Eastern Michigan University
DigitalCommons@EMU

Master's Theses and Doctoral Dissertations

Master's Theses, and Doctoral Dissertations, and Graduate Capstone Projects

8-31-2016

A study of information security awareness program effectiveness in predicting end-user security behavior

James Michael Banfield
Eastern Michigan University

Follow this and additional works at: http://commons.emich.edu/theses

Part of the Information Security Commons, Science and Technology Studies Commons, and the Technology and Innovation Commons

Recommended Citation

Banfield, James Michael, "A study of information security awareness program effectiveness in predicting end-user security behavior" (2016). *Master's Theses and Doctoral Dissertations*. 692.
http://commons.emich.edu/theses/692

This Open Access Dissertation is brought to you for free and open access by the Master's Theses, and Doctoral Dissertations, and Graduate Capstone Projects at DigitalCommons@EMU. It has been accepted for inclusion in Master's Theses and Doctoral Dissertations by an authorized administrator of DigitalCommons@EMU. For more information, please contact lib-ir@emich.edu.

A Study of Information Security Awareness Program Effectiveness in Predicting End-User Security Behavior

by

James Michael Banfield

Dissertation

Submitted to the College of Technology

Eastern Michigan University

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Dissertation Committee:

Denise Pilato, Ph.D.

Bilquis Ferdousi, Ph.D.

Michael McVey, Ed.D

Tierney Orfgen McCleary, Ph.D.

August 31, 2016

Ypsilanti, Michigan

Dedication

I am honored to dedicate this effort to the two most influential people in my life, my parents, Joyce and Richard Banfield. While both have passed on now, the lessons they taught me growing up are still with me and helped to complete this project. I know that they are watching from above with much pride.

Abstract

As accessibility to data increases, so does the need to increase security. For organizations of all sizes, information security (IS) has become paramount due to the increased use of the Internet. Corporate data are transmitted ubiquitously over wireless networks and have increased exponentially with cloud computing and growing end-user demand. Both technological and human strategies must be employed in the development of an information security awareness (ISA) program. By creating a positive culture that promotes desired security behavior through appropriate technology, security policies, and an understanding of human motivations, ISA programs have been the norm for organizational end-user risk mitigation for a number of years (Peltier, 2013; Tsohou, Karyda, Kokolakis, & Kiountouzis, 2015; Vroom & Solms, 2004). By studying the human factors that increase security risks, more effective security frameworks can be implemented. This study focused on testing the effectiveness of ISA programs on end-user security behavior.

The study included the responses of 99/400 employees at a mid-size corporation. The theory of planned behavior was used as model to measure the results of the tool. Unfortunately, while data collected indicated that ISA does cause change in security behavior, the data also showed no significance. Thus, we fail to reject the null hypothesis.

Table of Contents

List of Tables

Table Page

List of Figures

Figure Page

Chapter I: Introduction

Abundant research suggests that individual users play a critical role in the security of information systems and that no solution can be solely based in technology (Brdiczka et al., 2012; Crossler et al., 2013; Dhillon, Syed, & Pedron, 2016; Hsu, Shih, Hung, & Lowry, 2015). Cybercriminals (aka hackers) typically employ well-known social engineering tricks (the act of persuading users into careless security behaviors) such as malware, email phishing, and other behavior-related tactics in order to circumvent technical security solutions (Mann, 2012). Such "social engineering" continues to plague end-users, despite the existence of a breadth of information and countermeasures that help promote prudent security behavior (Furnell & Moore, 2014). It follows that informed awareness and an understanding of the types of behaviors that compromise security are key ingredients for a successful risk-mitigation program (Goodhue & Straub, 1991; Siponen & Oinas-Kukkonen, 2007; Viduto, Maple, Huang, & López-Peréz, 2012).

Both technological and human strategies must be employed in the development of an information security awareness (ISA) program. By creating a positive culture that promotes desired security behavior through appropriate technology, security policies, and an understanding of human motivations, ISA programs have been the norm for organizational end-user risk mitigation for a number of years (Peltier, 2013; Tsohou, Karyda, Kokolakis, & Kiountouzis, 2015; Vroom & Solms, 2004). It is therefore interesting to analyze whether ISA programs are effective in building desired end-user security behavior and whether they deliver on the promise of more secure user actions within the organization.

As accessibility to data increases, so does the need to increase security. For organizations of all sizes, information security (IS) has become paramount due to the increased use of the Internet. Corporate data are transmitted ubiquitously over wireless networks and have increased exponentially with cloud computing and growing end-user demand. This swing can be seen in the vast increase in the number of cybercrime-related incidents in the past few years. According to Brahme and Joshi (2013), cybercrime increased steadily every year from 1998 to 2013, with IS events peaking at over 3.5 million reported incidents in 2013. IS seeks to protect data under the confidentiality, integrity, and availability (CIA) model that has been in place since 1969 (Howe, 1978) and which is still used as a framework for today's security programs (Younis & Kifyat, 2013).

The three tenets of the CIA model embrace both technological and behavioral components of security: Confidentiality allows information to be used or seen only by intended targets; integrity dictates that data will be unchanged between author and consumer; and availability ensures that systems are up and able to provide information when called upon (Whitman & Mattord, 2011). The large majority of risk mitigation strategies are built on the CIA framework, and current research focuses more on the human components of the model (Alfawaz, Nelson, & Mohannak, 2010). This focus on human factors strays from the more traditional technological approach toward security.

A technologically-driven philosophy of cyber security is grounded in the theory that innovative technology builds stronger defenses against data loss and that human error can be curbed with deterrence. However, it has been shown that an organization's dependence upon deterrence and technical solutions to alleviate security risk is a vast oversight, as other human behavioral factors must be considered (Balcerek, Frankowski, Kwiecień, Smutnicki, & Teodorczyk, 2012; Crossler et al., 2013; Hu et al., 2011), and research that focuses on secure end-user habits is increasing (Alfawaz et al., 2010; Siponen, Mahmood, & Pahnil, 2014).

