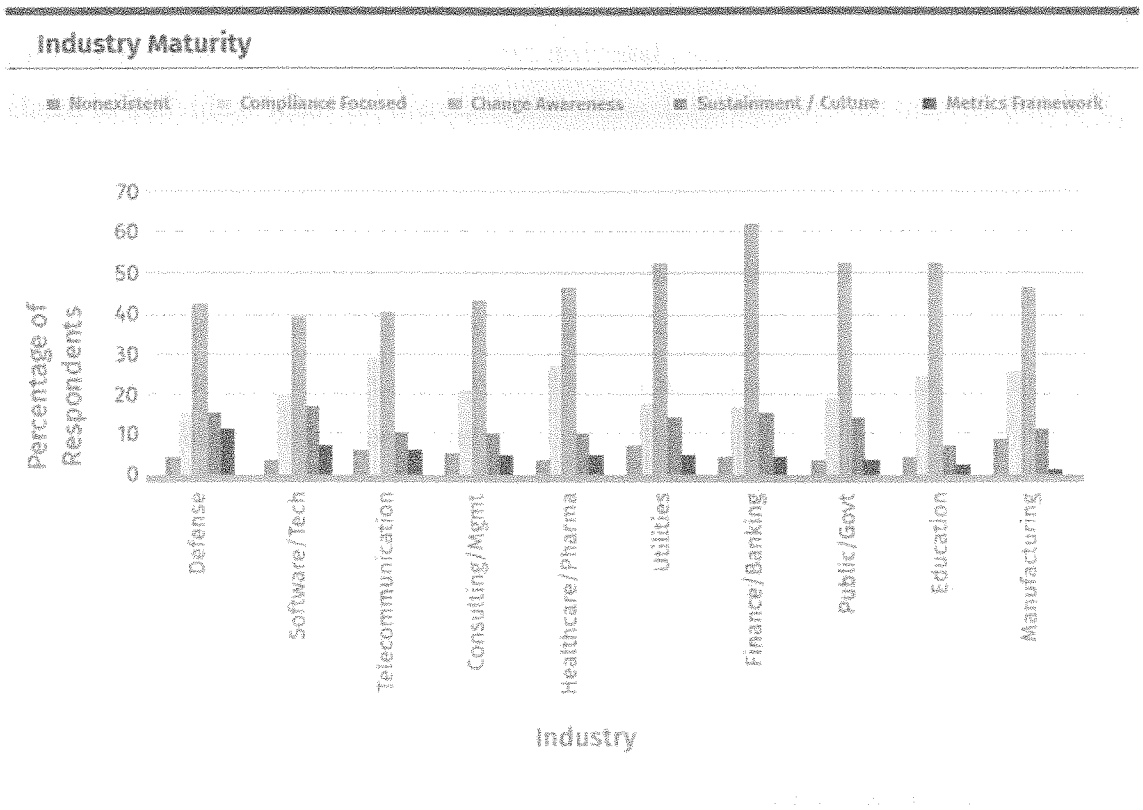

Figure 1. SANS Security Awareness Maturity Model

Theories and Models

M. T. Siponen (2000) argued that the currents descriptive nature of security awareness programs is not accomplishing its objective of improving security behavior. He linked the failure of information security programs to the nature of the security awareness programs and education. He called for IS research to investigate security in the realms of both motivation and behavioral theories. E. L. Deci and Ryan (1987) argued that motivation is a crucial determinant of general behavior in information technology acceptance behavior and work-related behavior (George & Brief, 1996). Two broad classes of motivation –extrinsic and intrinsic have been defined and examined across various contexts and studies (Ang, Quek, Teo, & Lui, 1999; E. L. Deci & Ryan, 1975, 1987). Ryan and Deci (2000) argued that there is a distinction between different types of motivation based on the various reasons or goals that give rise to an action. Moon and Kim (2001) claimed that together, extrinsic and intrinsic

motivation influence original intentions regarding activity as well as the individual's actual behaviors. It is clear from the past research that extrinsic and intrinsic motivations are strongly related to individual behavior; therefore, this research investigates the theories below that involve user behavior and intention.

The theory of reasoned action (TRA) (Ajzen & Fishbein, 1980), the theory of planned behavior (TPB) (Ajzen, 1991), and the technology acceptance model (TAM) (F. Davis, 1986) are the best known and most used models in IS to study the acceptance of technology. Although of the three, the TAM is arguably the most widely accepted for use in technology acceptance studies, we discuss the three models.

Theory of Reasoned Action (TRA)

Fishbein and Ajzen (1975) introduced TRA. Like the Social Cognitive Theory, the Theory of Reasoned Action also derived from social-psychological settings. To the contrast of the Social Cognitive Theory, where Attitude was the primary predictor of the behavior, the Theory of Reasoned Action assumes intention to be the most important determinant of individuals' behavior. In TRA, beliefs influence attitude to shape intention, which in turn guides or dictates behavior to perform, e.g. (Chau & Hu, 2001).

Ajzen and Fishbein (1980) suggested that the TRA is based on the assumption that individuals are rational and make systematic consideration of their actions' implications before they decide to engage or not engage in a given behavior. TRA is based on three significant constructs and their relation to each other as follows:

- Behavioral intention (BI): is the extent to which an individual formulates a conscious plan to perform or not perform some specified future behavior towards a target (Warshaw & Davis, 1985). Ajzen and Fishbein (1980) and Fishbein and Ajzen (1975) argued that an individual's relative strength to perform a task is dependent upon a person's attitude towards the behavior and/or the subjective norms.
- Attitude (A): is the product of critical behavioral beliefs and the individual's outcome evaluation (Fishbein & Ajzen, 1975). Behavioral beliefs are a subjective probability that behavior leads to a particular outcome. In an extension of TRA known as the TAM, F. D. Davis (1989) defined these

behavioral beliefs with the perception of usefulness (PU) and perception of ease of use (PEOU) by which one evaluates differently.

- Subjective norms (SN): defined as 'the person's perception that most people who are important to him or her think he should or should not perform the behavior in question' (Fishbein & Ajzen, 1975). In SCT, it is considered with the concept of social influence (Agarwal & Prasad, 1999), which is examined by the opinion of friends, family, colleagues, peers, and social groups (Miller et al., 2005). TRA suggested that the strength of SN is based on an individual's normative beliefs multiplied by the motivation to comply with the opinion of essential referents.

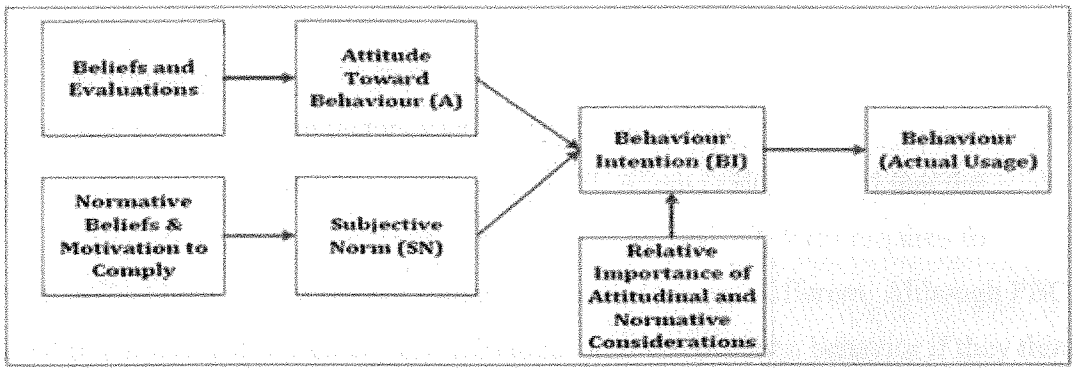

Figure 2. TRA Model

Madden, Ellen, and Ajzen (1992) suggested that the Theory of Reason Action can be explained by the notation of BI=A+SN, which means beliefs affect intentions and behavioral consequences either through A or SN. TRA demonstrates an individual's BI is dependent on the individual's A towards BI and SN.

Theory of Planned Behavior (TPB)

To overcome the limitations of TRA to predict behavior under the condition where individuals have a low level of violation control, Ajzen (1991) proposed a revised version of TRA known as the Theory of Planned Behavior (TPB). Ajzen (1991) incorporated an additional exogenous construct, namely perceived behavior control (PBC), in previous TRA constructs to predict planned and deliberate behavior. Taylor and Todd (1995b) argued that PBC was a perception of internal and external constraints on behavior. Behavioral control is

defined as beliefs about the presence of some factors that may facilitate or impede the performance of the behavior. It is considered different from SN, which is perceived as social pressure or normative expectations from others, which also influences the BI to use.

The Theory of Planned Behaviors has been adopted in several fields and has produced significant results. For example, Chau and Hu (2001) and Conner and Sparks (1996) used it in healthcare settings, Nguyen, Potvin, and Otis (1997) used it in an exercise program, and Conner, Povey, Sparks, James, and Shepherd (2003) used it in diet control settings. Within information system research, many studies examined TPB and emphasized the importance of the construct PBC in determining BI and usage (e.g., (Chau & Hu, 2001; Foxall, 1997; Mathieson, Peacock, & Chin, 2001; Taylor & Todd, 1995b).

The Theory of Planned Behaviors, like its predecessors, also suffers from several limitations. Eagly, Ajzen, and Taylor discussed some of the limitations. Eagly and Chaiken (1993) argued that there are more factors such as habit, moral obligation, and self-identity that might influence behavior but are not considered in TPB. Ajzen (1991) argued that the inability of TPB to move beliefs from context-specific to generalized form requires for measurement amendment every time the context or populations are different. Although PBC influences BI in a sense that it predicts any individual who can perform behavior if they think that they are able to do it, TPB fails to explain the mechanism by which the individual will perform that behavior (Taylor & Todd, 1995b). Finally, combining all unknown or unspecified factors affecting behavior in the PBC construct might affect the prediction accuracy (Taylor & Todd, 1995b).

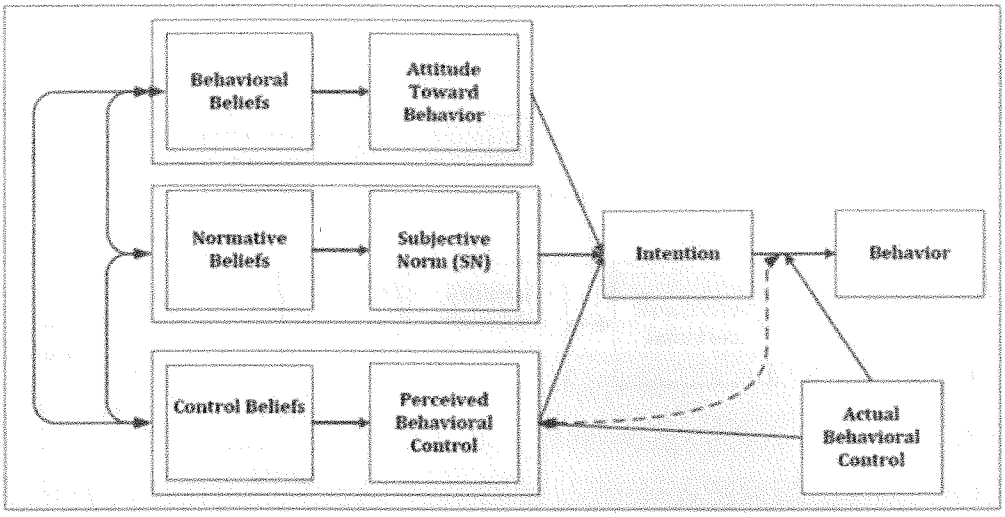

Figure 3. TRA Model

Technology Acceptance Model (TAM)

The Theory of Reason Action has received considerable attention in the fields of information system research as well as in social, health, and business studies. Within information system research, TRA has been revised by many researchers, and various external variables were added to examine the effect of attitude and/or subjective norms over behavioral intention for use in specific contexts. In a similar line of research, F. D. Davis et al. (1989) extended the theory with a theoretical framework of individuals' acceptance of technology known as the TAM. F. D. Davis et al. (1989) proposed a theory for the domain of IT in the form of the now widely accepted conceptualization of IT acceptance: the Technology Acceptance Model (TAM). TAM has initially been an adaptation of the Theory of Reason Action (TRA) that includes the idea that attitude (A) predicts intention (BI), and intention predicts behavior (BU) as a predictor of individual behavior. To the distinction of TRA, the TAM excluded subjective norms (SN) as a determinant of BI due to the uncertain theoretical and psychometric properties (F. D. Davis et al., 1989).

Fishbein and Ajzen (1975) urged researchers against the use of subjective norms (SN) as this last could create theoretical and empirical problems due to the difficulty of differentiating the direct effect of subjective norms on behavioral intention (BI) from indirect effect via Attitude (A). An additional distinction between TRA and TAM is that unlike expectancy formulation of beliefs within the TRA, the TAM suggested only two beliefs,

perceived usefulness (PU) and perceived ease of use (PEOU) are necessary to predict an individual's Attitude towards using technology.

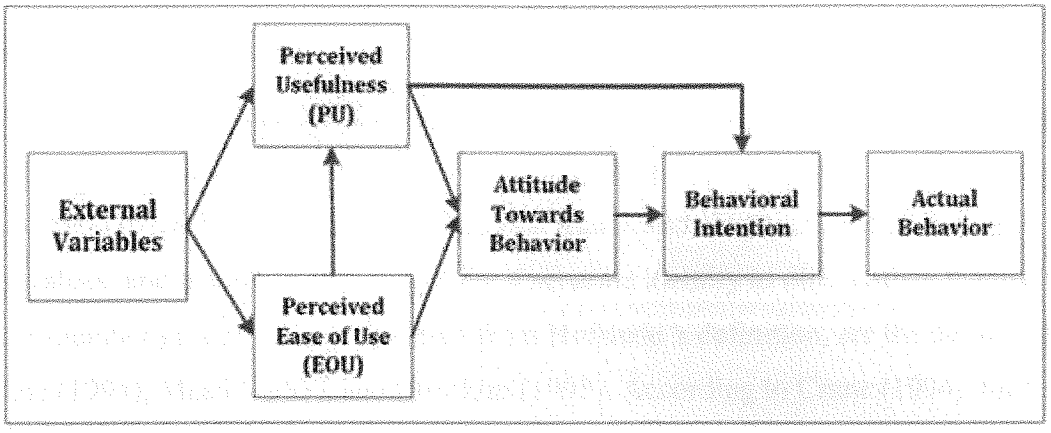

Figure 4. TAM Model

A large number of studies applying TAM has enabled researchers to detect TAM limitations. The explanatory power of TAM is doubtable because it does not take into account the effect of social, individual and cultural influence on the acceptance of technology (Bagozzi, 2007; Benbasat & Barki, 2007; D. Straub et al., 1997; Straub Jr & Burton-Jones, 2007; Teo, Wong, & Chai, 2008). Additionally, the majority of studies has been within the context of developed countries in North America.

Cultural Issues and Information Security Awareness

This section of the dissertation discusses culture and its impact on theories to predict an individual's behavior in information security. By reviewing the cultural aspect of research, more information about its role in behavioral theories related to information security will be understood. Additionally, answers to questions such as why the theories and models developed in one country are not all successful when applied in other countries, and why theories and models are not found to be uniformly effective across the cultures when the aim is to predict an individual's behavior in information security.

Leidner and Kayworth (2006) reviewed 82 articles from the body of knowledge and observed the following themes: (1) culture and information systems development, (2) culture, IT adoption, and diffusion, (3) culture, IT use, and outcomes, (4) culture, IT management, and strategy, (5) IT's influence on culture, and (6) IT culture. Details of the themes (1), (2), and (3) which are directly relevant to this study are discussed in the upcoming section. The next

section will define culture and discuss the different cultural models and dimensions and their impact on behavioral theories in the information security literature.

Definition of Culture

According to Hofstede and Hofstede (2005), culture is the collective programming of the mind that distinguishes the members of one group or category of people from another. He has argued that culture is a learned way of life that shares and shapes individuals'/groups' attitudes, values, and practices, and gives them a separate identity to differentiate themselves from other member groups. A little different from Hofstede 's definition, are the definitions from Crane (1994), Mead (1953), and Hoecklin (1995). According to Crane (1994), the term "culture" can be defined as something that is an obvious or recordable act; whereas, Mead (1953) argued that culture is a shared pattern of behavior. The commonality of the above two definitions is that culture is a group-level construct. Consistent with and in support of the themes of these two definitions, Hoecklin (1995) defined culture as a "shared system of meanings; relative, learned; (and) about groups." Kroeber and Kluckhohn (1952) defined culture as "patterned ways of thinking, feeling and reacting, acquired and transmitted by symbols, constituting the distinctive achievements of human groups, including their embodiments in artifacts; the essential core of culture consists of traditional (i.e., historically derived and selected) ideas and especially their attached values". Harry C Triandis (1972) argued, "Culture is defined as an individual's characteristics, way of perceiving the human-made part of one's environment. It involves the perception of rules, norms, roles, and values, is influenced by various levels of culture such as language, gender, care, religion, place of residence, and occupation, and it influences interpersonal behavior".

Culture and Information Systems Development (ISD)

Dagwell and Weber (1983) examined the systems designers' perceptions of end-users across four national groups (United States, United Kingdom, Australia, and Sweden) and found that Australian and Swedish systems designers favor a Theory Y orientation (people-oriented) in assessing user needs whereas UK and U.S. designers favor a Theory X (process and efficiency-oriented) approach in evaluating user needs. Tan, Smith, Keil, and Montealegre (2003) examined the impact of national culture on the predisposition to report

bad news about failing ISD projects and found that individualistic cultures amplify the impact of organizational climate on inclination to report bad news (compared to collectivism) whereas collectivism strengthens the impact of information asymmetry on predisposition to report bad news (compared to individualism). Kumar et al. (1990) used the Personal Values Questionnaire to study differences in systems designer values between Danish and Canadian subjects and found that the Danish designers (more socialist values) placed greater emphasis on people-related issues in ISD projects while the Canadian subjects (more capitalist values) tended to focus more on technical issues. Leidner and Kayworth (2006) argued that the variation across cultural values might lead to differing perceptions and approaches to how information systems are developed. The above findings provide reasonable evidence that culture may influence Information Systems Development.

Culture and Information Technology Adoption and Diffusion

Loch et al. (2003) studied the diffusing of the Internet in the Arab world. Their results suggest that the degree of similarity in values concerning technology between adopting and host countries will influence the level of adoption of IT. In particular, they found that the acceptability of computer culture in Arab countries was positively related to the level of Internet usage. Similarly, Hill, Loch, Straub, and El-Sheshai (1998) researched five Arab countries and found that specific cultural values (preference for face-to-face interaction, allegiance to family, the concept of time, religion, and gender relations) tended to either facilitate or impede technology transfer to the host countries. Hoffman and Klepper (2000) found that organizations low in sociability and high in solidarity (mercenary cultures) experienced more favorable outcomes with technology assimilation than did more networked (high sociability and low solidarity) cultures. Leidner and Kayworth (2006) argued that groups are more likely to adopt a technology if their values match or fit the values embedded within the technology or those associated with its development. The above findings provide reasonable evidence that culture may predispose certain social groups toward either favorable or unfavorable IT adoption and diffusion behaviors. The degree of fit between social groups' values and values embedded in the IT has emerged as an essential construct for studying the relationship between culture and IT adoption and diffusion.

Culture, Information Technology Use and Outcomes

Chau, Cole, Massey, and Montoya-Weiss (2002) researched cultural differences in the online behavior of consumers between Hong Kong and the United States. They found that consumer attitudes toward the Internet varied significantly between Hong Kong (value preferences for shared loyalty and relationships) and the United States (value preferences for personal competence and loyalty to oneself) subjects. The results indicate that Hong Kong subjects used the Internet primarily for social communication, while U.S. respondents used it primarily for information search. These results suggest that cultural values shape how people use information technology. Leidner, Carlsson, Elam, and Corrales (1999) also studied the use of executive information systems and concluded that cultural values influenced perceptions of EIS use outcomes. They found that this technology was more favorably perceived in countries with lower power distance and uncertainty avoidance than in countries high in uncertainty avoidance and power distance. The studies of Downing, Gallaugher, and Segars (2003) and Rose, Evaristo, and Straub (2003) have also produced similar results. Robey and Rodriguez-Diaz (1989) found that closeness of fit between U.S. headquarters and subsidiary cultural values was a significant predictor of implementation success of accounting information systems at two foreign subsidiaries in Panama and Chile. The subsidiary with values most like the U.S. office (Panama) experienced the least implementation difficulty. Leidner and Kayworth (2006) argued that the differences in culture result in differences in the use and outcomes of IT. The authors argued that like with the research on culture, IT adoption, and diffusion, the notion of fit figures prominently in the research on culture, IT use, and outcome. The above findings provide reasonable evidence that culture may predispose certain social groups toward either favorable or unfavorable information technology use and outcomes.

The table below presents investigations related to Culture and Information systems. A large portion of element of the table below have been borrowed from literature (Dagwell & Weber, 1983; Leidner & Kayworth, 2006; Walsham, 2002).

Table 3. Culture and Information Systems Studies

Citation	Methodology and Measure of National Culture	Independent Variables*	Dependent Variable *Moderating Variable*	Relevant Finding(s)
Information Systems Development				
Dagwell and Weber (1983)	Survey of systems designers from U.S., UK, Australia, and Sweden • culture not measured	System designers' perceptions of users	Systems design approach *National culture*	Study found that Australian and Swedish systems designers favor a Theory Y orientation (people-oriented) in assessing user's needs whereas UK and U.S. designers favor a Theory X (process and efficiency-oriented) approach in evaluating user needs.
Hunter and Beck (2000)	Field study interviews (using Repertory Grid Analysis) of 70 Canadian and 17 Singaporean respondents • Hofstede's Cultural Indices**	National culture (IC, PD, UA, MF)	Perceptions of excellent systems analysts	Differences found across cultures in how excellent systems analysts are perceived. Excellent analysts from Singapore (high collectivism, low UA) are perceived to follow a more technocratic, dominant approach to clients while Canadian analysts (high individualistic, moderate-low UA) follow a more participative approach.
Keil, Tan, Wei, Saarinen, Tuunainen, and Wassenaar (2000)	Matching lab experiments in Finland, Singapore, and Netherlands • Hofstede's Cultural Indices	Risk propensity, sunk cost, risk perception	Decision maker's willingness to continue a troubled IT project National culture (UA)	Cultures low in uncertainty avoidance (Singapore) exhibited greater tendencies to continue with troubled IT projects since their perceived risk was lower than with high uncertainty avoidance cultures.
Kumar, Bjorn-Andersen, and King (1990)	Field survey of 72 Danish and 132 Canadian systems designers • England's Personal Values Questionnaire (1967)	Designer's values (technical, economic, socio-political)	IS design choices	System designers' values vary across cultures. In the IS development process, Danish designers (socialistic culture) were found to be (1) more concerned with people issues, (2) less concerned about cost issues, and (3) less concerned about technical issues than their Canadian (capitalistic culture) counterparts.
Peterson and Kim (2003)	Survey of U.S., Japanese, and Korean IS developers • culture not explicitly measured	Level of user involvement and designer experience	Perceptions of IS risks and failures National culture	Lack of user involvement and a lack of experienced IS personnel was perceived as greater risk factors in Korea than in both Japan and the United States.
Tan, Smith, and Keil (2003)	Matching lab experiment in Singapore and U.S. • Hofstede's cultural indices	Organizational climate, information asymmetry	Predisposition to report bad news National culture (IC)	Individualistic cultures amplify the impact of organizational climate on predisposition to report bad news (compared to collectivism) whereas collectivism strengthens the impact of information asymmetry on predisposition to report bad news (compared to individualism).
Walsham (2002)	Structurational analysis of two IS development projects • culture not specifically measured (KVI)	Structure (meaning, forms of power relations, sets of cultural norms)	Conflict and contradiction in software production and use	Analysis explains how structural differences (e.g., cultural norms) of systems developers led to conflict and contradiction among developers in the software development process. However, findings also suggest that over time, the respective cultural values of developers were dynamically shaped through the software development process.
IT Adoption and Diffusion				

DeVreede, Jones, and Mgaya (1998)	Grounded theory field study of 11 African GSS projects • culture not measured	Adoption factors: TMT endorsement, satisfaction with use, computer literacy, referent power, oral communication preference	Technology (GSS) acceptance	Study indicates GSS acceptance is rated positively or negatively based upon several dimensions of African culture: high preference for oral communication (negative), high referent power (negative), and high power distance (positive).
Galliers, Madon, and Rashid (1998)	Single site case study of a government agency in Pakistan • culture not explicitly measured	National culture	Rate of technology adoption	Found that implementation efforts were thwarted by prevailing cultural values (e.g., low uncertainty avoidance, poor culture for information used for decision-making). Some anecdotal evidence that over time, newly introduced ITC influences certain cultural values related to honesty and information use.
Garfield and Watson (1998)	Descriptive case study (content analysis) of government NII archives across 7 countries • Hofstede's cultural indices	National culture (UA, PD)	Structure of national information infrastructure (NII)	National culture plays a significant role in the development of a NII. Seven-country study suggests that countries will follow similar NII development models (family, village market, pyramid of people, or well-oiled machine) based upon similar cultural values related to uncertainty avoidance and power distance.
Griffith (1998)	Laboratory experiment comparing U.S. and Bulgarian student GSS teams • Hofstede's culture indices	National culture (PD)	Satisfaction with GSS	Findings demonstrate that Bulgarian students (lower power distance) were more likely to report being dissatisfied with the GSS outcome than were the U.S. students (with higher power distance).
Hasan and Ditsa (1999)	Interpretive field study of 10 organizations in the Middle East, Africa, and Australia • Hofstede's culture indices	National culture (UA, PD, IC, MF)	Technology transfer outcome	Study reveals that (1) IT is less readily adopted in risk-averse cultures (uncertainty avoidance) since technology is perceived as inherently risky, (2) successful adoption of IT is more likely where IT staff are able to give advice to IT managers (low power distance), (3) adoption of group-oriented IT (e.g., GSS) is more favorably disposed to collectivist vs. individualistic cultures, and (4) patterns of IT adoption may vary according to level of masculinity (technology focus) vs. femininity (focus on people and end-users) of culture
Hill, Loch, Straub, and El-Sheshai (1998)	Multimethod study (focus groups, interviews, field research) using surveys and interviews • culture not explicitly measured	Cultural factors that impede or support transfer of IT to host country	Technology transfer success	IT transfer is hindered when certain aspects of culture embedded in information technology do not mesh with the prevailing Arab culture. Facets of Arab culture that strongly influenced IT transfer are preference for face-to-face interaction, allegiance to family and kin group, concept of time, religion, and gender relations.
Hussain (1998)	Qualitative field study of 5 Japanese-Brunei joint ventures • culture not explicitly measured	National culture (open vs. closed)	Technology transfer success	The extent of cultural openness (accommodation of each other's culture) has a strong positive influence on the degree to which the technology transfer is successful.

Jarvenpaa and Leidner (1998)	Single site case study (semi-structured interviews) of Mexican firm • Hofstede's culture indices	Resource-based competencies (information culture, information infrastructure)	Information services industry diffusion National culture (IC, UA)	Mexican information services company succeeded despite presence of certain cultural barriers (e.g., high uncertainty avoidance and collectivism). Results show how managerial actions to shaped resource-based competencies led to shaping/recreating an information culture receptive to the information services industry. This transformation of culture led to greater levels of diffusion/acceptance of company's information services products.
Loch, Straub, and Kamel (2003)	Multimethod study (survey with follow- up interviews) of Arab respondents • social norms (self- developed Likert scale)	Technical culturation, social norms	Level of Internet usage	The level of technical culturation (the level of cultural exposure and experiences that individuals have with technology developed in other countries) and acceptability of computers (a social norm) positively influences the level of Internet usage in an Arabic-speacking country.
Png, Tan, and Wee (2001)	Multinational survey of 153 businesses in 23 countries • Hofstede's culture indices	Organizational size, national culture (UA, PD)	IT infrastructure adoption (frame relay)	Results show that (1) businesses from higher uncertainty avoidance countries were less likely to adopt information technology infrastructure (frame relay), and (2) power distance was not significantly correlated with adoption of frame relay technology.
Srite (2000)	Field study of international students from 33 countries• Hofstede's culture indices	Willingness to innovate, trust in technology, subjective norms	Technology Acceptance National culture (UA, PD, IC, MF)	Individuals from high power distance countries were found to be less innovative and less trusting of technology.
Straub (1994)	Multimethod study (field interviews, survey, policy capturing) comparing U.S. and Japanese respondents • Hofstede's cultural indices	Perceived useful-ness, ease of use	Media use (e-mail and fax) National culture (UA)	Cultural differences between the U.S. and Japan account for differences in the diffusion rate of email technology. Japanese workers are less likely to adopt and use email since their high uncertainty avoidance culture prefers more information-rich, socially present forms of communication.
Al-Ghatani (2003)	Survey of 1200 Saudi managers and govt. officials • culture not explicitly measured	Perceived attributes of technology	Rate of technology adoption National culture	Study validated the use of Rogers' (1995) five perceived attributes of technology (relative advantage, complexity, trialability, compatibility, and observability) as predictors of technology adoption in a non-Western cultural context.
Shore and Venkatachalam (1999)	Case study • Hofstede's culture indices	Competitive environment, task congruency	IT transfer success National culture (PD, UA)	National culture has an influence on the success of information technologies transfer from host to recipient countries.
Straub, Keil, and Brenner (1997)	Survey of airline employees from U.S., Japan, and Switzerland • Hofstede's culture indices	Perceived usefulness, perceived ease of use	Information systems use National culture (IC, UA, PD, MF)	Results indicate that TAM holds for both U.S. and Switzerland, but not for Japan (high PD, high UA, collectivist, more assertive). This suggests that TAM may not be universally applicable across cultures.

Thatcher, Srite, Stepina and Liu (2003)	Survey of U.S. college students • Cultural indices by Hofstede	National culture (UA, IC, PD, MF), Qualitative and quantitative work overload (mediating)	Personal innovativeness with information technology (PIIT)	Results suggest that individuals high in uncertainty avoidance and power distance may be less willing to innovate or experiment with information technology
IT Use and Outcomes				
Calhoun, Teng, and Cheon (2002)	Survey of Korean and U.S. professionals • Cultural indices by Hofstede (1980), Hofstede and Bond (1988), and Hall (1976)	Intensity of IT use	Decision making activity *National culture*	High context culture respondents (Korea) experienced much higher levels of information overload from IT use on operational decisions as compared to respondents from a low context culture (U.S.).
Chau, Cole, Massey, Montoya-Weiss, and O'Keefe (2002)	Multimethod • Experimental study and follow-up survey of Hong Kong and U.S. undergraduate students • culture not explicitly measured	Purpose of internet use (social communication, hobby, e-commerce, information search)	Consumer attitudes toward web sites *National culture*	Differences between Hong Kong (characterized by respect for relationships and shared loyalty) and U.S. (characterized by focus on personal competence and loyalty to oneself) subject's use of the Internet (Hong Kong–social communication; U.S.–information search) results in differing attitudes toward web sites. Results suggest that web developers must tailor interface to be culturally relevant.
Choe (2004)	Survey of Korean and Australian firms Hofstede's culture indices	Use of Advanced Manufacturing Technology (AMT), type of information	Production performance *National culture (IC, UA, PD, MF, CD)*	Under a high level of AMT, the positive effects of AMT and information (nonfinancial performance and advanced cost-control information) on the improvement of production performance is greater in Korean than in Australian firms.
Chow, Deng, and Ho (2000)	Multimethod (interviews and surveys) study collecting data from U.S. and Chinese managers • Hofstede's cultural indices and Chinese Cultural Connection (Bond 1987)	Nature of knowledge, knowledge recipients relationship with knowledge sharer	Employee's propensity to share knowledge with coworkers *National culture (collectivism, CD, concern with face)*	Chinese professionals are much less willing to share knowledge with out-group members (e.g., those not part of the immediate social group) than U.S. counterparts. With knowledge sharing that involves a trade-off between self and collective interests, Chinese respondents are more likely to share knowledge since this is consistent with their collectivistic value system.
Chung and Adams (1997)	Comparative survey of U.S. and Korean business firms • Hofstede's cultural Indices	Group decision-making characteristics	Group decision-making process and outcomes (success) *National Culture (IC, PD, UA, MF)*	Comparison of respondents from significantly different national cultures (Korea and U.S.) resulted in no significant differences in group decision-making behaviors attributable to Hofstede's four dimensions of culture.
Downing, Gallaugher, and Segars (2003)	Interpretive field study of Japanese and U.S. organizations • Hofstede's culture indices	National culture (IC, UA, PD, MF)	Choice of IT for employee empowerment	Japanese companies (high uncertainty avoidance and collectivist) tend to select more information-rich, socially present forms of media (face-to-face, fax, and phone) to facilitate empowerment whereas U.S. companies (low uncertainty avoidance and individualistic) tend to select more lean (efficient) forms of electronic media (e-mail, groupware, intranets) to facilitate empowerment.
Gamble and Gibson (1999)	Qualitative study of 18 Hong Kong hotel managers and respective financial controllers • Culture measured through	Executive values (Confucian vs. Protestant values)	Transmission of financial information	Chinese controllers tended to distort (e.g., cover up or hide bad performance numbers) information to maintain harmony in relationships and loyalty to their managers. Implication: cultural values may influence the "objective outputs" of information systems.

	discourse analysis			
Leidner et al. (1999)	Survey of Swedish and Mexican senior managers • Hofstede's cultural indices	Executive information (EIS) system use	Senior management perceptions of EIS use outcomes *National culture (IC, UA, PD, MF, TO, CC)*	Survey found significant differences (as predicted by national cultural factors) in the impact of EIS use on senior management perceptions of EIS use outcomes. For example, Mexican managers perceived faster decision-making speed with EIS use, whereas Swedish managers did not. Overall, these findings suggest that EIS may be best suited in countries with low to moderate uncertainty avoidance and power distance values.
Rose, Evaristo, and Straub (2003)	Matching lab experiment • Hall's indices of polychronic vs. monochronic cultures	Web-site download delay	Attitude toward (web-site) download delays *National culture (poly vs. mono)*	Subjects from polychromic cultures (Egypt and Peru) were significantly less concerned with website download delays than subjects in monochromic (U.S. and Finland) cultures.

Layers of Culture

Based on the above definitions, Karahanna et al. (2006) argued establishing a precise definition of culture remains contentious due to lack of its understandability at different levels, ranging from individual to the national level. Hofstede (1980a) argued that several layers of cultural programming exist, which encompass the range of cultures operative on an individual's behavior. Hofstede and Hofstede (2005) described culture as an onion that can be peeled, layer by layer, to reach the core.

According to Hofstede, the outer layer represents symbols such as words, colors and the behavior of others that may have special meaning; the second layer represents heroes who are example of admiration and can be representative of model behavior; the third layer represents rituals; and finally, the fourth layer represents social values such as respect and greetings between people. Similarly, Karahanna et al. (2006) created five levels of culture in the information systems realm. Those five levels of culture included supranational, national, professional, organizational, and group-level cultures. Supranational is defined as any cultural differences that cross national boundaries or can be seen to exist in more than one nation. National is considered collective properties that are ascribed to the citizens of countries (Hofstede, 1984). Professional focuses on the distinction between loyalties to the employer organization versus loyalty to the industry (Gouldner, 1957). Organizational is considered to

be the social and normative glue that holds organizations together (Siehl, Martin, & Schneider, 1990).

Cultural Models

Many models study culture. Each of those models examines culture with a different viewpoint and uses its scope and variables to identify culture characteristics. The models of Hofstede (1980a), Schwartz (1994), and Hall (1973) are well-cited and widely accepted models in cross-cultural studies. Selecting an appropriate model to use for this study is imperative as each cultural model uses its scope and variables to identify cultural characteristics and organize data accordingly. By reviewing the research questions and aims of the study in terms of the cultural model's objective (e.g., examining it at an individual, organizational or national level), one can decide to pick an appropriate model of interest.

For this research study, Hofstede's (1980a) cultural model is selected for two reasons:

- The aim of the study: This study aims to examine the impact of culture on an individual level and organizational level rather than the cross-national level. Hofstede and Hofstede (2005) argued that the dimensions of national culture they propose could be examined at different levels ranging from the national level through the professional and organizational levels to the group level. Despite the fact that Hofstede's (1980a) cultural model only represents differences at a national level, it is still best suited and more relevant compared with the other models.
- Broad acceptance of Hofstede's dimensions: in the last two decades, Hofstede's (1980a) cross-cultural research and dimensions gained an extensive and wide-ranging audience across the diverse research context. Therefore, the results obtained using Hofstede's cultural dimensions for the present study will be more comfortable and more reliable to generalized from compared with other cultural theories and models.
- Hofstede's framework has been widely used in the Information Systems literature.

Hofstede's Cultural Model

While working for IBM from 1967 to 1973, Hofstede (1980b) conducted a very large-scale survey called the "value survey module" (VSM). The questionnaires were prepared in English and then translated into other languages as needed. Sixty-six questions were measuring the psychological characteristics of people from different cultural groups working for IBM. Specifically, 44 questions were related to personal goals and beliefs; 14 questions were related to awareness of the work environment, one to satisfaction, and the rest were related to demographic characteristics. Hofstede distributed 116,000 questionnaires in 50 countries around the world and received 60,000 responses. From the data collected and analyzed, Hofstede found that 32 questions were loaded into four dimensions of factor analysis with the representation of 40 countries' mean scores. Based on the results, Hofstede argued that differentiation between cultures should be based on four dimensions: Power Distance (PD), Individualism/Collectivism (IC), Uncertainty Avoidance (UA), and Masculinity/Femininity (MAS).