Such an approach proactively compensates for the many unanticipated factors (born in human carelessness) that compromise security and for which technology continues to fall short.

For instance, the problem with a penalty deterrent model is that it assumes all security attacks are done with malicious intent, ignoring the capricious idiosyncrasies of accidental events (D’Arcy, Hovav, & Goalletta. 2011; Desman, 2013; Guo, Yuan, Archer, & Connelly. 2011). A better solution is to develop an ISA program creating a culture of security awareness by combining technology, security policy, and an understanding of human behavior. Increasing employee awareness of how to protect data in both technical and human terms has been found to be the best risk-mitigation strategy within an organization, reducing the need, cost, and frustration of planning for every conceivable contingency (Bulgurcu et al., 2010; D’Arcy et al., 2009; Pahnila, Karjalainen, & Siponen, 2013). With these factors in mind, ISA would seem to be a more sensible alternative to the traditional technologically-driven approach to cybersecurity.

Abundant research supports the use of ISA as an effective method for risk-management programs (Ciampia, 2103; Mylonas, Kastania, & Gritzalis, 2013; Peltier, 2013), but research is lacking as to whether it truly promotes secure end-user habits. There is little to no research that looks at data loss, accidental or malicious, and how it relates to the habitual tendencies of end-users as moderated by ISA in mid-sized organizations. More specifically, it would be beneficial to the future of cybersecurity to analyze ISA’s contribution to information security risks and human factors in the corporate environment. By shedding light on the human factors that increase security risks, more effective security frameworks can be implemented hand in hand with the development of risk-mitigation strategies (Lin, 2010; Siponen et al., 2014; Whittman & Mattford, 2011). Such an analysis would seem to be critical toward understanding the true potential of ISA in effectively deterring cyber-attacks in the corporate setting.

Another factor that must be considered is that different-sized organizations require different security solutions. Since organizations vary greatly in staff size, budget, and culture, they present many of their own characteristic security challenges. This particular study will review cyber security in a single midsize organization and thus create a tool to measure the effects of ISA programs in other midsize organizations. A midsize company is defined by Gartner (2014), the leading IT analytics and metric organization in the world, as one that has 100–999 employees (end-users) with annual revenue of more than $50 million but less than $1 billion. An end-user is defined as the person for whom a hardware or software solution is designed. The terms *organization* and *company* will be treated with equal meaning in this document.

Organizational security behavior, or security hygiene, is the set of information data protection expectations that a company places on the end-user as part of security practice. A security event is a change from the operational norm of information systems or services that violates typical security policy, safeguards, or technology (Whittman & Mattford, 2011). As a consequence, technical and human security controls vary with the number of end-users and the type of data to be secured (Vroom & Von Solms, 2004). However, end-users of digital data do share similar security concerns, regardless of the size of an organization or the type of data, since data loss in any organization could be catastrophic (Whittman & Mattford, 2011). Hence, tactics for diligent planning and the constant assessment of behavioral traits that compromise company security would translate well to any company size or setting.

This study will extend Ajzen’s (1985) theory of planned behavior (TPB) to study the effect of ISA on end-user behaviors. Ajzen’s research found that by finding an individual’s intention, one could, in turn, predict behavior. A survey will collect data on the three main constructs (Fig 1) of TPB for a single midsize company that deploys an ISA program as a part of its security strategy. The results of the research will be limited to the company in question, as all ISA programs are deployed with some variation. The tool, however, could be used as a predictor of all midsize companies.

TPB constructs include attitude toward behavior (ATT), subjective norm (SN), and perceived behavioral control (PBC; Ajzen, 1985). ATT is a measure of how important the behavior in question is to the individual and is formed from Davis’s (1989) technology acceptance model, specifically ease of use and perceived usefulness. SN is a social measurement that examines the social burden (driven by peer and supervisor influences) to perform or not perform a certain behavior. PBC is built upon Bandura’s (1977) tested and proven theory of perceived self-efficacy being a key foundation to behavior (Ajzen, 1980, 1985).

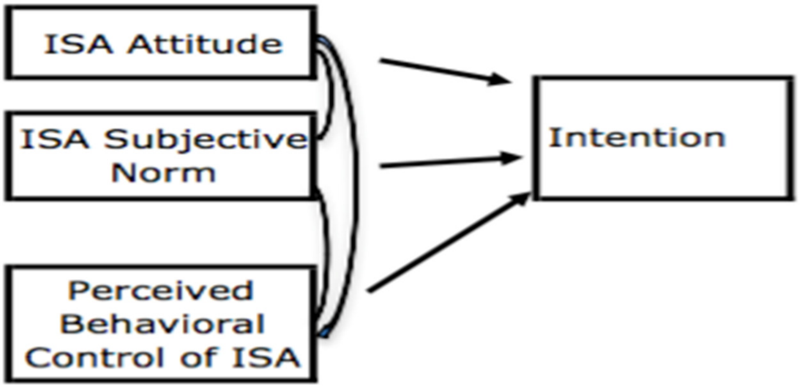


Figure 1. Construct of Ajzen’s TPB theory.

When data loss occurs from within a company, experts categorize it as an internal threat. Internal threats come in two major forms—intentional harm and misuse—but both forms result in data loss and/or service outage (Siponen, Mahmood, & Pahnil, 2014). Predictably, the nomenclature used to describe an organization's actions to mitigate threats describes *defensive* measures, while attacks, either intentional or unintentional, are described and classified as *offensive* threats (Lin, 2010). Table 1 describes some current tactics that companies use to deter internal threats, including end-user behavioral measures and ISA, the focus of this research (Ahmad, Maynard, & Park, 2012; Whitman & Mattord, 2013). Table 1 illustrates broad organizational *defense* tactics that preceded end-user security measures.

Table 1

Definitions of ISA Strategies

Information Security Awareness	**Operational measurement**
Organizational Information Security technology deployed: hardware/software tools used to mitigate security events	End-user awareness of installed technology such as firewalls, intrusion detection, access controls, and other deployed tools.
Organizational Information Security awareness/culture: the security culture of the organization	End-user awareness of corporate security environment. Is security an "all" corporate norm, or the responsibility of few?
Organizational Information Security knowledge: knowledge level of security topics (the other constructs)	End-user understanding and knowledge of organizational security tools and techniques.
Security Self-efficacy: the end-users own self-confidence to be and act securely	End-user knowledge of how security tools work, attack and defend techniques, and organizational risk structure.
Policy, Governance, and Compliance: An integrated approach used by corporations to act in accordance with the guidelines set for each data and system protection within given vertical markets.	End-user knowledge of security policy & guidelines that are deployed at a given organization
Benign detrimental security behavior: Unintentional behavior which could lead, or has led, to a security event.	User survey response on behavioral practice in information security * End-user resistance to social engineering * End-user data privacy, use of encryption * End-user handling of virus/malware

Background of the Study

Current research demonstrates that security is not simply a technology problem but is primarily a people problem caused by malicious intent, carelessness, or accident (Desman, 2013; Kim, Lee, Chun, & Benbasat, 2014; Peltier, 2013; Whitman & Mattord, 2013). For example, in January 2013, *The Wall Street Journal* reported on a malicious insider event by which 150 million private records containing social security numbers, financial information, and other private data had been stolen by four employees from the database servers of Dun and Bradstreet and sold for profit (Chu, 2013). In another example of malicious insider behavior leading to extreme data loss, DatalossDB.org (2014) reported that credentials for 104 million credit cards were stolen from the Korean Credit Bureau from inside employees and were later used to purchase more than $20 million worth of goods. In an example of accidental loss, the State of Texas released the social security numbers of 6.5 million registered voters in 2012 (DatalossDB.org, 2013). In 2011, the Texas Comptroller of Public Schools accidentally exposed 3.5 million teacher records that included salary, social security numbers, and other sensitive data to the public Internet (Shannon, 2011). There are literally thousands of such reports of data loss that range from small to large company security issues (DatalossDB.org, 2013). In the majority of cases, data loss can be attributed to human error or malicious intent (Spears & Barki, 2010). For this reason, research into the effectiveness of ISA on end-users and the promotion of a cyber-secure working environment would prove beneficial toward preventing such unfortunate occurrences.

Because information security can be rooted in human behavior (D’arcy et al., 2009), it is subject to the psychological and sociological behavior of the people who are associated with it (Ahmed et al., 2012). It is widely accepted that a strong ISA program solidifies the bridge between end-users and technology (Ahmad et al., 2012; Balcerek et al., 2012; Desman, 2013). However, a company that has innovative technology and a good security policy in place is still subject to the end-user’s willingness and ability to follow the policy (Peltier, 2011). Even with the growing implementation of such policies, end-user operational behavior remains the single greatest factor that increases information security risk (Alfawaz et al., 2012; Crossler et al., 2013; Tamjidyamcholo et al., 2010). Therefore, understanding the effectiveness of ISA in risk management and how it relates to human tendencies serves a vital need in the modern, information-centric world.

End-user behavior can be broken into two broad categories: intentional and accidental harm. One predictor of behavior that leads to both categories is the self-efficacy, or perceived behavioral control, of the end-user to practice good security hygiene. Figure 2 outlines the two-factor taxonomy of behavioral information security and illustrates that user expertise and intent are critical factors in its success (Stanton, Stam, Mastrangelo, & Jolton, 2005).

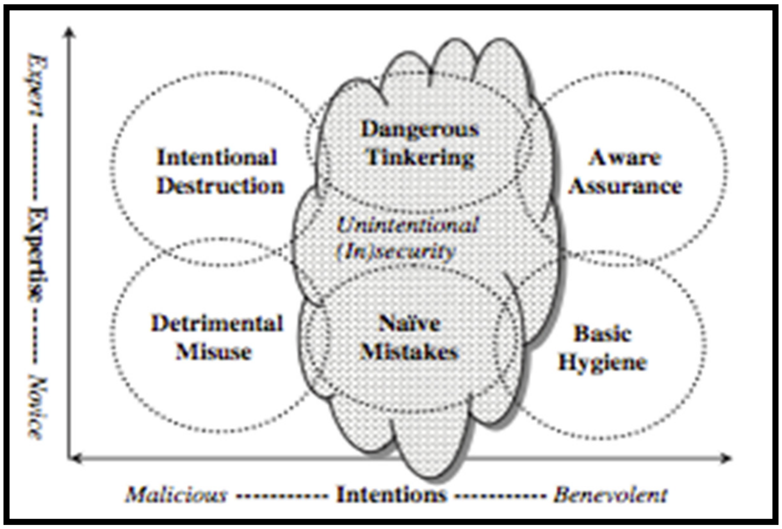

Expert ------- Expertise ------ Novice
Intentional Destruction
Dangerous Tinkering
Aware Assurance
Unintentional (In)security
Detrimental Misuse
Naïve Mistakes
Basic Hygiene
Malicious ---------- Intentions ---------- Benevolent

Figure 2. Illustration of the intersection of security expertise and intention. Reprinted from “Analysis of end user security behaviors,” by J. M. Stanton et al., 2005, *Computers & Security*, 24(2), 124-133.

This illustration demonstrates how a person's level of experience and expertise can promote certain intentions, running the gamut from intentional destruction to naïve mistakes. Expertise and intention are both variables independent to the dependent variable (in)security. Also in this illustration careful attention is paid to the level of loss, and the focus is on both internal and external threats; an attacker who is expertly trained and malicious in intent causes the most damage from intentional destruction. Therefore, perceived behavioral control, or self-efficacy, is a critical determinant in estimating how human behavior relates to ISA risk management.