Below are explanations of each variable of Hofstede's framework Hofstede (1980b):

- Power distance: This refers to the extent to which individuals expect and accept differences in power between different people; in other words, it reflects the attitudes to authority and power.
- Individualism/Collectivism: This refers to the extent to which individuals are integrated into groups. In other words, Individualism is defined as a situation in which people are supposed to look after themselves and their immediate family only. In contrast, Collectivism can be described as a situation where people who belong to the same group should look after each other for loyalty. This can be considered as reflecting attitudes toward group membership.
- Masculinity/Femininity: This refers to the extent to which traditional gender roles are differentiated. In general, Masculinity refers to a situation where the dominant values in society are success, money, and other things, while in contrast, Femininity refers to a position which is a preference for relationships, caring for the weak, and quality of life.
- Uncertainty avoidance: This applies to the extent to which ambiguities and uncertainties are tolerated.

Hofstede's framework includes four constructs, which are discussed below.

Power Distance

Hofstede (1980b) argued that in countries that scored low on PD, employees are less dependent on their boss and colleagues. Therefore, employees have a greater sense of freedom, and everyone is free to express and share in the decision-making process. The management hierarchies in low-Power Distance countries are flatter and more open to questioning. Additionally, privileges for the senior ranks are undesirable, and superiors are expected to be accessible to subordinates. Hofstede (1980b) results have shown countries that score low on PD included Israel, Austria, Great Britain, USA, and Canada (13, 11, 35, 40, and 39, respectively).

On the other hand, Hofstede and Hofstede (2005) results have shown that in countries that scored high on this dimension, employees were more afraid of expressing disagreement with their higher-level manager or boss. Consequently, a vast emotional distance is established between subordinate and boss, which in turn creates situations in which subordinates entirely either obey their superiors' orders or, in the worst case, entirely reject them. One of the reasons for this emotional disparity is that people in higher-PD cultures are more comfortable with centralized power, and management and superiors are highly privileged and have the last say (Pavlou & Chai, 2002). Hofstede (1980b) results have shown countries that score higher on PD include Malaysia, Arab countries, Guatemala, and Slovakia (104, 80, 95, and 104, respectively).

Individualism and Collectivism

Hofstede (1980a) argued that individualist societies (I) are those societies in which the ties between individuals are loose: everyone is expected to look after himself or herself and his or her immediate family. He argued that collectivist societies (C) are those societies that are the opposite of Individualism societies in the fact that collectivist societies are those in which people from birth onward are integrated into strong, cohesive in-groups, which throughout people's lifetimes continues to protect them in exchange for unquestioning loyalty. Hofstede (1980b) argued that in the context of working goals, individualism is associated with personal time, freedom, and challenges, whereas collectivism is associated with training, physical conditions, and use of skills. Hofstede (1980b) results have shown that

in countries that score high on individualism, such as the US, Britain, and Canada (91, 89, and 80 respectively), people were more disposed toward self-orientation and self-motivation and were encouraged by their perceptions. Additionally, people in these countries were working for their interests and gave less/no importance to the organization's interests (Hofstede, 1984).

McCoy et al. (2007) reported that people with an individualist nature always make their decisions according to their own choice and are less or not affected by others' suggestions and considerations. On the other hand, in countries that scored lower on individualism, such as Pakistan, Arab countries, and Guatemala (14, 38, and 6 respectively), people gave a higher interest to groups or organizations compared to their personal beliefs (Hofstede, 1984). In these societies, decisions are not made on an individual basis but are likely to be considered with the sharing and helping of colleagues (McCoy et al., 2007).

Masculinity and Femininity

Hofstede (2005) differentiated masculinity and femininity (MAS) as separate from the gender trait (male or female) based on work goals and quality of life. Hofstede (1980a) considered masculine values to reflect more assertiveness and material success as opposed to feminine values, which give more emphasis to the quality of life goals, nurturing, and modesty. Hofstede (1980a) defined working goals as an emphasis on earnings, recognition, advancement, challenge, greater work centrality, and achievements defined in terms of wealth. In contrast, he explained the quality of life as placing a greater focus on cooperation, employment security, a friendly atmosphere, an environment where work is less central, and finally, achievements as defined in terms of human contacts. According to Hofstede (1980a), the first set of values is related to masculine individuals, whereas the second is related to feminine individuals.

Hofstede (1980b) found that countries like Japan, Austria, and Mexico scored higher on the MAS index (95, 79, and 69 respectively), and men were mostly found to be more assertive, robust and materialistic at work, while women were found to be modest, tender and concerned with the quality of life. Hofstede found that countries like Sweden, Norway, and the Netherlands scored lower on the MAS index (5, 8, and 14 respectively), and both men and women were modest, tender, and concerned with the quality of life. Interestingly, he found that most of the South Asian countries like Pakistan, India, and Arab had a modest level of masculinity (50, 56, and 35 respectively) where people learn how to avoid aggression rather

than how to defend against it. Hofstede (1984) argued that societies that scored high on masculinity were usually marked by families who encouraged their children toward competition in societies, while in feminine societies, families train their younger generations in modesty and solidarity.

Uncertainty Avoidance

Hofstede (1980a) argued that in strong uncertainty avoidance cultures, individuals usually feel threatened by unknown or uncertain situations (Srite & Karahanna, 2006). Consequently, to reduce the level of uncertainty in these cultures, individuals tend to rely on specific rules and favor more stability at work and in their lives in general (Parboteeah, Bronson, & Cullen, 2005). In cultures that are high on UA, employees working in organizations never consider breaking company rules even if they know that doing this would be in the firm's best interest (McCoy et al., 2007). Hofstede (1980a) related UA with an individual level of risk tolerance and stated that within cultures that are high on UA, individuals possess less tolerance compared with cultures low on UA.

On the contrary, within cultures low on UA, individuals have higher levels of tolerance, experimentation, and/or innovative behavior; consequently, they are more open to taking risks. Additionally, he argued that feelings of uncertainty are not developed personally by individuals; however, they are also partially shared by the other members of society. In the workplace, job stress, and anxiety (the state of being worried about what may happen) were the main reasons for the creation of a higher UA culture. Hofstede (1980b) found that countries like Greece, Portugal, and Japan scored high on UA (112, 104, and 92 respectively), and people in these cultures were mostly psychologically characterized by a higher tendency to stay with the same employer, display higher average seniority in jobs, and show higher loyalty to the organization. On the other hand, in countries like Singapore, Sweden, and China, which scored low on UA (8, 29, and 30 respectively), most people had less anxiety about future policies and outcomes, and less aggression and emotions were displayed. Finally, countries like Pakistan, Taiwan, and Arab Nations were found to have a medium to a high level of UA (70, 69 and 68 respectively).

Hofstede's Cultural Model Results

During the analysis, Hofstede and Hofstede (2005) found that PD and IC shared points of similarities between the indexes scores culturally allocated to each country. By plotting a graph, the x-axis represents the PD index from small to large, and the y-axis represents the IC from low to high. Hofstede found that countries, which scored high on the PD index, were scored low on IC in the quadrant. On the other hand, countries with low PD were primarily found to be high on individualism in the quadrant. Hofstede and Hofstede (2005) reported this relationship with caution in that two dimensions of culture, PD, and IC, are negatively correlated, so that large- PD countries are likely to be more collectivist, and small-PD countries are more likely to be individualist on cultural indices.

Despite the fact that the dimensions of masculinity and femininity are independent of gender traits, and both men and women can acquire a masculine/feminine nature (Hofstede, 1980a), the literature suggests that men mostly have a masculine nature while women have a feminine nature (e.g., Bem, 1981; Hofstede, 2005; Venkatesh et al., 2004). For instance, Bem (1981) in the Sex-Role Inventory (BSRI), during an examination of the psychological characteristics of men and women, found that men displayed more masculine traits compared with women who exhibited more feminine features. Gender and age are also considered to be part of the masculine dimension (Venkatesh et al., 2004; Hofstede, 2005). Hofstede (1980) found during an examination of cultural dimensions, a higher ratio of men compared to women in countries, which scored higher on the masculine index. Similarly, Hofstede found that an early age people were more focused on career development (a characteristic of masculinity), but as they grew older, they tended to exhibit more social and less ego-oriented (i.e., characteristic of femininity) behavior. Hofstede (2005) argued that, particularly in masculine societies, mostly men are dominant and are pushed by society to work, while in feminine societies, both men and women are socialized to be ambitious.

Hofstede (2005) plotted a graph between the MAS and IC indices, and the MAS and PD indices to the interrelated effect of one dimension with another. From the masculinity and individualism results, he found that countries, which scored higher on the MAS index, were in the quadrant with a higher value of IC. Similarly, within the masculine and power distance plot, countries, which scored higher on the MAS index, were found in the quadrant with a

lower value of PD. From these two graphs, Hofstede argued that cultures, which are mostly higher on MAS, also tend to be higher on IC and PD.

Hofstede (2005) analyzed the interrelated effects of masculinity and UA dimensions. By plotting a graph where the x-axis represents MAS from low to high, and the y-axis represents UA from high to low, he found that countries, which scored higher on the MAS index, were located in a quadrant with lower UA values. On the other hand, countries that scored low on MAS were found in the quadrant with low UA.

CHAPTER 3

CONCEPTUAL FRAMEWORK

Theoretical Background

The previous chapters have presented a review of the models and theories used in explaining behaviors related to the acceptance and adoption of Information Systems. Also, this research identified a set of factors that fall in different domains, such as personal, social, behavioral, cultural, and technological, that might affect the effective use of security awareness programs in organizations in the Democratic Republic of Congo.

The development of the proposed model presents the influence of independent variables on the value of dependent variables and help hypothesize and test the relationships between the identified constructs, thereby verifying if the theorized model is valid or not. With the knowledge that prior models in the realm of acceptance and adoptions of Information Systems had limitations, the appropriate approach for this study was to select only those constructs deemed relevant in the context from the models reviewed in the previous chapter.

This study's framework used the technology acceptance model (TAM) as the foundation for the theoretical model of the study. Through the years and in multiple studies, TAM has demonstrated that perceived ease of use influences perceived usefulness and, in turn, both beliefs influence behavioral intention to use a specific system. Selecting TAM as the foundational model is due to consistent explanatory power since its creation and its popularity among social sciences researchers (e.g., Venkatesh and Bala, 2008; Venkatesh and Davis, 2000). By adopting TAM as the foundational model, perceived usefulness (PU), behavioral intention (BI), and behavioral usage (BU) are incorporated into the conceptualization model. This study recognizes that TAM is not without flaws, as pointed out by previous literature (F. D. Davis & Venkatesh, 1996; Mathieson, 1991; Taylor & Todd, 1995a). TAM did not incorporate the effect of the social environment on behavioral intention. Cooper et al. (Cooper, Wang, Bartram, & Cooke, 2019) argued that shared perceptions

provide powerful cues for individuals regarding appropriate and desired behavior, in addition to performance expectations, within a contextual setting. Shared perceptions can be linked to culture; therefore, it can be inferred that technology adoption depends on an individual's attitudes, beliefs, and behavior, which are influenced by their cultural environment. Based on TAM and TAM2's limitation to examine the direct effect of situational and social conditions on acceptance intention, the normative beliefs of peer-influence is incorporated from TRA, and control and self-efficacy (SE) are included from DTPB. None of the previously cited models explicitly conceptualized the importance of social influence on acceptance behavior. Therefore, using a similar conceptualization of UTAUT in terms of social influence effect on BI, the impact of management support is incorporated in the model.

Researchers (Jackson, 2011; Kacen & Lee, 2002; Kummer, Leimeister, & Bick, 2012; Turró, Urbano, & Peris-Ortiz, 2014; Venkatesh & Zhang, 2010) have previously demonstrated that cultural values can influence the needs and motives for using a product, and attitude toward purchasing and using products. Following this line of thought, this study suggests that culture, as proposed in our model, influences the effective use of security awareness. Also, the model incorporates the information quality (Strong, Lee, and Wang 1997a) to explore the effect of cultural factors on individuals' effective use behavior.

The research model presented in Figure 5 integrates cultural values into an extended version of TAM to illustrate their impact on the effective use of security awareness.

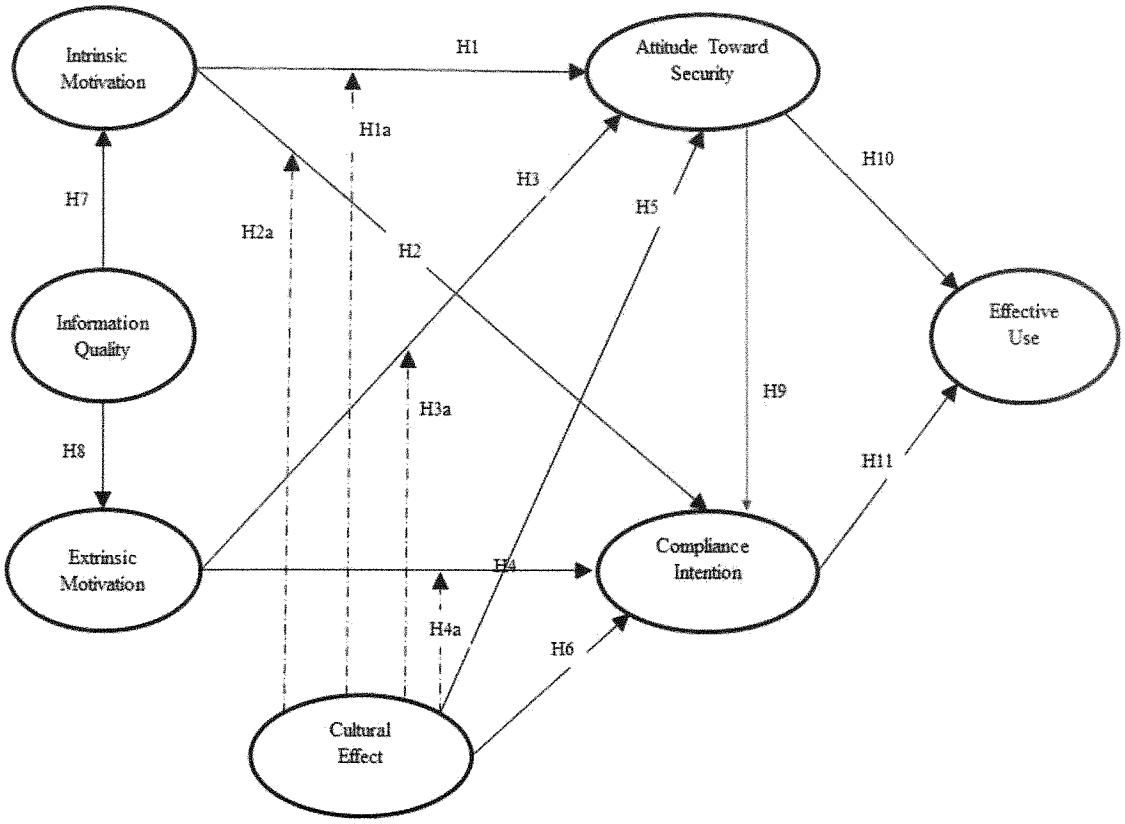

Figure 5. Research Model

Research Model and Hypotheses

Our research model integrates the determinants from TRA (Fishbein & Ajzen, 1975), TAM (Davis, 1989), and TPB (Ajzen, 1988). Also, the model incorporates the theory on information quality (Strong, Lee, and Wang 1997a), and the cultural theory of Hofstede (1980), to explore the effect of cultural factors on individuals' acceptance behavior, compliance intention and effective use of security awareness guidelines. The hypothetical relationships proposed can be seen in Figure 5 above.

Intrinsic and Extrinsic Motivation

Intrinsic motivation refers to feelings associated with an action. In contrast, extrinsic motivations come from peer pressure and interactions with others in a group, the physical environment, or how the culture of an organization rewards and punishes certain activities (Grenny, Patterson, Maxfield, McMillan, & Switzler, 2013).

From an intrinsic motivational (IM) perspective, employee behaviors arise from the employee's need to feel competent and self-determined in dealing with their working environment (E. Deci & Ryan, 1985; E. L. Deci & Ryan, 1975; Ryan & Deci, 2000).

Researchers have found that employees with high confidence in their ability to provide a valuable contribution are more likely to accomplish specific tasks (Bock & Kim, 2002; Constant, Kiesler, & Sproull, 1994). For this study, the intrinsic motivation variable comprises self-efficacy, perceived usefulness, and perceived value. Self-efficacy is typically manifested in people believing that their knowledge can help to solve job-related problems and improve work efficacy (Constant, Sproull, & Kiesler, 1996; Luthans, 2002). Perceived usefulness is considered to be the degree to which a person believes that using a particular system would enhance their job performance (Cook, Heath, & Thompson, 2000). Finally, perceived value refers to the overall evaluation of the change related to a new information system implementation, based on the comparison of benefits and costs (Kim, Chan, & Gupta, 2007; Kim & Kankanhalli, 2009).

While numerous empirical studies of technology acceptance and implementation focus on situations in which individuals have some discretion in adopting such technology, this study focuses on the mandatory aspect of adoption. This is because information security compliance in highly regulated industries, such as banking and telecommunications, are not voluntary. Boss, Kirsch, Angermeier, Shingler, and Boss (2009) found that the acts of specifying policies and evaluating behaviors are effective at convincing individuals that security policies are mandatory. The perception of obligation is effective in motivating individuals to take security precautions; when these individuals believe that the management is watching, they will comply. Based on the above, this study removes ease of use from this extended version of TAM, as the study was conducted in organizations in which compliance with security guidelines is mandatory. In this situation, individuals do not have a choice of whether to comply, even if the security requirements are not easy to use.

This study posits that employees who have a positive perception of their organizations' security awareness program and who believe that they can contribute to their organizations' performance by effectively using the program. This will develop a more positive attitude and intention to comply with the security requirements of their organization. Hence, the following hypotheses are proposed.

H1: Intrinsic motivation positively influences employees' attitudes toward the security awareness program.

H2: Intrinsic motivation positively influences employees' intentions to comply with the security awareness program.