By building on the research of psychosocial behavior (Stanton et al., 2005) and leveraging established TPB tools (Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1975), this study aims to provide data to help mitigate security attacks through the illumination of relevant human behavior. As mentioned previously, a construct of TPB is ATT, the attitude that a person takes toward desired behavior. The concept of ATT can be seen in two separate cases at the University of Washington Medical Center, with data loss stemming from both benevolent and malicious intent (www.datalossdb.org, 2014). In the first issue, an employee at a debt collection company working on behalf of the hospital intentionally, and maliciously, violated security protocol and stole financial information from patient records. The individual recorded patient credit card numbers as they were used for payment of services. In the second case, at the same medical center, x-rays and patient DVDs were found in furniture sold at a surplus auction and were determined to have accidentally been left behind by the previous user of the desk. The person's attitude toward security policies was diametrically opposed in these cases, but the result was the same: loss of sensitive data. In the first case, the individual may have adopted an attitude that the reward outweighed the penalty, in that sufficient punitive and/or technological deterrents were lacking in the company’s ISA policies. In the second case, the individual’s low-level awareness of or concern for the consequences resulted in a breach of ISA policies. Both cases illustrate fundamental attitudes toward externally desired behavior, where social pressures conflict with subjective norms, and how information security challenges can be met by predicting when such human behaviors are likely to occur through ISA risk-management policies.

Importance of the Study

Data loss resulting from internal human sources is on the rise and must be studied from all angles to mitigate it (Takebayashi et al., 2010). Data loss can lead to lost revenue, lost jobs, lack of trust in essential digital processes, and even lost identity. Therefore, understanding and investigating the causes of end-user behavior is critical to finding a successful mitigation strategy for data loss. ISA is the widely accepted strategy for end-user security behavior, and TPB is broadly accepted as a tool for predicting behavior (Ahmad et al., 2012; Aurigemma & Panko, 2012; Whitman & Mattord, 2013). Thus, by using TPB to understand the effectiveness of ISA programs, new security methods, frameworks, technologies, and policies may be discovered to help mitigate worldwide data loss.

Statement of the Problem

The solution to preventing data loss comprises both technological and human factors. Too-heavy reliance upon technological deterrents, as the demand for information and its transmission has increased, has, in turn, increased the exposure of sensitive data to cyber security risks. Since ISA programs are widely accepted as the primary tool for mitigating end-user security risks, researching the effectiveness of ISA in developing appropriate end-user security behavior is critical to developing new security methods, frameworks, technologies, and policies.

Objective of the Study

The objective of this study is to investigate the effectiveness of ISA on end-user security behavior using the TPB model in midsize corporations. Data loss is traditionally viewed as a technically-oriented problem, but current research indicates that most data loss events are rooted in human behavior (Alfawaz et al., 2010; Siponen, Mahmood, & Pahnil, 2014). Research on end-user security behavior (ESB) is prevalent in the security field (Altawaz et al., 2010; Balcerek et al., 2012; Stanton et al., 2005; Takebayashi et al., 2010; Tamjidyamcholo et al., 2013), but knowledge of the effectiveness of ISA on ESB is incomplete and deserves exploration.

The resulting data will help form new security frameworks, policies, training regimes, and tools for measuring the effectiveness of ISA on ESB in midsize organizations.

Research Questions

1. How effective are ISA programs in influencing end-user security intention (SI)?
2. To what extent does attitude (ATT) toward ISA programs significantly influence SI?
3. To what extent does the subjective norm (SN) of ISA programs significantly influence SI?
4. To what extent does perceived behavioral control (PBC) of ISA significantly influence SI?

Research Hypotheses

H_0: There is no significant relationship between ISA and security behavior.

H_1: There is a significant relationship between ISA and security behavior.

H_{2a}. There is a positive relationship between end-users' perceived ease of use of ISA and the attitude toward security behavior.

H_{2b}. There is a positive relationship between the end-users' perceived usefulness of ISA and the attitude toward security behavior.

H_3a There is a significant relationship between the end-users perceived peer influence on ISA and the attitude toward security behavior.

H_{3b} There is a significant relationship between the end-users perceived supervisor influence on ISA and the attitude toward security behavior.

H_4 There is a significant influence of ISA ATT on end-user intention (behavior)

H_5 There is a significant influence of ISA SN on end-user intention (behavior)

H_6 There is a significant influence of ISA PBC on end-user intention (behavior)

Figure 3 illustrates the constructs of TPB and they will be applied in this study of the effectiveness of ISA on secure behavior. Ease of use and perceived usefulness are both antecedents to attitude. Peer and supervisor influence are antecedents to subjective norm. ISA self-efficacy and tool self-efficacy are both antecedents to behavioral control (Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1975; Davis, 1989).

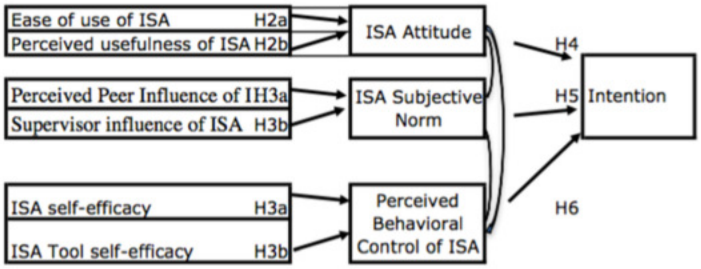

Ease of use of ISA H2a
Perceived usefulness of ISA H2b
ISA Attitude
H4
Perceived Peer Influence of I H3a
Supervisor influence of ISA H3b
ISA Subjective Norm
H5
Intention
ISA self-efficacy H3a
ISA Tool self-efficacy H3b
Perceived Behavioral Control of ISA
H6

Figure 3. Illustration of the study hypotheses (Banfield, 2016).