From the perspective of extrinsic motivation (EM), employee behaviors are motivated by external variables that are independent of the content of the activity itself (Ko, 2005). For this study, the EM variable is composed of top management support, sanction, reward, and social pressure. Top management support is defined as the enthusiasm, support, personal involvement, and overall leadership offered by senior management concerning a specific activity (Karimi, Somers, & Bhattacherjee, 2007). A reward is defined as the tangible or intangible compensation that an organization gives to an employee in return for compliance with the requirements of the information security policy (Bulgurcu, Cavusoglu, & Banbasat, 2010). Sanction is defined as the tangible or intangible penalties—such as demotion, loss of reputation, reprimand, monetary or nonmonetary penalties, and an unfavorable personal mention in oral or written assessment reports—incurred by an employee for noncompliance with the requirements of the information security policy (Bulgurcu, Cavusoglu, & Banbasat, 2010). Social pressure is defined as the social pressure perceived by an employee regarding compliance with the requirements of the information security policy, caused by the behavioral expectations of such important referents as executives, colleagues, and managers (Bulgurcu, Cavusoglu, & Banbasat, 2010).

This study proposes that employees who have a positive perception of the external motivation factors—that is, management support for the security awareness program, organizational reward for complying with security guidelines, proportional sanction when an employee fails to comply with policy, and positive social pressure from colleagues—will develop a more positive attitude and intention to comply with the security requirements of their organizations. Hence, the following hypotheses are proposed:

H3: Extrinsic motivation positively influences employees' attitudes toward the security awareness program.

H4: Extrinsic motivation positively influences employees' intentions to comply with the security awareness program.

Cultural Effect

Srite and Karahanna (Srite & Karahanna, 2006) found that the effect of culture on individuals depends on the degree to which an individual is willing to become involved and engage with the values of their own culture. Their scales were found to have adequate psychometric properties and were successfully integrated with a model derived from TAM. This paper follows the same approach and measures culture at the individual level, thus enabling the moderating effects of culture within the developed model.

The general prediction is that users with higher PD values are more likely to be dependent on referent power in decision-making; that is, they would be more influenced by the views of others, particularly their superiors, in deciding whether to adopt technologies. Dinev et al. (Dinev, Goo, Hu, & Nam, 2009) compared samples from South Korea and the USA in the context of adopting protective (e.g. anti-virus) software and found that the relationship between SN and BI was significant for the South Korean sample (which had a high-PD culture) but not for the USA sample (low-PD culture). Like South Korea, the DRC is considered a high-PD culture, which can be seen in the hierarchical structure of its society.

A high-masculinity culture emphasizes work goals, while a low-masculinity culture encourages people to follow traditional standards that are more people-oriented than those with high masculinity values. A high-femininity culture is expected to be more influenced by interpersonal contact, while a high-masculinity culture would be expected to be more influenced by features that encourage the achievement of work goals. Srite and Karahanna (Srite & Karahanna, 2006) found the opposite effect, with a significant effect of PU on BI for a USA sample (which is a more feminine culture) but no significant effect for a Chinese sample (a more masculine culture). The DRC was initially considered a low-masculinity culture where people cared for the wellbeing of their neighbors. However, the DRC has been through two decades of internal civil war that may have changed its original position.

Srite and Karahanna (Srite & Karahanna, 2006) and Dinev et al. (Dinev et al., 2009) supported the prediction that subjective norms such as social pressure have more influence in

a high-UA context than in a low-UA context. While great uncertainty is a part of everyday life in the DRC, the people of the DRC are characterized as being high UA.

In individualistic societies, individuals focus on their achievements and personal goals rather than the group to which they belong. In collectivistic societies, people prefer loyalty and group success to their gain. Numerous researchers (Dinev et al., 2009) have proved the relationship between SN and BI to be stronger in collectivist cultures than in individualistic cultures. Srite (Srite & Karahanna, 2006) found that while SN was a significant predictor of BI in a Chinese sample (which is a collectivist culture), there was no significant effect of SN on BI in the USA (an individualistic culture). The DRC is considered to be a collectivist society where decisions are made by families, clans, and tribes. Based on the discussion above, we postulate the following hypotheses:

H5: The cultural effect influences employees' attitudes toward the security awareness program.

H6: The cultural effect influences employees' intentions to comply with the security awareness program.

H1a: The cultural effect moderates the relationship between intrinsic motivation and employees' attitudes toward the security awareness program.

H2a: The cultural effect moderates the relationship between intrinsic motivation and employees' intentions to comply with the security awareness program.

H3a: The cultural effect moderates the relationship between extrinsic motivation and employees' attitudes toward the security awareness program.

H4a: The cultural effect moderates the relationship between extrinsic motivation and employees' intentions to comply with the security awareness program.

Information Quality

Pahnila, Siponen, and Mahmood (2007b) developed a theoretical model that combines GDT, PMT, TRA, Information Systems Success, and Triandis's Behavioral Framework and Rewards. Based on a sample of 245, the study found that information quality has a substantial effect on actual compliance with information security policy. In our context, information

quality refers to the relevancy, clarity, and accessibility of the security awareness program materials. Prior research by Delone and McLean (2003) on information quality qualified it as a critical determinant for identifying the factors which may affect the success of information systems. DeLone and McLean have identified five other information success features: system quality, use, user satisfaction, individual impact, and organizational impact. Previous research has developed numerous measures of information quality and identified various constructs. Larcker and Lessig (1980) introduced the notion of the perceived importance of information and the perceived usefulness of the information. Perceived importance of information refers to factors related to relevance, meaningfulness, importance, helpfulness, and significance of the information presented. Perceived usefulness of information refers to the factors associated with things such as unambiguity, clarity, and readability. Lee, Strong, Kahn, and Wang (2002) mapped sixteen different dimensions of information quality, accessibility, completeness, and timeliness to four descriptive quadrants: sound, dependable, useful, and usable. Dee Dickerson and Gentry (1983) have argued that innovation with substantial complexity requires more technical skills and needs more significant implementation and operational efforts to decrease its chances of adoption. Thus, this study expects that if employees believe information provided by the security awareness program to be complete, accurate, and easy to apply, they will develop more positive attitudes toward the security awareness program of their organization. Hence, the following hypothesis is proposed:

H7: Information quality positively influences employees' intrinsic motivation.
H8: Information quality is positively associated with employees' extrinsic motivation.

Attitude toward Security

The association between attitude and behavioral intentions has been considered in previous studies (Venkatesh et al., 2003), which have shown that attitude toward complying with acceptable information system behaviors positively influences behavioral intentions (Bulgurcu, Cavusoglu, & Benbasat, 2010; Herath & Rao, 2009; Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009; Pahnila, Siponen, & Mahmood, 2007a; Pahnila et al., 2007b; M. Siponen, Mahmood, & Pahnila, 2014). Davis, Bagozzi, and Warshaw (F. D. Davis et al.,

1989) used the TAM to explain why a user accepts or rejects information technology. The TAM provides an understanding with which researchers can explain how external variables influence belief, attitude, and intention to use. According to the TAM, people's actual use of the technology system is influenced directly or indirectly by the user's behavioral intentions, attitude, perceived usefulness of the system, and perceived ease of use the system. Furthermore, attitude toward moral behavior has been investigated by Chang (Chang, 1998), who found that it significantly influences behavioral intentions. The TPB aims to explain all behaviors over which people can exert self-control. The model is based on behavioral intent, whereby behavioral achievement depends on both motivation (intention) and ability (behavioral control). Attitude has proven to be a significant predictor of employee behavioral intentions. In this study, attitude toward security refers to positive or negative evaluations of the security awareness program by an employee. Attitude refers to the degree to which a person has a favorable or unfavorable evaluation of the behavior of interest. This entails consideration of the outcomes of performing the behavior. Based on the above assertions regarding employee attitude toward security and behavioral intentions, the following hypotheses are proposed:

H9: Attitude toward security program positively influences employees' intentions to comply with the security awareness program.
H10: Attitude toward security program positively influences employees' effective use of the security awareness program.

Compliance Intention

Numerous studies have incorporated the subjective norm (SN) and found that it has a significant effect on intention in mandatory settings, but not involuntary ones (Hartwick & Barki, 1994; Venkatesh & Bala, 2008). Venkatesh, Brown, Maruping, and Bala (Venkatesh & Bala, 2008) found that the effect of SN on behavioral intention was stronger in a mandatory setting and that SN was a significant determinant of PU. In the context of information security, SN has been identified as a significant predictor of behavioral intention to comply with or use protective security measures (C. L. Anderson & Agarwal, 2010; Bulgurcu,

Cavusoglu, & Benbasat, 2010; Dinev & Hu, 2007). In this study, compliance with the security awareness program refers to the mandatory obligation of employees to adhere to the security requirements of their organization. Behavioral intention refers to the motivational factors that influence a given behavior, where the stronger the intention to perform the behavior, the more likely the behavior will be performed. Based on the above assertions regarding employee compliance with the security awareness program, the following hypotheses are proposed:

H11: Intention to comply with security guidelines positively influences employees' behavior toward effective use of the security awareness program.

CHAPTER 4

RESEARCH METHODOLOGY

Background

This chapter describes and justifies the philosophical approach, methods, and techniques used in this research to achieve the primary research objectives and to answer the research questions. This study uses a quantitative method to understand and validate the conceptual framework. A survey research approach based on positivism was employed to guide the research. A questionnaire was used as a data collection technique. Additionally, Structural Equation Modelling (SEM) using Smart-PLS was used as a data analysis technique.

Setting, Subjects and Data collection

The Congolese government has recognized that small and medium organizations are an integral part of the nation's critical infrastructure. These critical infrastructure systems are vulnerable to a variety of threats from accidents, naïve adversaries, and sophisticated adversaries. These critical infrastructures can be manipulated to influence decision-makers, the economy, and the will of the general population.

Critical infrastructure institutions are highly regulated and continuously supervised by the government to ensure that they can withstand the various and increasing threats they face. Critical infrastructure institutions, of all sizes, are required to comply with different laws and regulations. Large institutions, which typically hold billions in financial assets, have different abilities and needs compared to smaller institutions that usually hold millions in financial assets. However, both types of institution sizes have the same threats, regulations, and requirements as critical national infrastructure.

To test our hypotheses, the positivist epistemology and ontology were selected; therefore, the selection of a quantitative research strategy for this study. This research adopted a survey approach for data collection. The data collection was conducted in one bank and one Telecommunication Company in the Democratic Republic of Congo. The subjects of the

study are individuals employed in the selected organizations. The survey was administered using SurveyMonkey. No restriction was placed on who in the two organizations was to take the survey. Given that English is a second language in Congo, the additional step of translating the survey in French was made, therefore giving people the choice of language (English or French).

Positivism Paradigm for our research

The positivist approach was selected after considering the differences between all the other three underlying approaches and the nature of our study. Below are the key motivator for choosing this approach:

- In the adoption and technology acceptance research, it was noted that the positivist approach was dominant among the other three approaches, with more than 75% research using this last (Mingers, 2003).
- The current research aims to investigate the effective use of security awareness programs in small and medium-sized businesses while being moderated by the effect of culture. This research is related to social subjects where employee behavior is measured and where the researcher is isolated from the aim of the study (Saunders, Lewis, Thornhill, & Wilson, 2009). Therefore, the positivist approach was justifiable from the ontological point of view.
- This research suggests several hypothesized relationships be tested and quantitatively measured. The positivist approach is mostly linked with quantitative methodology, which in turn uses a deductive process (Alan Bryman, Becker, & Sempik, 2008). Therefore, this research is also justified from the methodological point of view.

Survey Research Approach

For the current research, we employed the survey approach to collect data from the participants in both a bank and a telecom company for the following reasons:

- Mingers (2003) investigated the research approaches in IS and found that more than 74% of the articles employed the survey approach in information systems

journals in North America as it relates to the technology adoption, and only the remaining 26% used the case study method. For example, Venkatesh and Davis (2000), Venkatesh and Morris (2000), Srite and Karahanna (2006), and Venkatesh and Bala (2008). Therefore, we selected the survey approach as it has been the most widely considered within technology adoption research.

- The survey approach was associated with research using positivist-quantitative methodologies (Saunders et al., 2009).

Within the survey research approach, data collection is often performed through several methods such as mail, telephone interviews, email, and self-administrated questionnaires. This research employed the self-administrated web questionnaire as a data collection method for the following reasons:

- Data can be collected from a large number of participants simultaneously in a quick, easy, efficient, and economical way compared with other methods such as interviews (Alan Bryman et al., 2008; Sekaran & Bougie, 2011).
- It is effectively designed and administrated. For example, interviews usually require many administrative skills (Sekaran & Bougie, 2011).
- The Web questionnaire provided more privacy for respondents since the questionnaire was anonymous, and issues such as anonymity and confidentiality were dealt with in the cover letter.
- Collecting the questionnaires immediately after being completed will assure a higher response rate (Sekaran & Bougie, 2011).
- Respondents can seek clarity and, therefore, can understand the concepts on any question they are answering, which in turn, minimizes the outliers in the study (Aaker, 2009).
- A questionnaire as a data collection method has been widely used in studies similar to the context of this study. For example, Venkatesh and Morris (2000), Venkatesh and Bala (2008), and Srite and Karahanna (2006).

Research Design

A research design is of critical importance as it links the theory and the empirical data collected to answer the research questions. A Bryman and Bell (2011) argued that it provides overall guidance and a framework for the data collection, sampling techniques, and analysis of the study. Therefore, it is imperative that a researcher select the appropriate research design as this last will influence the use and type of data collection, sampling techniques, and the budget (Hair, Ringle, & Sarstedt, 2011).

From guidance about research design provided by Sekaran and Bougie (2011), the current study was to test the hypotheses generated from the conceptual model. The relationships that exist among variables can be easily understood through hypothesis testing, as such studies usually explain the nature of individual relationships among variables. A correlational type of study was selected over a casual type to delineate the variables that are associated with the research objectives and examine the relationships between the determinants of an individual's behavior within a non-western nation. As such, this research was conducted in a non-contrived setting. Since the data collection method used in this study was based on a survey, there was no intervention from the researcher. As previously mentioned, the unit of analysis is an individual employee within the bank and the telecommunication company selected for the study.

Population and Sampling

Prior to the data collection process, this research ensured that the appropriate sampling technique was used. Bryman and Bell (2011) argued that researchers must consider the sampling technique to be a critical concern to their research to represent the targeted population and to eliminate the bias in the data collection methods. Fowler Jr and Cosenza (2009) argued that there are four critical issues to be considered when designing the sample as follows: (1) the choice of probability or non-probability sample technique; (2) the sample frame; (3) the size of the sample; and (4) the response rate. The table below describes each sampling method within each sampling technique.

Table 4. A Classification of Sampling Techniques.

A Classification of Sampling Techniques		
Sampling Technique	1. Probability Sampling Techniques	(1) Simple Random Sampling (2) Systematic Sampling (3) Stratified Sampling (4) Cluster Sampling (5) Other Probability Sampling Techniques
	2. Non-probability Sampling Techniques	(1) Convenience Sampling (2) Judgmental Sampling (3) Quota Sampling (4) Snowball Sampling

Source: Groves et al. (2009)

For this research, the non-probability sampling techniques and convenience sampling method were selected. The convenience sampling method was selected because it allows the researcher to select the sample subjects from the targeted population based on who is willing and easily accessible to be recruited and included in the research. Additionally, Stangor (2014) argued the convenience sampling method is the most commonly used in behavioral and social science studies. This method is also considered to be the least expensive and least time-consuming among all techniques.

The time and budget constraints led to the decision to employ the non-random approach with the potential to collect the sample sizes needed for the analysis. The targeted population is employees in the two-selected organizations with implemented information security programs in the Democratic Republic of Congo.

Sample Size

Roscoe (1975) suggested the following rules should be applied when considering a sample size:

- The sample size should be superior to 30 and less than 500 to be considered appropriate for most research,
- A minimum sample size of 30 is required within each category when categorizing the sample into sub-groups, and
- The sample size should exceed by several times (preferably ten times) the number of variables within the proposed framework or study. In line with the above suggestions and considering the complexity of the proposed model in terms of variables and ratio of respondents (estimation of approximately 20 parameters), the sample size required should be at least 200.

Non-response Bias

The sample is intended to be representative of the entire population, and thus, consistent with Saunders et al. (2009), a relatively high response rate to acquire a large sample will increase the level of confidence and decrease the bias from the collected data. Based on the pre-test and pilot study results of the questionnaire, a high response rate was acquired with also a high satisfaction rating about the length, clarity of wording, and layout of the self-administrated survey. Therefore, this will also help to reduce the bias in the research. Additionally, a case deletion is performed with all the biased questions in this study.

Survey Design and Development

A web-based survey was developed to collect the data required to answer the research questions. The survey items were mainly obtained from reviewing the literature about technology acceptance models, culture and effective use outlined in Chapter 2, and were more accurately based on the conceptual framework and the research hypotheses outlined in Chapter 3.

To ensure that there were neither vague nor confusing questions and keeping in mind the primary objective of the research, the questionnaire design took a long time to finalize. The questionnaire consisted of four pages, a consent form, and a cover letter. The purpose of the study was briefly explained to the respondents in the cover letter with other information, which indicates that their participation would be strictly confidential (see Appendix A).

Instrument Scale Measurement

This study developed a questionnaire technique incorporating nominal and ordinal scale (see Appendix A). Nominal scales were mainly used to determine the participants' demographic characteristics such as age, gender, educational level, and experience. Likert scales were used to measure the participants' beliefs and opinions toward the effective use of information security programs in their organizations. This scale was first developed by Rensis Likert (Likert, 1932) and provided a sequential point scale that varies by equal intervals. Participants indicated their agreement or disagreement with specific statements or questions related to their attitudes and beliefs using a 7-point Likert scales were used to allow varieties in the answers as participants in this study share many similarities in their characteristics. Also, this scale is widely used by many scholars in the IS and social science literature (Davis, 1989; Venkatesh and Davis, 2000; Dorfman and Howell, 1988).

Data Analysis

Exploratory data analysis included an examination of the pattern of missing data and the calculation of descriptive statistics. Because the security scales were being used with a new population, the principal component analysis was conducted when appropriate on each scale to determine the unidimensionality of the scale items. Partial least squares structural equation modeling (PLS-SEM) was used to evaluate the hypothesized model.

PLS-SEM was used instead of covariance-based structural equation modeling (CB-SEM) for three reasons. First, our objective is theory testing, and PLS-SEM is used for theory testing, while CB-SEM is used primarily for theory confirmation. Second, our hypothesized model is involved with eighteen latent variables, including three second-order constructs; PLS-SEM is used when the structural model is complex. Third, we did not want to make any assumptions about the distribution of scores on our indicator variables, and CB-SEM assumes that scores on the model variables are generally distributed while PLS-SEM does not assume normality.

Missing values were handled using mean replacement. A follow-up bootstrap procedure, which drew five thousand subsamples, was used to estimate bias-corrected and accelerated (BCA) confidence intervals for loadings, weights, and path coefficients. BCa

confidence intervals are confidence intervals that have been adjusted for potential bias and skewness of the bootstrap distribution. All significance tests were two-tailed, and the alpha level was set at 0.05. Both exploratory data analysis and the principal components analysis were conducted using SmartPLS 3 (Ringle, Wende, & Becker, 2015a).