Assumptions

1. Individuals responding to the survey will answer honestly.
2. Security mangers will provide honest data on security programs and training within their respective organizations.
3. The expert panel will be unbiased and participate openly and honestly.

Limitations and Delimitations

Limitations. All aspects of security behavior could not be fully encompassed in this research due to the breadth of topic. Thus, caution should be used as to the generalization of this research. Fatigue may play a factor in the survey response, so the number of survey questions was held to a minimum. Another issue is that end-users may not be willing to share information about their security intentions (Straub, 1986).

Delimitations. To make the data collected more manageable, a Likert scale was used, and open-ended questions will be avoided. The study cannot be generalized, as the survey population is a single company.

Definitions

Access: An end-user's ability to use, manipulate, modify, or affect another subject or object. Authorized users have legal access to a system, whereas hackers have illegal access to a system. Access controls regulate this ability (Whitman & Mattord, 2011).

Asset: The company resource that is being protected. An asset can be logical (a website, information, data) or physical (i.e., a person, computer system, or other tangible object). Assets, and particularly information assets, are the focus of security efforts; they are what those efforts are attempting to protect.

Attack: An intentional or unintentional act that can cause damage to, or otherwise compromise, information and/or the systems that support it. Attacks can be active or passive, intentional or unintentional, and direct or indirect.

Best practice: A norm accepted as the best method for accomplishing an information system objective.

Defense-in-depth: Best practice method for layering information technology hardware, software, policy, and people in an effort to mitigate the risk of data loss.

End-user: The person by whom hardware or software technology solutions are designed to be used.

Exploit: A technique used to compromise a system. This term can be a verb or a noun. Threat agents may attempt to exploit a system or other information asset by using it illegally for their personal gain, or an exploit can be a documented process to take advantage of a vulnerability or exposure, usually in software, that is either inherent in the software or is created by the attacker.

Exposure: A condition or state of being exposed. In information security, exposure exists when a vulnerability known to an attacker is present.

Information Security: An official organizational program with the goal of training users about the potential threats to an organization's information and how to avoid and behave in these situations.

Information Security Awareness: A formal process for educating end-users about computer security and organizational security practice. A good security awareness program should educate end-users about specific expectations and behaviors that they are held accountable for.

Internal Security Event: A change from the operational norm of information systems or services that is identified as a violation of a security policy, safeguard, or technology.

Loss: An unintended instance of an information asset suffering damage through unauthorized modification or disclosure.

Organizational Information Security Awareness/Culture: The security postures, policies, and culture of an organization.

Organizational Information Security Knowledge: The knowledge level of an organization’s security topics and its specific training in risk mitigation.

Organizational Information Security Technology Deployed: Hardware/software tools used to mitigate security events

Protection Profile or Security Posture: The entire set of controls and safeguards, including policy, education, training and awareness, and technology that an organization implements (or fails to implement) to protect the asset.

Risk: The probability that something unwanted will happen. Companies must minimize risk to match their risk appetite—the quantity and nature of risk the organization is willing to accept.

Security Self-efficacy: The end-users’ own self-confidence to be secure and act in a secure manner.

Subjects and Objects: A computer can be either the subject of an attack (an agent entity used to conduct the attack) or the object of an attack (the target entity).

Theory of Planned Behavior (TPB): A psychological tool used to predict an individual's intention to engage in a behavior at a specific time and place. It is built on the following constructs:

1. Attitude toward behavior (ATT) is a measure of how important the behavior in question is to the individual.
2. Subjective norm (SN) is a social measurement that examines the social burden to perform or not perform the behavior.
3. Perceived behavior control (PBC) is built upon Bandura's tested and proven theory of perceived self-efficacy being a key foundation to behavior (Ajzen, 1985; Bandura, 1977).

Threat: A category of objects, persons, or other entities that presents a danger to an asset. Threats are always present and can be purposeful or undirected. For example, hackers purposefully threaten unprotected information systems, while severe storms incidentally threaten buildings and their contents.

Vulnerability: A weakness or fault in a system that opens it to attack or damage.

Summary

Chapter 1 is an introduction to the research that encompasses the study. It consists of the purpose of the study, the importance and significance of the study, the research questions/hypothesizes, and research objectives. This section also provided brief information about ISA and TPB. This study will define the role ISA plays in security behavior, thus allowing the development of new security frameworks, tools, and research to mitigate security events.

Chapter II: Literature Review

Introduction

The purpose of this literature review is to summarize the existing research closely related to the research aim of this study. Data loss at the hand of internal end-users in midsize companies is increasing (Alfawaz et al., 2010; Siponen, Mahmood, & Pahnil, 2014) and is usually combated with information security awareness (ISA) programs (Brdiczka et al., 2012; Crossler et al., 2013; Dhillon, Syed, & Pedron, 2016; Hsu et al., 2015). To study the effectiveness of ISA on behavior, the research was constructed around the theory of planned behavior (TPB).

Information Security Awareness (ISA)

The creation of information security policies, standards, procedures, and guidelines is only the beginning of an effective information security program. Technology plays a role but is not as effective as a trained work force (Brdiczka et al., 2012; Crossler et al., 2013; Hsu et al., 2015; Dhillon et al., 2016). A well-built technical security architecture will be rendered less effective if there is no process in place to make certain that the end-users are made aware of their responsibilities with regard to information assets (Crossler et al., 2013). An ISA program encompasses end-user awareness, education, and training programs to address security practices, policies, and tools.

Security policy is the bedrock of an ISA program as it establishes practice, sets boundaries, and creates desired behavior. In most organizations, security policy guidelines and implementations are the responsibility of the information technology (IT) department and often a security executive. In particular, a security policy consists of a set of rules and practices that control how an organization protects and distributes its key information assets, striking a balance between security and usability (Safa et al., 2012). According to Peltier (2013), a good security policy dictates user responsibility, threat reporting, identification of key information security personal, and deterrents for violations. Specifically, Peltier offers the following five major components of a good security and risk management policy:

1. Physical Security
    a. Offices secured
    b. Desks and cabinets secured
    c. Workstations secured
    d. Information secured following CIA practice
2. Roles and Responsibilities
    a. Who has responsibility for what
    b. What is expected of end-users
    c. How do different groups within the organization interact (communication plan)
    d. Spell out accountabilities
3. Technical Securities
    a. Wireless security
    b. Wired security
    c. Virtual private networks
    d. Access control
    e. Identity management
    f. Virus/Malware protection
    g. Secure application architecture
        i. Email security
        ii. Web application security
        iii. Privacy policy
    h. Vendor security
    i. Firewall IDS/IPS management
4. Incident management
    a. Incident response
    b. Network security monitoring and policy enforcement
    c. Data classification
    d. Acceptable use policy
    e. Communication plan
5. Deterrent
    a. Training and education
    b. Violation schedule
    c. Access alarms
    d. Due diligence reporting of suspicious activity

Security policy is used to create the culture of security for an organization and establishes the ISA (Alhogail, 2015; Hassan, 2015; Kearney & Kruger, 2016). From the ISA, both desired end-user security behavior and undesired misbehavior is accounted for.

Security Misbehavior

Security misbehavior can be broadly defined as the set of end-users who violate organizational security policy, which leads to the loss of organizational assets. Users who engage in intentional misbehavior are either out for profit and/or destruction and are labeled intentional malicious insiders. End-users who unintentionally neglect to follow policy and engage in behaviors that result in asset loss or risk are categorized as unintentional insider threats (Whitman & Mattord, 2011).

Inappropriate modification of data, altering access to data and the availability of systems, copying software, selling organizational IP property, and stealing corporate data as they leave for other jobs are a few examples of *intentional* undesired behaviors. While a strong ISA program won't bring these behaviors to a 100% stop, a weak ISA program could lead to such behavior (Siponen, 2014). *Unintentional* undesired behavior such as understanding and being capable of following security policy and practice but failing to do so can also lead to loss of organizational assets (Guo, 2010). Unintentional undesired behavior can also be caused by lack of knowledge or efficacy. At the core of both intentional and unintentional loss, a weak ISA program can usually be found. Conversely, security-trained and educated end-users who have a clear understanding of their responsibilities help to create a strong ISA (Peltier, 2013; Tsohou et al., 2015; Vroom & Solms, 2004).

In the literature on security, several terms have been proposed to describe "bad" behaviors that are regarded undesirable and "good" behaviors that are seen as desired from an organizational perspective. Such terms include *compliance, governance, computer abuse, hacking, system misuse,* and *inappropriate computer use* (Guo, 2010). Desired behaviors are the aim of ISA programs, since they represent actions that are deemed beneficial to the organization. Reporting security policy violations and following security policy are two such desired behaviors related to compliance (Ghaisas et al., 2015; Hendre & Joshi, 2015; Vance & Siponen, 2012). End-users must understand their roles and responsibilities in protecting organizational assets and how to respond to any potential threat. To make this undertaking easier, ISA programs should focus on educating and training users on how to effectively protect information assets.

This study to evaluated the effectiveness of ISA programs are in predicting desired behavior. The literature review illustrated that the common tool to mitigate human security issues is an ISA. This study then examined exactly how ISA programs can be a predictor of behavior using TPB.

Theory of Planned Behavior (TPB)

TPB has long been accepted as a framework and proven successful in predicting and explaining behavior across multiple domains of study. It examines attitude, norm, and control as determinants for an individual’s intention to perform a specific behavior (Ajzen, 1980, 1985). TPB was extended from the theory of reasoned action and proposes three constructs of intention (Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1975):

TPB construct 1: Attitude toward Behavior, Perceived Usefulness / Ease of use

> According to Davis (1989), people have many reasons to use or decline information technology. They may choose to use technology if they believe it will help them with their work: a so-called “perceived usefulness.” On the other hand, people may find

technology to be useful but difficult to use and balk before its daunting “ease of use.” Both determinants (i.e. “perceived usefulness” and “ease of use”) serve to influence an end-user’s attitude and behavior concerning technology. Liaw and Huang (2013) applied the theory of perceived usefulness to the adoption of e-learning environments. In their study, they found that the more difficult an interface was to e-learning, the less likely students were to follow complete instruction sets. They also used ease of use as a functionality to investigate self-regulating behavior and e-learning.

TPB construct 2: Subjective norm, Peer/Supervisor social pressure

Cheng et al. (2013) studied the impact of social control and deterrence theory on security violations within an organization. Their research found that social pressure exerted by subjective norms influenced employee security policy violations and can be in the form of peer or supervisor pressure. This finding was similar to the findings of Ifinedo (2013), who found that social bonds formed at work have tremendous influence on security policy compliance and subjective norms.

TPB Construct 3: Perceived Behavioral Control, An individual’s self-evaluation of ease toward performing a particular behavior

Johnston et al. (2016) researched security behaviors in organizations and found PBC to have a major influence on security compliance. Users were asked about following security policy for their organization, and a significant cross-section of the 317 workers questioned reported that they lacked the confidence to follow every security policy. The researchers then provided a fictional case study and discovered, with statistical significance, that these same people lacking confidence also failed to follow security policy in some cases.

Attitude Toward Behavior (ATT)

ATT is the TPB construct that measures an individual’s judgment of the importance of a particular behavior. The research in this study focuses on the end-user ATT of an ISA program and the behaviors that lead to compliance of information security guidelines, practices, and policies. Current behavioral research in information security relies heavily on attitude as a precursor to behavior.