CHAPTER 5

DATA ANALYSIS AND RESULTS

Partial least squares (PLS), as implemented in SmartPLS version 3.0, is used for data analysis (Ringle, Wende, & Becker, 2015b). The PLS approach allows researchers to assess measurement model parameters and structural path coefficients simultaneously. This study primarily aims to carry out causal-predictive analysis, and PLS is effective for those early theory testing situations.

Data Collection and Missing Data

The total number of surveys downloaded from the host server was 715. Of these, 494 were from the telecommunication company, and 221 surveys were from the bank. 215 surveys (30.07% of the original 715) were eliminated because they were missing answers to all or nearly all demographic and scale items. 122 of these were telecommunication surveys, and 43 were bank surveys. This left 500 surveys (322 from participants in telecommunications and 178 from participants in banking).

The 500 remaining participants had completed almost all of the demographic questions. However, 30.80% of participants (n = 154) had skipped one or more scales on the survey. The pattern of missing data was not random, for participants had not merely overlooked a survey item here or there. Participants either responded to all items on a scale, or they responded to none of the items. Table 4 lists the proportion of missing responses for each scale. Intent to Comply and Effective Use of Security Awareness was the scale most often skipped by participants. The only scale with no missing responses was self-efficacy.

Table 5. Scales on the security awareness survey with missing responses

Scale	Proportion of Missing Response
Intention to comply	0.31
Effective use of security awareness	0.31

Power distance	0.30
Uncertainty avoidance	0.30
Attitude toward security	0.30
Masculinity / femininity	0.29
Individualism / collectivism	0.28
Social pressure	0.27
Punishment	0.24
Reward	0.24
Management support	0.19
Information quality	0.11
Perceived value	0.07
Perceived usefulness	0.04
Self-efficacy	0.00

This pattern of missing data does not appear to be random, so it must be investigated in later study. We compared the demographic information of participants who completed the entire survey to the participants who skipped one or more scales. The two groups were significantly different on four of the ten demographic variables: age, $\chi 2(5) = 13.22$, $p = 0.02$; position within the organization, $\chi 2(3) = 13.09$, $p < 0.01$; the area of the company that participants worked in, $\chi 2(5) = 11.56$, $p = 0.04$; and the organization type (telecom or bank), $\chi 2(1) = 12.28$, $p < 0.001$. Tables 5, 6, 7, and 8 show the observed counts and expected counts for participants with no missing data compared to participants with missing data by age, a position with the organization, the area worked in, and the organization type, respectively.

Those who skipped one or more scales at higher rates than expected were in their 20s or 30s were employed in telecommunications and worked as staff in the front office. These participants may have skipped sections of the survey for a variety of reasons such as feeling less invested in the organization and its security, not being informed about the organization's security policy, or thinking that security was not significant in their jobs. These reasons and others will need to be explored in future research as it is beyond the scope of this research.

Table 6. The number of participants with no missing scales compared to the number of participants with missing scales by age. The expected counts are in parentheses.

Age	**Number of participants with no missing scales**	**Number of participants with missing scales**
18-20	2	0

	(1.38)	(.62)
21-29	45 (54.67)	34 (24.33)
30-39	154 (159.16)	76 (70.84)
40-49	104 (95.50)	34 (42.50)
50-59	37 (32.52)	10 (14.48)
60 or older	4 (2.77)	0 (1.23)

Table 7. The number of participants with no missing scales compared to the number of participants with missing scales by position within the organization. The expected counts are in parentheses.

Position within the organization	**Number of participants with no missing scales**	**Number of participants with missing scales**
Clerk / Staff	122 (137.71)	77 (61.29)
Supervisor	61 (58.13)	23 (25.87)
Manager	129 (123.18)	49 (54.82)
Executive / C-Level	34 (26.99)	5 (12.01)

Table 8. The number of participants with no missing scales compared to the number of participants with missing scales by the area where participants worked. The expected counts are in parentheses.

Area where participants worked	**Number of participants with no missing scales**	**Number of participants with missing scales**
Accounting / Finance	29 (32.45)	18 (14.55)

Customer Care	56 (64.90)	38 (29.10)
Operations	72 (66.28)	24 (29.72)
Compliance / Audit	20 (18.64)	7 (8.36)
IT	34 (38.66)	22 (17.34)
Other	128 (118.06)	43 (52.94)

Table 9. The number of participants with no missing scales compared to the number of participants with missing scales by type of organization. The expected counts are in parentheses.

Type of organization	**Number of participants with no missing scales**	**Number of participants with missing scales**
Bank	141 (123.18)	37 (54.82)
Telecommunications	205 (222.82)	117 (99.18)

Descriptive statistics

Even though the participants with no missing data differ from those with missing data, we feel it is essential to test the model with only completed surveys. Therefore, we excluded the 154 surveys with missing data, leaving 346 participants (and completed surveys) in our study. Although our sample is now less representative of the two organizations surveyed, we

do not feel that the sample is too biased to use in model testing. Table 9 displays the demographic information for participants included in the study.

Table 10. Demographics of participants included in the PLS-SEM analysis

Demographic	n	Demographic	n	Demographic	n
Organization Type		*Gender*		*Language*	
Bank	141	Male	272	French	310
Telecommunications	205	Female	74	English	36
Age		*Education level*		*Highest degree earned*	
18-20	2	No high school	1	Mathematics	10
21-29	45	degree	4	Science	9
30-39	154	High school degree	7	Healthcare	2
40-49	104	Some college	67	Medicine	51
50-59	37	Associate degree	219	Computing	27
60 or older	4	Bachelor degree	48	Engineering	39
		Graduate degree		Technology	117
				Business	12
				Other	79
Post high school education		*Time in current industry*		*Time worked abroad*	
				Not Applicable	283
In Congo	273	1-5 years	127	1-5 years	29
Abroad French Lang.	31	6-10 years	107	6-10 years	15
Abroad English Lang.	37	10-15 years	84	10-15 years	10
		16 or more years	28	16 or more years	9
Area worked in		*Position in company*			
Accounting / Finance	29	Clerk / Staff	122		
Customer Care	56	Supervisor	61		
Operations	72	Manager	129		
Compliance / Audit	20	Executive / C-Level	34		
IT	34				
Other	128				

For each statement on each of the scales, participants chose one of seven options: Strongly Disagree, Disagree, Slightly Disagree, Neutral, Slightly Agree, Agree, and Strongly Agree. For data analysis, this scale was converted to a seven-points numeric scale with 1 = Strongly Disagree, 2 = Disagree, and so on up to 7 = Strongly Agree. For each scale of the survey, participant's numeric responses were added to yield a total score for the scale.

The responses of participants from banking were similar to the responses of participants from telecommunications. The two groups were significantly different on only

three of the scales. The mean total score for Management Support was slightly higher for those in banking (M = 41.89, SD = 8.77) than for those in telecommunications (M = 39.84, SD = 9.10), t (344) = 2.08, p = 0.04. The mean total score for Reward was also higher for those from banking (M = 25.37, SD = 9.42) than those from telecommunications (M = 21.75, SD = 9.07), t (344) = 3.59, p = 0.00037. And those in banking had a mean total Power Distance of 19.72 (SD = 7.66) compared to those from telecommunications, M = 17.53, (SD = 7.54), t (344) = 2.64, p = 0.0087.

Since the two groups did not differ on any of the dependent measures, we felt comfortable in combining the data of participants from banking and telecommunications. The means and standard deviations of total scale scores for all participants included in the final analysis are listed in Table 10. Since the scales have a different number of items, we cannot compare the total scale means. However, if we divide each total scale mean by the number of items on the scale, we obtain the mean item score for each scale. For most scales, the average response was between 5 (Slightly Agree) and 6 (Agree). However, for Power Distance, Masculinity / Femininity, and Work Impediment, the average response was between 2 (Disagree) and 3 (Slightly Disagree).

Table 11. Mean and standard deviation for each total scale score and the mean item score for each scale of the Security Awareness Survey

Scale	Number of items	M Total Score	SD Total Score	M Item Score
Self-efficacy	6	34.95	5.57	5.83
Perceived usefulness	5	30.28	3.75	6.06
Perceived value	6	35.75	4.94	5.96
Information quality	8	41.48	8.06	5.18
Management support	8	40.68	9.01	5.08
Punishment	5	20.89	5.96	4.18
Reward	7	23.22	9.37	3.32
Social pressure	5	23.72	5.95	4.74
Individualism – collectivism	6	31.86	7.15	5.31
Masculinity – femininity	5	13.13	6.62	2.63

Power distance	7	18.42	7.65	2.63
Uncertainty Avoidance	5	29.65	4.45	5.93
Attitude toward security	5	30.58	3.81	6.12
Intention to comply	5	31.32	3.94	6.26
Effective use of security awareness	5	24.84	5.62	4.97

PLS-SEM

The model to be tested is illustrated by the path diagram in Figure 5. The circles represent latent variables, theoretical concepts that are not directly measured. The indicators along with the constructs they are linked to comprise the measurement model or outer model. The latent variables and the paths that connect them make up the structural model or inner model.

In the measurement model, when arrows point from the construct to the indicators, the model is reflective. In this case, the construct is thought to cause the indicators, or to put it another way; the indicators are representative of the construct. Since the indicators are meant to be representative, they are expected to be highly correlated. On the other hand, the measurement model is formative when the path arrows point from the indicators to the construct. Then the indicators form or cause the construct. Each indicator in a formative model captures one facet of the latent variable, and therefore the indicators are not expected to be highly correlated.

Our hypothesized model is a hierarchical-component model since it contains lower-order constructs as well as higher-order constructs. Lower-order constructs are directly measured by indicator variables; higher-order constructs either are a manifestation of or caused by lower-order constructs. Table 11 lists each latent variable in our model and whether it is a lower or higher-order construct and whether it is reflective or formative. The table also lists the abbreviations for construct names that will be used throughout this paper.

Table 12. List of latent variables included in the model, their level of abstraction, and measurement type. Abbreviations for variables names are given in parentheses.

Latent Variable	Level of Abstraction	Measurement Type
Attitude toward security (ATTS)	Lower-order	Reflective
Cultural Effects (CUE)	Higher-order	Formative
Effective use of security awareness (EUSA)	Lower-order	Reflective
Extrinsic Motivation	Higher-order	Formative
Individualism / collectivism (IN_COLL)	Lower Order	Formative
Information quality (INQ)	Lower-order	Reflective
Intention to comply (IC)	Lower-order	Reflective
Intrinsic Motivation (IM)	Higher-order	Formative
Management support (MSUPP)	Lower-order	Reflective
Masculinity / femininity (MA_FE)	Lower Order	Formative
Perceived usefulness (PU)	Lower-order	Reflective
Perceived value (PVA)	Lower-order	Reflective
Power distance (PD)	Lower Order	Formative
Punishment (PUN)	Lower-order	Reflective
Reward (RE)	Lower-order	Reflective
Self-efficacy (SE)	Lower-order	Reflective
Social pressure (SP)	Lower-order	Reflective
Uncertainty Avoidance (UA)	Lower Order	Formative

The indicators linked to each higher-order construct in our model are not shown in Figure 5 to simplify the path diagram. However, Table 12 lists the indicators related to each higher-order construct.

Table 13. The indicators linked to each higher-order construct.

	Higher-order construct		
	CUE	EM	IM
Indicators	IN_COLL_1	MSUPP_1	PU_1
	IN_COLL_2	MSUPP_2	PU_2
	IN_COLL_3	MSUPP_3	PU_3
	IN_COLL_4	MSUPP_4	PU_4
	IN_COLL_5	MSUPP_5	PU_5

	IN_COLL_6	MSUPP_6	PVA_1
	MA_FE_1	MSUPP_7	PVA_2
	MA_FE_2	MSUPP_8	PVA_3
	MA_FE_3	PUN_1	PVA_4
	MA_FE_4	PUN_2	PVA_5
	MA_FE_5	PUN_3	PVA_6
	PD_1	PUN_4	SE_1
	PD_2	PUN_5	SE_2
	PD_3	RE_1	SE_3
	PD_4	RE_2	SE_4
	PD_5	RE_3[b]	SE_5
	PD_6	RE_4	SE_6
	PD_7	RE_5	
	UA_1	RE_6	
	UA_2	RE_7	
	UA_3	SP_1	
	UA_4	SP_2	
	UA_5	SP_3	
		SP_4	
		SP_5	

Model Evaluation

Reflective Constructs

The lower-order measurement model consists of indicators, the variables that are directly measured, and the latent variables that are linked directly to indicators. Reflective measurement models have path arrows that point from the construct to the indicators, and the indicators related to a given construct are all manifestations of that construct. As a result, reflective indicators of a construct should be unidimensional, interchangeable, and highly correlated. To assess the adequacy of reflective constructs, we examine their factor loadings, reliability, convergent validity, and discriminant validity.

This study adopted factors from different studies and build relationships between those variables. However, most of the items used to measure the constructs were developed and tested in different studies. Furthermore, some of these items are being studied for the first time in the security domain and the DRC context. Therefore, EFA was conducted as an essential first step in data analysis.

Initial assessments were conducted using SmartPLS 3.0. The guidelines of Hair et al. (Hair Jr, Hult, Ringle, & Sarstedt, 2016) were adopted to assess the factor loadings. Based on the guidelines, six items loaded less than 0.7 on an assigned factor and were deleted. The deletion of these six items had a positive effect on content validity. Four (4) additional items were removed due to high collinearity. All of the formative indicators have a VIF of less than five, except for one indicator (IN_COLL2) of the cultural effect. This indicator was removed from the model and with it the collinearity problem.

Table 14. Factor loadings, item mean score, and item standard deviation for reflective indicators

	Loading	**Item M**	**Item SD**
Self-Efficacy			
SE_1	0.80	5.62	1.37
SE_2	0.79	5.37	1.45
SE_3	0.76	6.12	1.00
SE_4	0.77	5.90	1.17
SE_5	0.71	6.30	1.04
SE_6	0.66	5.64	1.33
Perceived Usefulness			
PU_1	0.87	6.65	0.76
PU_2	0.90	6.57	0.76
PU_3	0.81	6.08	0.99
PU_4	0.35	4.87	1.61
PU_5	0.74	6.12	1.10
Perceived Value			
PVA_1	0.62	6.57	0.81
PVA_2	0.62	6.49	0.96
PVA_3	0.80	6.04	1.10
PVA_4	0.85	6.04	1.09
PVA_5	0.73	5.21	1.42
PVA_6	0.72	5.40	1.35
Information Quality			
INQ_1	0.62	5.55	1.25

INQ_2	0.81	5.52	1.22
INQ_3	0.86	5.23	1.24
INQ_4	0.87	5.28	1.20
INQ_5	0.85	5.19	1.24
INQ_6	0.79	5.16	1.25
INQ_7	0.81	4.90	1.30
INQ_8	0.75	4.64	1.44
Management Support			
MSUPP_1	0.74	5.06	1.37
MSUPP_2	0.75	5.16	1.41
MSUPP_3	0.77	5.76	1.32
MSUPP_4	0.65	4.75	1.63
MSUPP_5	0.81	5.02	1.54
MSUPP_6	0.71	4.49	1.57
MSUPP_7	0.81	5.44	1.43
MSUPP_8	0.82	4.99	1.59
Punishment			
PUN_1	0.70	3.33	1.78
PUN_2	0.75	3.84	1.82
PUN_3	0.67	4.29	1.68
PUN_4	0.74	4.82	1.45
PUN_5	0.75	4.62	1.49
Reward			
RE_1	0.76	2.51	1.64
RE_2	0.77	2.62	1.73
RE_3	0.47	4.55	1.62
RE_4	0.84	3.23	1.84
RE_5	0.79	3.75	1.75
RE_6	0.88	3.16	1.75
RE_7	0.84	3.40	1.81
Social Pressure			
SP_1	0.73	4.20	1.95
SP_2	0.74	3.99	1.92
SP_3	0.83	5.19	1.30
SP_4	0.84	5.07	1.26
SP_5	0.65	5.27	1.34
Attitude Toward Security			
ATTS_1	0.92	6.37	0.84
ATTS_2	0.87	6.33	0.81
ATTS_3	0.93	6.35	0.83
ATTS_4	0.54	5.23	1.34
ATTS_5	0.90	6.31	0.85
Intent to Comply			
IC_1	0.87	6.32	0.77

IC_2	0.92	6.38	0.81
IC_3	0.93	6.30	0.83
IC_4	0.90	6.16	1.00
IC_5	0.90	6.16	0.95
Effective Use of Security Awareness			
EUSA_1	0.85	5.15	1.26
EUSA_2	0.90	4.88	1.22
EUSA_3	0.92	5.04	1.28
EUSA_4	0.90	4.86	1.25
EUSA_5	0.93	4.91	1.23

Reliability and Validity Assessment

The reliability of a set of items refers to their internal consistency or the extent to which a set of items that measure the same concept yield similar results. If a set of items has high reliability, then each participant should have similar scores on all items. One widely accepted measure of reliability is Chronbach's alpha. Cronbach's alpha ranges from 0 to 1, with higher numbers indicating greater reliability. A value of 0.7 is considered to be the minimum acceptable alpha (Nunnally & Bernstein, 1978). Another measure of reliability used in structural equation modeling is composite reliability. Like Chronbach's alpha, composite reliability ranges from 0 to 1, with 0.7 considered to be the threshold value (Henseler, Ringle, & Sarstedt, 2012).

Following the EFA analysis, construct reliability was calculated. Table 14 presents the results, which show that Cronbach's alpha values for all of the constructs in the research model were greater than 0.7, indicating that all constructs had adequate reliability assessment scores. The composite reliability of all of the reflective constructs was above the 0.7 threshold value, which demonstrated high levels of internal consistency reliability for all reflective constructs. Moreover, the AVE values for all reflective constructs were above 0.5, which means that the measure of all reflective constructs has a high level of convergent validity.

The discriminant validity was reviewed using the Fornell–Larcker criterion. The cross-loadings were checked for discriminant validity, and the square root of the AVE of each construct was found to be higher than the construct's highest correlation with any other construct in the model. Table 14 presents the results; the requirements for the Cronbach's alpha, composite reliability, and discriminant validity were met for each construct.

Table 15. Reliability and Validity

	ATT	IC	EUSA	INQ	MSUPP	PU	PUN	PVA	RE	SE	SP
ATT	0.91										
IC	0.71	0.90									
EUSA	0.33	0.31	0.90								
INQ	0.40	0.39	0.39	0.83							
MSUPP	0.39	0.38	0.45	0.60	0.76						
PU	0.54	0.56	0.23	0.40	0.35	0.84					
PUN	0.17	0.22	0.42	0.36	0.43	0.14	0.75				
PVA	0.54	0.60	0.37	0.52	0.42	0.66	0.27	0.73			
RE	-0.01	-0.13	0.17	0.14	0.16	-0.06	0.32	0.01	0.82		
SE	0.45	0.47	0.25	0.48	0.35	0.56	0.14	0.53	0.05	0.75	
SP	0.27	0.30	0.34	0.33	0.39	0.25	0.34	0.35	0.26	0.19	0.79
Reliability and validity											
Cronbach	0.90	0.93	0.94	0.92	0.90	0.79	0.74	0.82	0.88	0.85	0.79
CR	0.94	0.95	0.95	0.94	0.92	0.88	0.84	0.87	0.91	0.89	0.87
AVE	0.83	0.82	0.81	0.68	0.58	0.70	0.57	0.53	0.67	0.57	0.63
Attitude toward security (ATT), effective use (EUSA), compliance intention (IC), information quality (INQ), management support (MSUPP), punishment (PUN), perceived value (PVA), reward (RE), self-efficacy (SE), social pressure (SP), perceived usefulness (PU)											

Higher-order measurement model (Formative Constructs)

Formative constructs have path arrows that point from the indicators to the constructs. Unlike the indicators of reflective constructs, the indicators of formative variables are not meant to be interchangeable; instead, each indicator should measure a unique aspect of the construct. A formative construct, therefore, is a composite of its indicators. To assess the adequacy of the formative measurement model, we examine the variance inflation factor (VIF) and the outer weights of indicators.

Collinearity

Since indicators of formative constructs are unique, they are not expected to be highly correlated. High correlations between formative indicators (collinearity) are problematic. One measure of the degree of correlation between indicators is the VIF. The VIF is the inverse of tolerance—the proportion of an indicator's variance not explained by the other indicators of the construct. Indicators with a VIF above 5 are considered to be too highly

correlated to being unique (Hair Jr, Sarstedt, Ringle, & Gudergan, 2017). Table 15 displays the VIF for each formative indicator. All the formative indicators have a VIF less than 5 except for IN_COLL_2. Each of these indicators shared a significant proportion of its variance with the other indicators and was deleted from the measurement model.

Outer weights.

The other method of evaluating the adequacy of formative indicators is to examine their outer weights. The outer weights are the path weights for the links from formative indicators to their constructs, and they represent the relative contribution of indicators to their associated construct. Each formative indicator should represent a unique facet of the construct, and so each indicator should make some contribution to its construct. If an indicator contributes anything to form the construct, the outer weight will be statistically significant, meaning the weight is unlikely to be 0 in the population. Indicators that are not significant should be considered for deletion (Henseler et al., 2012).

The higher-order constructs in our model were estimated using the repeated indicators approach (Hair et al., 2018). In this approach, indicators can be used twice. First, the loading or weight of each indicator for a lower-order construct is estimated using construct's indicators. Second, the path coefficients between the higher-order construct and its lower-order constructs are estimated using the indicators of the lower-order constructs. When evaluating higher-order measurement models, the important relationships are not between the higher-order constructs and their indicators, but rather between the higher-order constructs and their associated lower-order constructs.

Most of the same tests used to assess lower-order measurement models are used to assess higher-order models. Since the higher-order constructs in our model are formative, VIF and path weights are the tests used.

Table 15 displays the VIF and path weights for the second-order constructs. All of the path weights from lower-order constructs to IM are significant. And all of the path weights for the lower-order constructs that make up EM are also significant. The same result for all the path weights for the lower-order constructs that make up CUE are also significant.

Table 16. Path coefficient (weight) for each lower-order construct and the associated higher-order construct.

Higher-Order Construct	Lower-order Construct	VIF	Path Coefficient	p-value
CUE	IN_COLL	1.13	0.28	< 0.01
	MA_FEM	1.43	0.23	< 0.01
	PD	1.43	0.27	< 0.01
	UA	1.20	0.65	< 0.01
EM	MSUPP	1.38	0.85	< 0.01
	PUN	1.44	0.70	< 0.01
	RE	1.90	0.36	< 0.01
	SP	1.34	0.70	< 0.01
IM	PU	2.37	0.86	< 0.01
	PVA	2.04	0.88	< 0.01
	SE	1.68	0.79	< 0.01

Model Testing

Having established that the theoretical model demonstrates adequate validity and reliability, a test of the structural model was conducted. A PLS approach to structural equation modeling was used to estimate the measurement model. Figure 6 shows the results of the model estimation, path coefficients, path significant level biased on a two-tailed t-test, and the variance explained by the independent variables (R2). The PLS bootstrapping procedure provides the SRMR criterion, which has a value of less than 0.08; hence, the model meets the goodness of fit criteria.

The relationships between constructs were tested after supporting the validity and reliability of the measurement model. All hypothesized relationships and the moderating cultural effects were tested. Figure 6 presents the result of the model testing.

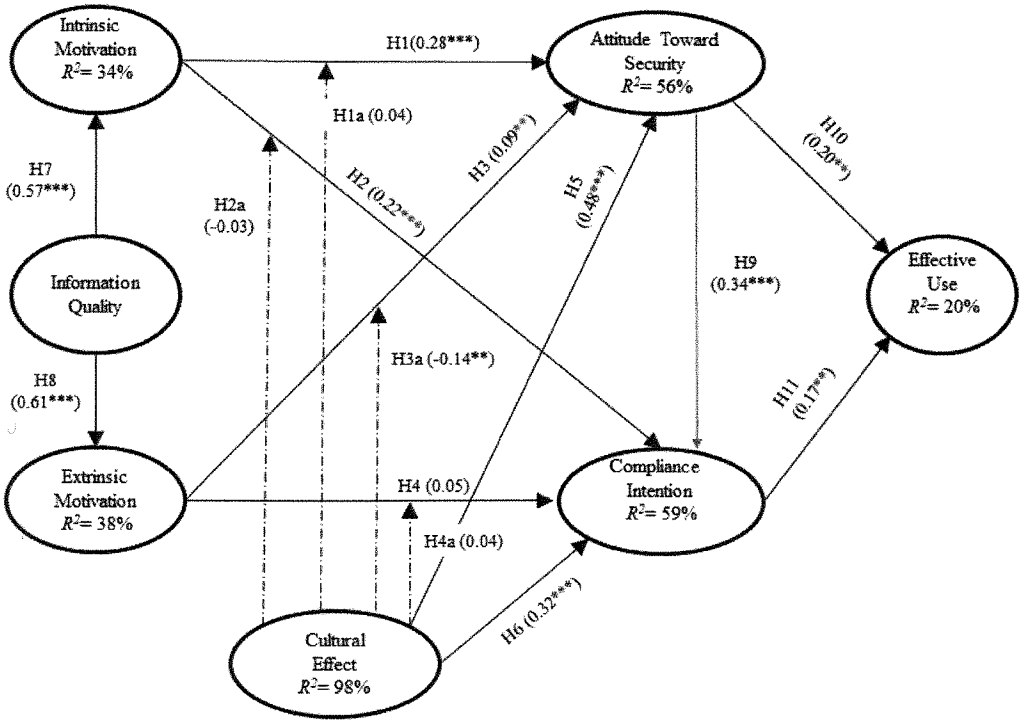

Figure 6. Hypothesis Results

Table 17 presents the indirect effects through which each construct and dimension affects the effective use.

Table 17. Model Indirect Effects

Indirect Effect	β	P value
MA_FE -> EUSA	0.01	0.39
PD -> EUSA	0.02	0.08
EM -> EUSA	0.03	0.03
IN_COLL -> EUSA	0.03	0.01
IM -> EUSA	0.11	0.00
INQ -> EUSA	0.09	0.00
UA -> EUSA	0.15	0.00
CUE -> EUSA	0.18	0.00

Hypothesis Discussion

The research question that drove this study was, "How do cultural values at the individual level influence the effective use of security awareness in organizations in the DRC?" The study answered this question by examining the effect of culture on the relationship between employees' intrinsic and extrinsic motivations; the relationship between employees' intrinsic and extrinsic motivations with both attitudes toward security and intention to comply with security guidelines; and finally the relationship between information quality, employee attitude, and compliance intention with employees' effective use of security awareness. The results of this study show that individual culture positively influences the attitude of employees, which then influences their effective use of the security awareness program.

Cultural Effect

Cultural effects had a positive influence on employees' attitudes toward security awareness (H5) and employees' compliance intention (H6). Cultural effects also had a negative moderating effect on the relationship between employees' extrinsic motivation and attitude toward security (H3a). The remaining moderating effects of culture on the various relationships were not significant.

The results in table 16 indicate that out of the four elements constituting cultural effects, only individualism/collectivism and uncertainty avoidance have a positive influence on employees' effective use of the security awareness program. These results imply that for the effective use of security awareness in the Congolese context, organizations must promote these two factors in their security programs. This result can also be seen in the way that participants answered the survey question. 80% of participants agreed that being loyal to the group (collectivism) is more important than individual gain, and 85% agreed that group success is more important than individual success. 94% of participants agreed with the statement, "To me, it is important to have information on security requirements and instructions spelled out so that employees always know what they are expected to do (uncertainty avoidance)." On the other hand, only 83% agreed that "To me, managers expect workers to closely follow information security awareness instructions and procedures." It

should be troubling to management that almost 20% of employees doubt whether they are expected to follow the information security guidelines.

Four moderating effects were hypothesized in the study. It was found that in the Congolese context, cultural effects negatively influenced the relationship between extrinsic motivation and attitude toward security (H3a). The three remaining moderating effects were not statistically significant. Further investigation is required to determine which of the specific element(s) within cultural effects creates a negative moderating influence in the relationship.

Information Quality

Information quality had a positive influence on employees' intrinsic motivation (H7) and extrinsic motivation (H8), and an indirect positive effect on the effective use of the security awareness program by employees. The participants agreed with all of the items on the information quality scale. However, the survey does reveal that many participants had doubts about the quality of the information on security awareness that they received. One in four were neutral toward or disagreed with the claim that information was presented. Only two-thirds agreed that the information on security awareness was up-to-date or personalized to their needs. Moreover, only half of the employees believed that security awareness information was easily accessible.

The results show that INQ positively influences all items of both intrinsic and extrinsic motivation. Its highest influence was on MSUPP, followed by PVA, PU, SE, PUN, SP, and finally RE. This result suggests that in the Congolese context, INQ is a very important construct that information security professionals must take into account to gain management support; this is essential to guarantee a successful information security program.

Motivation

Intrinsic motivation had a positive influence on employees' attitudes toward security awareness (H1) and compliance intention (H2). Extrinsic motivation had a positive influence on employees' attitudes toward security awareness (H3), but it did not have a significant influence on employees' compliance intention (H4). As shown in Table 16, both intrinsic motivation and extrinsic motivation have an indirect positive effect on the effective use of security awareness.

1. Intrinsic Motivation

Intrinsic motivation—self-efficacy, perceived usefulness, and perceived value—had a positive effect on employees' attitudes toward security and their intention to comply. The results in table 3 indicate that intrinsic motivation also has a positive indirect effect on employees' effective use of the security awareness program. Hence, for employees of an organization to have a favorable attitude toward information security, the intention to comply with security guidelines, and effectively use the security awareness program in the Congolese context, the implemented security awareness programs must satisfy employees' need for knowledge about security (perceived value). Furthermore, employees must feel that the programs have perceived usefulness; that is, they must believe that the programs will help them to reduce security threats effectively. Finally, employees must feel that they have the ability to understand and implement the organization's security programs (self-efficacy).

2. Extrinsic Motivation

Extrinsic motivation - top management support, sanction, reward, and social pressure - had a positive effect on employees' attitudes toward security, but it did not influence the employees' intention to comply with security awareness guidelines. The results in table 3 indicate that extrinsic motivation also has a positive indirect effect on employees' effective use of the security awareness program. Hence, for employees of an organization to have a favorable attitude toward information security and effectively use the security awareness program in the Congolese context, the implemented security awareness programs must consider management support and level of support as a top priority. The result also implies that cybersecurity program manager must not make punishment the primary motivator to change attitude neither should they use reward for the same purpose as they both exhibited limited effect on both attitude and intention to comply.

Attitude toward Security

Employees' attitudes toward security had both a positive influence on their effective use of the security awareness program (H10) and their intention to comply with security guidelines (H9). The vast majority of participants seemed to have a positive attitude toward

security. The data shows that over 90% of participants agreed that security awareness was relevant, useful, and necessary. Only 1% did not believe that security awareness was useful, and just 4% did not agree that it was important or necessary. More surprisingly, in response to the statement "To me, the security awareness program is beneficial," none of the participants chose strongly agree or agree. Almost 47% chose slightly agree, and 44.80% chose neutral.

Despite the moderately significant relationship between attitude toward security awareness and the effective use of security awareness, the model only explained 20% of the variance of effective use. This could be partly caused by a lukewarm attitude toward security awareness. Therefore, if an organization would like to increase the effective use of its security awareness program, it must begin by working on its employees' attitude toward security. There is a need to shift the attitude from neutral to a more positive one.

Compliance Intention

Employees' compliance intention had slightly less influence on employees' effective use of the security awareness program (H11) than attitude toward security. The intention to comply shows a similar pattern to attitude toward security. This result can also be seen in the way that participants answered the survey questions. Like attitude, intent to comply may not be strong. While over 90% of participants agreed with the statements "I intend to protect information resources according to the requirements of the security awareness programs of my organization" and "I intend to carry out my responsibilities prescribed in the security awareness programs of my organization when I use information resources," no one strongly agreed with them. Moreover, no participant chose agree or strongly agreed in response to the statement "I intend to comply with the requirements of the security awareness programs of my organization." Only 44.80% chose slightly agree, and 47.11% chose neutral. As in the case of attitude, this may be partly attributed to a lukewarm attitude toward security awareness. Therefore, if an organization in the Congolese context would like to increase the effective use of its security awareness program, it must work on its employees' intention to comply with security guidelines by improving INQ, EM, and IM.

CHAPTER 6

CONCLUSION AND LIMITATION

Theoretical and practical Contribution

Given the trend of globalization in business and the sharing of security awareness processes and guidelines, it has become particularly important to understand how local and individual culture influences the effective use of security awareness. While much of the previous literature concentrated on the deterrent effect of sanctions or incentives to encourage desirable employee behavior, no studies have addressed the problem of employees' effective use of security awareness programs with a focus on the individual cultural dimension.

To our knowledge, this study is the first to develop a model to investigate the influence of employees' culture on the effective use of security awareness programs. This study contributes to behavioral aspects of the body of knowledge on information security by presenting empirical support that employees' culture, intrinsic motivation, extrinsic motivation, information quality, and attitude toward security awareness programs are essential factors to consider to predict employees' decisions on the effective use of security awareness program. Collectivism and uncertainty avoidance are positively associated with the effective use of security awareness programs, while masculinity/femininity and power distance did not.

This study presents empirical evidence that employees' intention to comply with security awareness guidelines is not as good of a predictor as the attitude toward security when it comes to employee's effective use of a security awareness program. Both intrinsic and extrinsic factors considered in this study are positively associated with the effective use of security awareness programs.

Furthermore, the study confirms that top management support is a decisive positive factor in helping increase the effective use of security awareness in the Congolese context. According to the findings, senior management must work on improving employees' intrinsic motivation and attitude concerning security awareness guidelines and must follow through with both reward and punishment. Finally, organizations should create a culture where each

employee makes their peers accountable for following the security awareness program guidelines.

Conclusion and Limitations

The objective of the study was to illustrate how cultural values at the individual level of analysis may influence the effective use of a security awareness program, using a proposed model with constructs from TAMs. This study provides a general framework and sets the stage for future research on the effective use of security awareness and the role of culture in information security in general.

Although no statistically significant bias was found for this study, we identify at least two limitations to the research effort. First, the usage measurements were self-reported, which could lead to a bias in reporting; we believe that when people are asked about their security-related behavior, they are unlikely to answer with complete honesty. Second, although the variables in the study explain the variation in effective use, other variables that may also influence effective use, such as computer skills, were left out.

REFERENCES

Aaker, D. A. (2009). *Managing brand equity*: Simon and Schuster.

Agarwal, R., & Prasad, J. (1999). Are individual differences germane to the acceptance of new information technologies? *Decision sciences, 30*(2), 361-391.

Agrawal, A., Fantham, D., Ghosh, D., Kelley, D., Florio, E., Avena, E., . . . Zohar, Y. (2019). *Microsoft Security Intelligence Report*. Retrieved from https://www.microsoft.com/en-us/security/operations/security-intelligence-report

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In *Action control* (pp. 11-39): Springer.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211.

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behaviour.

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Information security policy compliance: The role of information security awareness.

Alsajjan, B., & Dennis, C. (2010). Internet banking acceptance model: Cross-market examination. *Journal of business research, 63*(9-10), 957-963.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613-643.

Anderson, J. P. (1972). *Computer Security Technology Planning Study. Volume 2*. Retrieved from

Anderson, J. P. (1980). Computer security threat monitoring and surveillance. *Technical Report, James P. Anderson Company*.

Ang, J. S., Quek, S., Teo, T. S., & Lui, B. (1999). Modeling IS planning benefits using ACE. *Decision sciences, 30*(2), 533-562.

Aytes, K., & Connolly, T. (2004). Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing (JOEUC), 16*(3), 22-40.

Bagozzi, R. P. (2007). The legacy of the technology acceptance model and a proposal for a paradigm shift. *Journal of the Association for Information Systems, 8*(4), 3.

Banerjee, C., & Pandey, S. (2010). Research on software security awareness: problems and prospects. *ACM SIGSOFT Software Engineering Notes, 35*(5), 1-5.

Bauer, S., & Frysak, J. (2014). Developing a viral artifact to improve employees' security behavior. *Int J Soc Behav Educ Econ Bus Indus Eng, 8*(8), 2449-2452.

Bem, S. L. (1981). The BSRI and gender schema theory: A reply to Spence and Helmreich.

Benbasat, I., & Barki, H. (2007). Quo vadis TAM? *Journal of the Association for Information Systems, 8*(4), 7.

Birnbaum, D., & Sommers, M. J. (1988). ACTOR/TASK INCONGRUITY AND NURSES'WORK ATTITUDES. *Journal of health and human resources administration*, 351-360.

Bock, G. W., & Kim, Y.-G. (2002). Breaking the myths of rewards: An exploratory study of attitudes about knowledge sharing. *Information Resources Management Journal (IRMJ), 15*(2), 14-21.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164.

Bourdieu, P. (1984). *Distinction: A social critique of the judgement of taste*: Harvard university press.

Bryman, A., Becker, S., & Sempik, J. (2008). Quality criteria for quantitative, qualitative and mixed methods research: A view from social policy. *International Journal of Social Research Methodology, 11*(4), 261-276.

Bryman, A., & Bell, E. (2011). Ethics in business research. *Business Research Methods*.

Bulgurcu, B., Cavusoglu, H., & Banbasat, I. (2010). INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS. *MIS Quarterly, 34*(3), 523-A527.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Roles of information security awareness and perceived fairness in information security policy compliance. *AMCIS 2009 Proceedings*, 419.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly, 34*(3), 523-548.