Hu, Kuamg, Lu, and Wu (2014) used ATT in the study of software piracy in China and the United States. The hypothesis of the research was that the attitude toward software privacy was positively related to piracy intent. Specifically, they analyzed software cost, punishment severity, and punishment certainty as antecedents to attitudes that subsequently contribute to intent. Not only did the study find that the antecedents influence attitude, but they also found that attitude had the largest influence on piracy intent.

Siponen, Mahmood, and Pahinila (2014) performed a field study that found that security compliance was positively influenced by attitude and that attitude could be cultivated into a culture by executive-level influence.

The technology acceptance model (TAM) holds two constructs that are clear antecedents to ATT. Perceived ease of use, which is defined as the user’s perceived level of effort needed in a given system, and perceived usefulness, which is defined as the level at which a user perceives a system would enhance job performance (David, 1989). Chueng and Vogel (2013) used an extension of TAM to predict a user’s behavioral acceptance of collaborative technologies.

Subjective Norm (SN)

SN refers to the perceived social pressures to carry out or not perform a given action (Ajzen, 1985). ISA programs depend upon creating a culture of security behavior for their success, stemming from executives and supervisors insisting on and prioritizing appropriate security behavior (Aurigemma & Panko, 2012). Boss, Kirsch, Angermeier, Shingler, and Boss (2009) developed a model to explain end-user information security behavior. They found that when end-users perceive security policies to be mandatory, the motivation to adopt good security behavior increases. They also noted that if end-users believe organizational leaders are monitoring their actions, they will be more likely to comply. This shows how SN pressure and culture, promoted by the watchful direction of proactive supervisors, can change the perspectives of end-users who may be somewhat apathetic to information security.

Top management thus plays a proactive role in end-user compliance to security policies and organizational culture (Hu, Dinev, Hart, & Cooke, 2012). The research done here illustrates the impact that SN and PBC can have on end-user intentions. Ifinedo (2012) surveyed 124 business managers and information system professionals and found that PBC, ATT, and SN positively influenced end-user security policy compliance.

Self-Efficacy (SE) or Perceived Behavioral Control (PBC)

Perceived behavioral control as defined by TPB can be measured in self-efficacy (SE) (Ajzen 1980, 1985). SE theory has been applied to understand the process of gaining and the importance of confidence in many domains of behavior such as learning, achievement, career choice, and the ability to persevere through tough situations (Bandura 1977, 1982, 1986, 1989, 2006). Bandura (1986) uses an understanding of SE to formulate his social cognitive theory and argues that behavior is composed of positive and negative reinforcement, modeling the behavior of others, and self-correction built upon performance feedback (Bandura, 1977). Motivation to complete a task is embedded in cognitive activity and behavior due to the individual's perception of the future consequences of the action (1989). This cognitive activity is stated as SE, which is defined as "the conviction that one can successfully execute the behavior required to produce the [desired] outcomes" (1977).

Individuals with a strong sense of efficacy are more likely to challenge themselves with difficult tasks and be intrinsically motivated (Bandura, 1986; Margolis & Cabe, 2006). These individuals will put forth a high degree of effort in order to meet their obligations and rebound quickly from setbacks, which makes them more likely to achieve personal goals. On the other hand, individuals with low self-efficacy believe that they cannot be successful. They are less likely to put forth a rigorous, prolonged effort and may consider challenging tasks as threats to be ignored. Since every person has goals or improvements that they wish to make, self-efficacy would appear to be a universal promoter of successful change and action; beyond skills and knowledge, an individual must believe with confidence that a given action will return a desired result and that he or she is capable of performing the action (Bandura, 1977; Caprara, Vecchione, Alessandri, Gerbino, & Barbaranelli, 2011; McKeachie & Svinicki, 2013).

Furthermore, cognitive social theory suggests that successful experiences influence the sense of efficacy, belief, and behavior; in general, successful experience increases SE and negative experience decreases SE (Bandura, 1986). Within the context of information security, negative experiences would include lost data, inability to remove malware, being a victim of a phishing ploy, and fraud. Positive experiences could include avoiding a phishing scam, encrypting data, and managing the integrity of data.

Additionally, general controllability is also a factor in SE. In information security, this can be seen in the end-users' beliefs that an organization adequately deploys technology to protect data from harm (Rhee et al., 2009). In other words, end-users' SE will increase when they believe that the organization for which they work has adequate security practices and technologies in place to protect their data. Conversely, end-user SE decreases when the opposite is true.

It is important to understand the difference between ability and capability in order to understand SE. *Ability* is a derivative of the Latin word *skillful*, which means to be currently able (Bandura, 2006; Vygotsky, 1980). *Ability* refers to proficiency in doing a skill that has already been attained. Therefore, SE for current ability is called "self-efficacy for performance," which is a confidence that one can do a particular task right now. On the contrary, capability refers to the potential to perform a future function not yet learned. Both capability and ability are key ingredients influenced by SE but distinctively different in meaning. For an information security awareness program to be completely successfully, end-users need ability and capability. In ISA both are encouraged through education, training, and organizational culture.

Mahatma Gandi (1939) captured SE and the difference between ability and capability by stating simply, "If I have the belief that I can do it, I shall surely acquire the capacity to do it even if I may not have it at the beginning." SE is centered on perceived capability or a *can do* perspective, while intention is a statement of *will do*. Simply stated, SE is one's own confidence to complete a given task (Bandura, 2006). This research studied the influence that end-user SE has on ISA risk management programs and security behavior.

Many have learned the power of "I think I can!" from Watty Piper's (1930) *The Little*

Engine That Could or, as Henry Ford (n.d.) stated, “Whether you think you can or can’t, you’re usually right.” Both sources are seminal reminders of the power of SE to bring both positive and negative results; individuals with higher levels of SE possess a strong sense of conviction about their abilities to achieve goals (Stajkovic & Luthans, 1998). Much research has been done in many different disciplines using Bandura’s social cognitive theory and SE, including motivation to learn (Zimmerman, 2000), computer use (Compeau & Higgins, 1995), weight loss motivation (Armitage, Norman, Noor, Alganem, & Arden, 2014), and information security (Rhee, Kim, & Ryu, 2009), to name a few. Bandura (1977) was very careful to illustrate that a specific domain, such as security self-efficacy (SSE), must be identified in order to successfully measure self-efficacy and behavior.