Carmel, E., & Agarwal, R. (2002). Offshore sourcing of IT work. *MIS Quarterly Executive, 1*(2).

Center, I. T. R. (2018). *2018 End-of-Year Data Breach Report*. Retrieved from https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/?utm_source=print&utm_campaign=2018BreachReport

Chang, M. K. (1998). Predicting unethical behavior: a comparison of the theory of reasoned action and the theory of planned behavior. *Journal of business ethics, 17*(16), 1825-1834.

Chau, P. Y., Cole, M., Massey, A. P., & Montoya-Weiss, M. (2002). Cultural differences in the online behavior of consumers. *Association for Computing Machinery. Communications of the ACM, 45*(10), 138-138.

Chau, P. Y., & Hu, P. J. H. (2001). Information technology acceptance by individual professionals: A model comparison approach. *Decision sciences, 32*(4), 699-719.

Chen, C. C., Shaw, R., & Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. *Information Technology, Learning, and Performance Journal, 24*(1), 1.

Choi, N., Kim, D., & Goo, J. (2006). Managerial Information Security Awareness' Impact on an Organization's Information Security Performance. *AMCIS 2006 Proceedings*, 406.

Choudrie, J., & Lee, H. (2004). Broadband development in South Korea: institutional and cultural factors. *European Journal of Information Systems, 13*(2), 103-114.

Conner, M., Povey, R., Sparks, P., James, R., & Shepherd, R. (2003). Moderating role of attitudinal ambivalence within the theory of planned behaviour. *British Journal of Social Psychology, 42*(1), 75-94.

Conner, M., & Sparks, P. (1996). *The theory of planned behaviour and health behaviours*: Maidenhead, BRK, England: Open University Press.

Constant, D., Kiesler, S., & Sproull, L. (1994). What's mine is ours, or is it? A study of attitudes about information sharing. *Information Systems Research, 5*(4), 400-421.

Constant, D., Sproull, L., & Kiesler, S. (1996). The kindness of strangers: The usefulness of electronic weak ties for technical advice. *Organization science, 7*(2), 119-135.

Cook, C., Heath, F., & Thompson, R. L. (2000). A meta-analysis of response rates in web-or internet-based surveys. *Educational and psychological measurement, 60*(6), 821-836.

Cooper, B., Wang, J., Bartram, T., & Cooke, F. L. (2019). Well-being-oriented human resource management practices and employee performance in the Chinese banking sector: The role of social climate and resilience. *Human Resource Management, 58*(1), 85-97.

Crane, D. (1994). *The sociology of culture: Emerging theoretical perspectives*: Blackwell Publishers.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.

Dagwell, R., & Weber, R. (1983). System designers' user models: a comparitive study and methodological critique. *Communications of the ACM, 26*(11), 987-997.

Davis, F. (1986). Technology acceptance model. *York University, par, 1*.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319-340.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management science, 35*(8), 982-1003.

Davis, F. D., & Venkatesh, V. (1996). A critical assessment of potential measurement biases in the technology acceptance model: three experiments. *International Journal of Human-Computer Studies, 45*(1), 19-45.

Davis, F. D., & Venkatesh, V. (2004). Toward preprototype user acceptance testing of new information systems: implications for software project management. *IEEE Transactions on Engineering Management, 51*(1), 31-46.

Deci, E., & Ryan, R. M. (1985). *Intrinsic motivation and self-determination in human behavior*: Springer Science & Business Media.

Deci, E. L., & Ryan, R. M. (1975). *Intrinsic motivation*: Wiley Online Library.

Deci, E. L., & Ryan, R. M. (1987). The support of autonomy and the control of behavior. *Journal of personality and social psychology, 53*(6), 1024.

Dee Dickerson, M., & Gentry, J. W. (1983). Characteristics of adopters and non-adopters of home computers. *Journal of Consumer research, 10*(2), 225-235.

DeLone, W. H., & McLean, E. R. (1992). Information systems success: The quest for the dependent variable. *Information Systems Research, 3*(1), 60-95.

Delone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: a ten-year update. *Journal of management Information Systems, 19*(4), 9-30.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal, 19*(4), 391-412.

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), 386.

Downing, C. E., Gallaugher, J., & Segars, A. H. (2003). Information technology choices in dissimilar cultures: Enhancing empowerment. *Journal of Global Information Management (JGIM), 11*(1), 20-39.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45*(1), 67-87.

Dwivedi, Y., Khoumbati, K., Williams, M., & Lal, B. (2007). Factors affecting consumers' behavioural intention to adopt broadband in Pakistan. *Transforming Government: People, Process and Policy, 1*(3), 285-297.

Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes*: Harcourt Brace Jovanovich College Publishers.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research.*

Fowler Jr, F. J., & Cosenza, C. (2009). Design and evaluation of survey questions. *The SAGE handbook of applied social research methods*, 375-412.

Foxall, G. (1997). Affective responses to consumer situations. *The International Review of Retail, Distribution and Consumer Research, 7*(3), 191-225.

Galvez, S. M., & Guzman, I. R. (2009). Identifying factors that influence corporate information security behavior. *AMCIS 2009 Proceedings*, 765.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Inexperience and experience with online stores: The importance of TAM and trust. *IEEE Transactions on Engineering Management, 50*(3), 307-321.

George, J. M., & Brief, A. P. (1996). *Motivational agendas in the workplace: The effects of feelings on focus of attention and work motivation*: Elsevier Science/JAI Press.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). 2005 CSI/FBI computer crime and security survey. *Computer Security Journal, 21*(3), 1.

Gouldner, A. W. (1957). Cosmopolitans and locals: Toward an analysis of latent social roles. I. *Administrative science quarterly*, 281-306.

Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. *Security Focus, December, 18.*

Grenny, J., Patterson, K., Maxfield, D., McMillan, R., & Switzler, A. (2013). *Influencer: The power to change anything*: McGraw-Hill Professional.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing theory and Practice, 19*(2), 139-152.

Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*: Sage Publications.

Hair Jr, J. F., Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2017). *Advanced issues in partial least squares structural equation modeling*: SAGE Publications.

Hall, D. L. (1973). The Civilization of Experience a Whiteheadian Theory of Culture.

Harrington, S., Anderson, C., & Agarwal, R. (2006). Practicing safe computing: Message framing, self-view, and home computer user security behavior intentions. *ICIS 2006 Proceedings*, 93.

Hartwick, J., & Barki, H. (1994). Explaining the role of user participation in information system use. *Management science, 40*(4), 440-465.

Häußinger, F. (2015). *Studies on Employees' Information Security Awareness.* Niedersächsische Staats-und Universitätsbibliothek Göttingen,

Helmreich, R. L. (1994). Anatomy of a system accident: The crash of Avianca Flight 052. *The international journal of aviation psychology, 4*(3), 265-284.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2012). Using partial least squares path modeling in advertising research: basic concepts and recent issues. *Handbook of research on international advertising, 252*.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Hill, C. E., Loch, K. D., Straub, D., & El-Sheshai, K. (1998). A qualitative assessment of Arab culture and information technology transfer. *Journal of Global Information Management (JGIM), 6*(3), 29-38.

Hoecklin, L. A. (1995). *Managing cultural differences: Strategies for competitive advantage*: Addison-Wesley Longman Limited.

Hoffman, N., & Klepper, R. (2000). Assimilating new technologies: The role of organizational culture. *Information Systems Management, 17*(3), 36-42.

Hofstede, G. (1980a). Culture and organizations. *International Studies of Management & Organization, 10*(4), 15-41.

Hofstede, G. (1980b). Motivation, leadership, and organization: do American theories apply abroad? *Organizational dynamics, 9*(1), 42-63.

Hofstede, G. (1984). *Culture's consequences: International differences in work-related values* (Vol. 5): sage.

Hofstede, G., & Hofstede, G. J. (1991). Cultures and organizations: Culture of the mind. In: New York, NY: McGraw-Hill.

Hofstede, G., & Hofstede, G. J. (2005). *Organisationer och kulturer*: Studentlitteratur.

Hussain, S. (1998). Technology transfer models across cultures: Brunei-Japan joint ventures. *International Journal of Social Economics, 25*(6/7/8), 1189-1198.

Jackson, S. (2011). Organizational culture and information systems adoption: A three-perspective approach. *Information and Organization, 21*(2), 57-83.

Kacen, J. J., & Lee, J. A. (2002). The influence of culture on consumer impulsive buying behavior. *Journal of consumer psychology, 12*(2), 163-176.

Kaiser, K. M., & Hawk, S. (2008). Evolution of offshore software development: From outsourcing to cosourcing. *MIS Quarterly Executive, 3*(2), 3.

Karahanna, E., Evaristo, J. R., & Srite, M. (2006). Levels of culture and individual behavior: An integrative perspective. *Advanced Topics in Global Information Management, 5*(1), 30-50.

Karger, P. A., & Schell, R. R. (1974). *Multics Security Evaluation Volume II. Vulnerability Analysis*. Retrieved from

Karimi, J., Somers, T. M., & Bhattacherjee, A. (2007). The Role of Information Systems Resources in ERP Capability Building and Business Process Outcomes. *Journal of management Information Systems, 24*(2), 221-260.

Kim, H.-W., Chan, H. C., & Gupta, S. (2007). Value-based adoption of mobile internet: an empirical investigation. *Decision support systems, 43*(1), 111-126.

Kim, H.-W., & Kankanhalli, A. (2009). Investigating user resistance to information systems implementation: A status quo bias perspective. *MIS Quarterly, 33*(3), 567-582.

Ko, D.-G. (2005). Antecedents of knowledge transfer from consultants to clients in enterprise system implementations. *MIS Quarterly, 29*(1), 59-85.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security, 27*(5-6), 224-231.

Kroeber, A. L., & Kluckhohn, C. (1952). Culture: A critical review of concepts and definitions. *Papers. Peabody Museum of Archaeology & Ethnology, Harvard University*.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296.

Kummer, T.-F., Leimeister, J. M., & Bick, M. (2012). On the importance of national culture for the design of information systems. *Business & Information Systems Engineering, 4*(6), 317-330.

Landauer, T. K. (1995). The Trouble with Computers: Usefulness, Usability, and Productivity, The MIT Press. *Cambridge, Mass*.

Larcker, D. F., & Lessig, V. P. (1980). Perceived usefulness of information: A psychometric examination. *Decision sciences, 11*(1), 121-134.

Latham, D. C. (1986). Department of defense trusted computer system evaluation criteria. *Department of Defense*.

Lee, Y. W., Strong, D. M., Kahn, B. K., & Wang, R. Y. (2002). AIMQ: a methodology for information quality assessment. *Information & management, 40*(2), 133-146.

Leidner, D. E., Carlsson, S., Elam, J., & Corrales, M. (1999). Mexican and Swedish managers' perceptions of the impact of EIS on organizational intelligence, decision making, and structure. *Decision sciences, 30*(3), 632-658.

Leidner, D. E., & Kayworth, T. (2006). A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS Quarterly, 30*(2), 357-399.

Likert, R. (1932). A technique for the measurement of attitudes. *Archives of psychology*.

Loch, K. D., Straub, D. W., & Kamel, S. (2003). Diffusing the Internet in the Arab world: The role of social norms and technological culturation. *IEEE Transactions on Engineering Management, 50*(1), 45-63.

Luthans, F. (2002). Positive organizational behavior: Developing and managing psychological strengths. *The Academy of Management Executive, 16*(1), 57-72.

Mackenzie, K. (2006). Employees may be opening the door to criminals. *Financial Times*.

Madden, T. J., Ellen, P. S., & Ajzen, I. (1992). A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and Social Psychology Bulletin, 18*(1), 3-9.

Martinez-Moyano, I. J., Conrad, S. H., & Andersen, D. F. (2011). Modeling behavioral considerations related to information security. *Computers & Security, 30*(6-7), 397-409.

Mathieson, K. (1991). Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. *Information Systems Research, 2*(3), 173-191.

Mathieson, K., Peacock, E., & Chin, W. W. (2001). Extending the technology acceptance model: the influence of perceived user resources. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 32*(3), 86-112.

McCoy, S., Galletta, D. F., & King, W. R. (2007). Applying TAM across cultures: the need for caution. *European Journal of Information Systems, 16*(1), 81-90.

Mead, S. E. (1953). Prof. Sweet's Religion and Culture in America: A Review Article. *Church History, 22*(1), 33-49.

Miller, M. R., Hankinson, J., Brusasco, V., Burgos, F., Casaburi, R., Coates, A., . . . Gustafsson, P. (2005). Standardisation of spirometry. *European respiratory journal, 26*(2), 319-338.

Mingers, J. (2003). The paucity of multimethod research: a review of the information systems literature. *Information Systems Journal, 13*(3), 233-249.

Mitnick, K. D., & Simon, W. L. (2009). *The Art of Intrusion: The real stories behind the exploits of hackers, intruders and deceivers*: John Wiley & Sons.

Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*: John Wiley & Sons.

Moon, J.-W., & Kim, Y.-G. (2001). Extending the TAM for a World-Wide-Web context. *Information & management, 38*(4), 217-230.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems, 18*(2), 126-139.

Neumann, P. G., Robinson, L., Levitt, K. N., Boyer, R., & Saxena, A. (1975). *A Provably Secure Operating System*. Retrieved from

Nguyen, M. N., Potvin, L., & Otis, J. (1997). Regular exercise in 30-to 60-year-old men: Combining the stages-of-change model and the theory of planned behavior to identify determinants for targeting heart health interventions. *Journal of Community Health, 22*(4), 233-246.

Nunnally, J. C., & Bernstein, I. H. (1978). Psychometric theory.

Pahnila, S., Siponen, M., & Mahmood, A. (2007a). *Employees' behavior towards IS security policy compliance.* Paper presented at the System sciences, 2007. HICSS 2007. 40Th annual hawaii international conference on.

Pahnila, S., Siponen, M., & Mahmood, A. (2007b). Which factors explain employees' adherence to information security policies? An empirical study. *PACIS 2007 Proceedings*, 73.

Parboteeah, K. P., Bronson, J. W., & Cullen, J. B. (2005). Does national culture affect willingness to justify ethically suspect behaviors? A focus on the GLOBE national culture scheme. *International journal of cross cultural management, 5*(2), 123-138.

Pavlou, P. A., & Chai, L. (2002). What drives electronic commerce across cultures? Across-cultural empirical investigation of the theory of planned behavior. *J. Electron. Commerce Res., 3*(4), 240-253.

Peltier, T. R. (2005). *Information security risk analysis*: CRC press.

Rhee, E., Uleman, J. S., & Lee, H. K. (1996). Variations in collectivism and individualism by ingroup and culture: Confirmatory factor analysis. *Journal of personality and social psychology, 71*(5), 1037.

Richardson, R. (2007). Csi. *FBI Computer Crime and Security Survey*.

Richardson, R., & Director, C. (2008). CSI computer crime and security survey. *Computer security institute, 1*, 1-30.

Ringle, C. M., Wende, S., & Becker, J.-M. (2015a). SmartPLS 3. *Boenningstedt: SmartPLS GmbH, http://www. smartpls. com.*

Ringle, C. M., Wende, S., & Becker, J.-M. (2015b). SmartPLS 3. Boenningstedt: SmartPLS GmbH. In.

Robey, D. (1979). User attitudes and management information system use. *Academy of Management Journal, 22*(3), 527-538.

Robey, D., & Rodriguez-Diaz, A. (1989). The organizational and cultural context of systems implementation: Case experience from Latin America. *Information & management, 17*(4), 229-239.

Rogers Everett, M. (1995). Diffusion of innovations. *New York, 12*.

Roscoe, J. T. (1975). *Fundamental research statistics for the behavioral sciences [by] John T. Roscoe*.

Rose, G. M., Evaristo, R., & Straub, D. (2003). Culture and consumer responses to web download time: a four-continent study of mono and polychronism. *IEEE Transactions on engineering management, 50*(1), 31-44.

Ryan, R. M., & Deci, E. L. (2000). Intrinsic and extrinsic motivations: Classic definitions and new directions. *Contemporary educational psychology, 25*(1), 54-67.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal, 19*(3), 122-131.

Saunders, M., Lewis, P., Thornhill, A., & Wilson, J. (2009). Business research methods. *Financial Times, Prentice Hall: London*.

Schacht, J. (1975). *Jobstream Separator System Design*. Retrieved from

Schlienger, T., & Teufel, S. (2003). Information security culture-from analysis to change. *South African Computer Journal, 2003*(31), 46-52.

Schwartz, S. H. (1994). *Beyond individualism/collectivism: New cultural dimensions of values*: Sage Publications, Inc.

Sekaran, U., & Bougie, R. (2011). Business Research Methods: A skill-building approach. In: New York: McGraw-Hill.

Sharif Abbasi, M., Hussain Chandio, F., Fatah Soomro, A., & Shah, F. (2011). Social influence, voluntariness, experience and the internet acceptance: An extension of technology acceptance model within a south-Asian country context. *Journal of Enterprise Information Management, 24*(1), 30-52.

Shih, Y.-Y., & Fang, K. (2004). The use of a decomposed theory of planned behavior to study Internet banking in Taiwan. *Internet Research, 14*(3), 213-223.

Siehl, C., Martin, J., & Schneider, B. (1990). Organizational climate and culture. In: Chicago, IL: Jossey-Bass.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management, 51*(2), 217-224.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2).

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Srite, M., & Karahanna, E. (2006). The role of espoused national cultural values in technology acceptance. *MIS Quarterly*, 679-704.

Stangor, C. (2014). *Research methods for the behavioral sciences*: Nelson Education.

Straub, D., Keil, M., & Brenner, W. (1997). Testing the technology acceptance model across cultures: A three country study. *Information & management, 33*(1), 1-11.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, 441-469.

Straub Jr, D. W., & Burton-Jones, A. (2007). Veni, vidi, vici: Breaking the TAM logjam. *Journal of the Association for Information Systems, 8*(4), 223.

Straub Jr, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: a field study. *MIS Quarterly*, 45-60.

Tan, B. C., Smith, H. J., Keil, M., & Montealegre, R. (2003). Reporting bad news about software projects: Impact of organizational climate and information asymmetry in an individualistic and a collectivistic culture. *IEEE Transactions on engineering management, 50*(1), 64-77.

Taylor, S., & Todd, P. (1995a). Assessing IT usage: The role of prior experience. *MIS Quarterly*, 561-570.

Taylor, S., & Todd, P. (1995b). Decomposition and crossover effects in the theory of planned behavior: A study of consumer adoption intentions. *International journal of research in marketing, 12*(2), 137-155.

Teo, T., Wong, S. L., & Chai, C. S. (2008). A cross-cultural examination of the intention to use technology between Singaporean and Malaysian pre-service teachers: an application of the Technology Acceptance Model (TAM). *Journal of Educational Technology & Society, 11*(4), 265.

Triandis, H. C. (1972). The analysis of subjective culture.

Triandis, H. C. (1995). *Individualism & collectivism*: Westview press.

Turró, A., Urbano, D., & Peris-Ortiz, M. (2014). Culture and innovation: The moderating effect of cultural values on corporate entrepreneurship. *Technological Forecasting and Social Change, 88*, 360-369.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision sciences, 39*(2), 273-315.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425-478.

Venkatesh, V., & Zhang, X. (2010). Unified theory of acceptance and use of technology: US vs. China. *Journal of global information technology management, 13*(1), 5-27.

Walsham, G. (2002). Cross-cultural software production and use: a structurational analysis. *MIS Quarterly*, 359-380.

Warshaw, P. R., & Davis, F. D. (1985). Disentangling behavioral intention and behavioral expectation. *Journal of experimental social psychology, 21*(3), 213-228.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security, 17*(1), 4-19.

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special publication, 800*(50), 1-39.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security, 17*(4), 330-340.

APPENDICES

APPENDIX A: SURVEY INSTRUMENT

Information Security awareness Program in Financial Organizations: Elements of effective use.

Selection de la langue / Language Selection

1. Please select the language in which you are more comfortable taking the survey / Veuillez choisir la langue qui vous convient pour répondre aux questions de l'enquête.

- ◯ French / Francais
- ◯ English / Anglais

Information Security awareness Program in Financial Organizations: Elements of effective use.

Welcome to My Security Awareness Survey EDIT

March 1, 2017

Dear Bankers:

I, Nzailu Basinsa Arnold, am conducting a research project titled "Information Security awareness Program in Financial Organizations: Elements of effective use." as part of my dissertation at Dakota State University. The purpose of the study is to understand the human elements that are relevant for an effective use of a security awareness program which takes into account our local culture in the Democratic Republic of Congo.

You as a banker, you are invited to participate in the study by completing the survey in the next pages. We realize that your time is valuable and have attempted to keep the requested information as brief and concise as possible. It will take you approximately 30 minutes of your time. Your participation in this project is voluntary. You may withdraw from the study at any time without consequence.

There are no known risks to you for participating in this study.

There are no direct benefits to your organization. However, we are hoping that the result of this study will have the following two contribution to our national information security culture in general:

1. Practical contribution

From a managerial perspective, given the importance of information security awareness in contemporary organizations, the findings of this study will empower managers and policy-makers to formulate policies that appropriately target organizations to ensure the creation of effective security awareness programs.

2. Theoretical contribution

The findings of this study will also provide a theoretical basis and empirical evidence of human elements needed to build an effective security awareness program in a financial organization. Additionally, the findings of this study may lead to the creation of native theories in the information security research field.

Your responses are strictly confidential. When the data and analysis are presented, you will not be linked to the data by your name, title or any other identifying item. It is not possible for me the researcher to link answers to email addresses. However, your email address will be used to select winners of the giveaway prize as explained below.

To thank you for your participation, at the end of the first week and at least 100 fully completed surveys, we will give away 25 Dreaman USB 3.0 16GB Flash Drive Memory Thumb Stick Storage Pen Disk Digital U Disk. Only employees who have fully complete the survey questions will be part of the population used to select the prize winners. To ensure transparency in the process, selection process will be recorded in the presence of the HR representative and the recording will be made available to employees through the bank intranet. The following process will be follow to select the prize winners. Email of employees who have fully complete the survey questions will be put in an excel file and using the random sampling function in excel, 25 employees will be picked to receive the USB drive. At the end of the second week and at least 150 fully completed surveys, we will give away a Sony PlayStation 4 with 500GB Console. The prize winner will be selected following the same process previously described.

Your consent is implied by completing the remaining part of the questionnaire. Please keep this letter for your information. If you have any questions, now or later related to the content of this study, you may contact me at abnzailu@pluto.dsu.edu. Thank you very much for your time and assistance.

If you have any questions regarding your rights as a research participant in this study, you may contact the DSU Office of Sponsored Programs at 605-256-5100 or at irb@dsu.edu.

Sincerely,
Arnold Nzailu
abnzailu@pluto.dsu.edu
+1 605-291-6406
This project has been approved by the DSU Institutional Review Board, Approval No.: _____

Information Security awareness Program in Financial Organizations: Elements of effective use.

Demographic Data EDIT

*** 2. Are you male or female?**

- ◯ Male
- ◯ Female

*** 3. What is your age?**

- ◯ 18-20
- ◯ 21-29
- ◯ 30-39
- ◯ 40-49
- ◯ 50-59
- ◯ 60 or older

*** 4. What is the highest level of school you have completed or the highest degree you have received?**

- ◯ Less than high school degree
- ◯ High school degree or equivalent (e.g., GED)
- ◯ Some college but no degree
- ◯ Associate degree
- ◯ Bachelor degree
- ◯ Graduate degree

*** 5. Which of the following best describes the field in which you received your highest degree?**

- ◯ Mathematics
- ◯ Science
- ◯ Healthcare
- ◯ Medicine
- ◯ Computing
- ◯ Engineering
- ◯ Technology
- ◯ Business
- ◯ Other (please specify)

*** 6. Where did you receive you post high school education ?**

- ◯ In Congo
- ◯ Abroad in French-speaking country
- ◯ Abroad in English-speaking country

*** 7. How long have you been working in the banking sector ?**

- ◯ 1 - 5 years
- ◯ 6 - 10 years
- ◯ 10 - 15 years
- ◯ 16 + years

*** 8. How long have you worked in the banking sector abroad (outside Congo) ?**

- ◯ Not Applicable
- ◯ 1 - 5 years
- ◯ 6 - 10 years
- ◯ 10 - 15 years
- ◯ 16 + years

*** 9. In which area of the bank do you work ?**

- ◯ Accounting & Finance
- ◯ Customer Care / Front office
- ◯ Operations / Back office
- ◯ Compliance / Audit
- ◯ Information Technology
- ◯ other

*** 10. How does the bank consider you position ?**

- ◯ Clerk / Staff
- ◯ Supervisor
- ◯ Manager
- ◯ Executive / C-Level

Information Security awareness Program in Financial Organizations: Elements of effective use.

Self-Efficacy

*** 20. Below are a number of statements regarding the security awareness program at the bank. Please read each one and indicate to what extent you agree or disagree with each statement.**

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
I have the necessary skills to effectively use the security awareness program.	○	○	○	○	○	○	○
I have the necessary knowledge to effectively use the security awareness program.	○	○	○	○	○	○	○
I am confident that I can effectively comply with a security awareness program guidelines.	○	○	○	○	○	○	○
I have the expertise to follow preventative measures from the security awareness program to stop people from getting my confidential information.	○	○	○	○	○	○	○
I believe that it is within my control to protect myself from information security violations.	○	○	○	○	○	○	○
I feel comfortable following my organization' security awareness program guideline on my own.	○	○	○	○	○	○	○

Information Security awareness Program in Financial Organizations: Elements of effective use.

Perceived Usefulness

*** 22. Below are a number of statements regarding the security awareness program at the bank. Please read each one and indicate to what extent you agree or disagree with each statement.**

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
To me, Information security awareness is useful to the Bank.	○	○	○	○	○	○	○
To me, It is useful to comply information security awareness.	○	○	○	○	○	○	○
I can integrate security awareness knowledge in my daily work.	○	○	○	○	○	○	○
I know how to search, evaluate and select appropriate security awareness program resources to support my daily decision making at work.	○	○	○	○	○	○	○
I believe that following Security awareness guidelines will enhance my effectiveness in working with computer.	○	○	○	○	○	○	○

Information Security awareness Program in Financial Organizations: Elements of effective use.

Perceived Value

*** 24. Below are a number of statements regarding the security awareness program at the bank. Please read each one and indicate to what extent you agree or disagree with each statement.**

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
To me, security awareness program is useful to the Bank	○	○	○	○	○	○	○
To me, security awareness program is important to the Bank	○	○	○	○	○	○	○
To me, security awareness program is helpful to the Bank	○	○	○	○	○	○	○
To me, security awareness program is valuable to the Bank	○	○	○	○	○	○	○
To me, using security Awarness guidelines makes me feel good	○	○	○	○	○	○	○
To me, using security Awarness guidelines makes a good impression on others	○	○	○	○	○	○	○

Information Security awareness Program in Financial Organizations: Elements of effective use.

Information Quality

*** 26. Below are a number of statement regarding the information quality of the security awareness program. Please read each one and indicate to what extent you agree or disagree with each statement.**

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
To me, the security awareness program provided me with relevant information.	○	○	○	○	○	○	○
To me, It is easy to follow the reasoning in the information provided by security awareness program.	○	○	○	○	○	○	○
To me, the concepts and language use by the security awareness program source make sense.	○	○	○	○	○	○	○
To me, the security awareness program presents ideas clearly.	○	○	○	○	○	○	○
To me, the information that I obtain from the security awareness program is actionable.	○	○	○	○	○	○	○
To me, the security awareness program provides Up-to-date information.	○	○	○	○	○	○	○
To me, the security awareness program provides information personalized to my needs.	○	○	○	○	○	○	○
To me, the security awareness program materials are easily accessible.	○	○	○	○	○	○	○

Information Security awareness Program in Financial Organizations: Elements of effective use.

Information Quality

*** 26. Below are a number of statement regarding the information quality of the security awareness program. Please read each one and indicate to what extent you agree or disagree with each statement.**

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
To me, the security awareness program provided me with relevant information.	○	○	○	○	○	○	○
To me, it is easy to follow the reasoning in the information provided by security awareness program.	○	○	○	○	○	○	○
To me, the concepts and language use by the security awareness program source make sense.	○	○	○	○	○	○	○
To me, the security awareness program presents ideas clearly.	○	○	○	○	○	○	○
To me, the information that I obtain from the security awareness program is actionable.	○	○	○	○	○	○	○
To me, the security awareness program provides Up-to-date information.	○	○	○	○	○	○	○
To me, the security awareness program provides information personalized to my needs.	○	○	○	○	○	○	○
To me, the security awareness program materials are easily accessible.	○	○	○	○	○	○	○

Information Security awareness Program in Financial Organizations: Elements of effective use.

Management Support

*** 28. Below are a number of statement regarding the management support of the security awareness program. Please read each one and indicate to what extent you agree or disagree with each statement.**

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
Management support of the information security awareness program influenced my attitude toward it.	○	○	○	○	○	○	○
Management support of the information security awareness program influenced my intention to comply with its guidelines.	○	○	○	○	○	○	○
To me, management within my organization is very serious about the security awareness.	○	○	○	○	○	○	○
Security awareness training is included as part of orientation for new employees.	○	○	○	○	○	○	○
My organization motivates me to use knowledge from the security awareness program.	○	○	○	○	○	○	○
Employees in my organization receive updated information or training regarding Security awareness program.	○	○	○	○	○	○	○
The degree to which the management considers the deployment of security awareness program as an important issue.	○	○	○	○	○	○	○
The extent to which the management is willing to communicate with staff and participate in Security awareness program	○	○	○	○	○	○	○

Information Security awareness Program in Financial Organizations: Elements of effective use.

Sanction / Reward / Work Impediment

*** 30. Below are a number of statement regarding Sanction / Reward / Work Impediment as it relates to the security awareness program. Please read each one and indicate to what extent you agree or disagree with each statement.**

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
My attitude toward the information security awareness program depended on the punishment attached to it.	○	○	○	○	○	○	○
The punishment for failure to comply with the security awareness program will give me incentive to actually comply.	○	○	○	○	○	○	○
If I were caught violating organization security awareness program guidelines, I would be severely punished.	○	○	○	○	○	○	○
Our Bank disciplines employees who break information security rules	○	○	○	○	○	○	○
Our Bank terminates employees who repeatedly break security rules	○	○	○	○	○	○	○
My attitude toward the information security awareness program depended on the monetary reward attached to it.	○	○	○	○	○	○	○

To me, monetary reward will give me incentive to follow information security awareness guidelines.	○	○	○	○	○	○	○
I will receive increased job security in return for following information security awareness guidelines.	○	○	○	○	○	○	○
My pay raises and/or promotions depend on whether I follow documented security policies and procedures.	○	○	○	○	○	○	○
I will receive personal mention in oral or written reports if I comply with security policies and procedures at our Bank	○	○	○	○	○	○	○
I will be given monetary or non-monetary rewards for following security policies and procedures.	○	○	○	○	○	○	○
Tangible rewards are tied to whether I follow our Bank's IT security policies, procedures, and guidelines.	○	○	○	○	○	○	○
Following security awareness program guidelines holds me back from doing my actual work.	○	○	○	○	○	○	○
Following security awareness program guidelines slows down my response time to my colleagues, customers, managers, etc.	○	○	○	○	○	○	○
Following security awareness program guidelines hinders my productivity at work	○	○	○	○	○	○	○
Following security awareness program guidelines impedes my efficiency at work	○	○	○	○	○	○	○

Information Security awareness Program in Financial Organizations: Elements of effective use.

Social Pressure

*** 32. Below are a number of statement regarding the social pressure as it relates to the security awareness program. Please read each one and indicate to what extent you agree or disagree with each statement.**

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
I have to have a positive attitude toward the information security awareness program because all my colleague do.	○	○	○	○	○	○	○
I have to comply with the information security awareness program because all my colleague do.	○	○	○	○	○	○	○
I believe other employees comply with security awareness program guidelines.	○	○	○	○	○	○	○
I am convinced other employees comply with security awareness program guidelines.	○	○	○	○	○	○	○
To me, it is likely that the majority of other employees comply with security awareness program guidelines to help protect the organization's information systems.	○	○	○	○	○	○	○

Information Security awareness Program in Financial Organizations: Elements of effective use.

Individualism/ Collectivism

*** 34. Below are a number of statement regarding Individualism/ Collectivism as it relates to the security awareness program. Please read each one and indicate to what extent you agree or disagree with each statement.**

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
To me, being accepted as a member of a group is more important than having autonomy and independence.	○	○	○	○	○	○	○
To me, being accepted as a member of a group is more important than being independent.	○	○	○	○	○	○	○
To me, group success is more important than individual success.	○	○	○	○	○	○	○
To me being loyal to a group is more important than individual gain.	○	○	○	○	○	○	○
To me, individual rewards are not as important as group welfare.	○	○	○	○	○	○	○
To me, it is more important for a manager to encourage loyalty and a sense of duty in subordinates than it is to encourage individual initiative.	○	○	○	○	○	○	○

Information Security awareness Program in Financial Organizations: Elements of effective use.

Masculinity/ Femininity

* 36. Below are a number of statement regarding Masculinity and Femininity as it relates to the security awareness program. Please read each one and indicate to what extent you agree or disagree with each statement.

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
To me, it is preferable to have a man in high level position rather than a woman.	○	○	○	○	○	○	○
To me, there are some jobs in which a man can always do better than a woman.	○	○	○	○	○	○	○
To me, it is more important for men to have a professional career than it is for women to have a professional career.	○	○	○	○	○	○	○
To me, solving organizational problems requires the active forcible approach which is typical of men.	○	○	○	○	○	○	○
To me, women do not value recognition and promotion in their work as much as men do	○	○	○	○	○	○	○

Information Security awareness Program in Financial Organizations: Elements of effective use.

Power Distance

*** 38. Below are a number of statement regarding Power Distance as it relates to the security awareness program. Please read each one and indicate to what extent you agree or disagree with each statement.**

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
To me, managers should make most decisions without consulting subordinates.	○	○	○	○	○	○	○
To me, managers should not ask subordinates for advice, because they might appear less powerful.	○	○	○	○	○	○	○
To me, decision making power should stay with top management in the organization and not be delegated to lower level employees.	○	○	○	○	○	○	○
To me, employees should not question their manager's decisions.	○	○	○	○	○	○	○
To me, a manager should perform work which is difficult and important and delegate tasks which are repetitive and mundane to subordinates.	○	○	○	○	○	○	○
To me, higher level managers should receive more benefits and privileges than lower level managers and professional staff.	○	○	○	○	○	○	○
To me, managers should be careful not to ask the opinions of subordinates too frequently, otherwise the manager might appear to be weak and incompetent.	○	○	○	○	○	○	○

*** 39. Below are a number of statement regarding Uncertainty Avoidance as it relates to the security awareness program. Please read each one and indicate to what extent you agree or disagree with each statement.**

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
To me, it is important to have information security requirements and instructions spelled out in detail so that employees always know what they are expected to do.	○	○	○	○	○	○	○
To me, managers expect workers to closely follow information security awareness instructions and procedures.	○	○	○	○	○	○	○
To me, rules and regularities are important because they inform workers what the organization expects of them	○	○	○	○	○	○	○
To me, information security awareness guidelines are helpful to employees on the job	○	○	○	○	○	○	○
To me, information security awareness instructions for operations are important for employees on the job.	○	○	○	○	○	○	○

Attitude toward Security

*** 42. Below are a number of statement regarding the attitude toward the security awareness program. Please read each one and indicate to what extent you agree or disagree with each statement.**

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
To me, the security awareness program is necessary.	○	○	○	○	○	○	○
To me, the security awareness program is beneficial.	○	○	○	○	○	○	○
To me, the security awareness program is important.	○	○	○	○	○	○	○
To me, the security awareness program is exciting.	○	○	○	○	○	○	○
To me, the security awareness program is useful.	○	○	○	○	○	○	○

Intention to comply

*** 44. Below are a number of statement regarding the intention comply with the security awareness program guidelines. Please read each one and indicate to what extent you agree or disagree with each statement.**

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
I intend to comply with the requirements of the security awareness program of my organization.	○	○	○	○	○	○	○
I intend to protect information resources according to the requirements of the security awareness program of my organization.	○	○	○	○	○	○	○
I intend to carry out my responsibilities prescribed in the security awareness program of my organization when I use information resources.	○	○	○	○	○	○	○
I intend to recommend that others comply with the security awareness program guidelines.	○	○	○	○	○	○	○
I intend to assist others in complying with the security awareness program guidelines.	○	○	○	○	○	○	○

*** 45. Below are a number of statement regarding the effective use of the security awareness program guidelines. Please read each one and indicate to what extent you agree or disagree with each statement.**

	Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree
To me, relative to other banks, our bank is successful in using information security awareness guidelines while executing operational activities	○	○	○	○	○	○	○
To me, relative to other banks, our bank is successful in using information security awareness guidelines while executing Marketing activities	○	○	○	○	○	○	○
To me, relative to other banks, our bank is successful in using information security awareness guidelines while executing customer services activities	○	○	○	○	○	○	○
To me, relative to other banks, our bank is successful in using information security awareness guidelines while enhancing third parties relationships	○	○	○	○	○	○	○
To me, relative to other banks, our bank is successful in using information security awareness guidelines while executing sales activities	○	○	○	○	○	○	○

Information Security awareness Program in Financial Organizations: Elements of effective use.

Comments / Commentaires

48. Do you have any other comments ?