Computer Self-Efficacy (CSE) and Security Self-Efficacy (SSE) Domains

Davis, Bagozzi, and Warshaw (1989) first combined Bandura’s theories of self-efficacy and social cognitive theory to computer usage and defined CSE as a person’s own judgment of his or her capability to use a computer. Bandura (1986) pointed out in his research that mastery of a task develops positive SE, whereas failure contributes to reduced SE. Much research has been built upon the CSE theory developed by Davis et al. (1989), such as user adoption of social networks (Lee & Suh, 2013), dissemination of innovative computer technology (Rogers, 2010), and general technology acceptance (Holden & Karsh, 2010).

Using a Likert scale, Compeau and Higgins (1995) developed a tool that has been used by multiple researchers to drive self-efficacy-based studies. Vankatesh, Brown, and Bala (2003) used it to do work on user acceptance of information technology; Maynard, Rapp, and Gilson (2010) used the CSE model to investigate global virtual team effectiveness; and Tan and Teo (2000) constructed a research framework identifying CSE factors that influence the use of internet banking. More recently, Huffman, Whetten, and Huffman (2013) used CSE to study gender roles and technology acceptance in higher education, while Tamjidyamcholo, Bin Baba, Tamjid, and Gholipour (2013) used it to study the role that knowledge-sharing plays on information security within virtual communities.

Without due consideration of the specific domain to be studied, many researchers make the error of reusing existing instruments and fail to recognize that general CSE is inadequate for specialized domains (Marakas, Johnson, & Clay, 2007). Thus, it is imperative to this study to narrow the specific domain to computer security self-efficacy (SSE). SSE is defined as an end-user's confidence in complying with organizational risk mitigation strategies and behavior within the boundaries of good security hygiene (Clarke, 2010; Rhee, Ki, & Ryu, 2009). Because Bandura's social cognitive theory is founded on self-regulating motivation and behavior models, it is well matched for investigating the behaviors individuals have in the field of information security (Rhee et al., 2009). SSE is a new domain that has grown from CSE and extends security research in a new direction (Clarke, 2010). Understanding SSE and the motivational drivers that inspire the confidence in appropriate behavior is critical to the mitigation of security risk.

Rhee et al. (2009) created a variable called self-efficacy in information security (SEIS) to conduct a study using social cognitive theory. The net result of the research showed that merely listing expected behaviors and associated penalties for creating security risk will have a limited impact on effective security mitigation techniques. The authors defined security practice as an individual's two-faceted information security risk management behavior. The first was the individual's use of security software such as anti-virus, anti-malware, and other security tools. The second facet revolved around compliant behavior regarding computer and

Internet use. For them, compliance wasn't governed, referring exclusively to voluntary security behaviors. Examples include the user's willingness to use secure passwords and back up critical data. Their research proceeded from and answered (*in italics*) the following hypotheses:

H1a: Individuals with higher SEIS use more security protection software.
H1b: Individuals with higher SEIS demonstrate more security-conscious behavior.
SEIS significantly influenced users' use of security software and user security behavior.

H2: Individuals with higher SEIS have greater intention to exert more effort to strengthen their information security.
SEIS demonstrated a significant positive relationship with intention to strengthen security effort. Users with higher SEIS were more likely to exert high levels of effort to enhance information security.

H3a: The greater one's experience with a computer and the Internet, the higher is his or her SEIS.

H3b: Security incidents lower SEIS.
Prior experiential influence with SEIS had a positive influence on security. Also, experience with security breaches had a direct negative effect upon SEIS. Both H3a and H3b were found to be true.

H4: As one perceives that information security threats are controllable, his or her own self-efficacy toward information security increases.
The perception that security threats are controllable was found to significantly increase SEIS.

This research into information security seeks to build mainly upon the tenets of Bandura and Rhee et al.'s research.

Marlon Clarke (2010) studied an individual's ability to use encrypted email as his specific measurement in the self-efficacy domain of SSE in his dissertation, *The Role of Self-Efficacy in Computer Security Behavior: Developing the Construct of Computer Security Self-Efficacy.* He also studied other significant factors related to SSE and established their validity through an expert panel. Building upon Clarke's work, new research can be done to identify the necessary precursors to SSE and user security behavior. Specifically, Clarke's tool can be used to measure behavioral constructs relevant to information security such as social engineering, data privacy, virus/malware confidence, security circumvention, data integrity, and intellectual property espionage. Clarke's method is built upon the CSE method developed by Compeau and Higgins (1995) but within the specific domain of SSE.

Other Behavioral Theories

Several other behavioral theories were reviewed that could be applied to information security:

- The *protection motivation theory* focuses on the conditions under which appeals to fear may influence behavior. The theory works off of the human need for self-preservation in the face of threats, their severity, the perceived probability of the event, efficacy of the recommended preventative behavior, and perceived self-efficacy (Rogers, 1975).
- *Deterrence theory* comes from a criminal research background and was used by D'arcy et al. (2009) to statistically confirm a perceived certainty and severity of organizational sanctions in order to reduce information security misuse.
- *Self-determination theory* is a motivational theory that describes an intrinsic human tendency to make choices without external input (Deci & Ryan, 2012). Wall, Palvia, and Lowry (2013) used self-determination theory as one factor in explaining intrinsically-driven behavior within autonomous actions in the field of information security; organizations produce security controls to mitigate harmful autonomous actions while encouraging helpful autonomous actions.
- *Rational choice theory* (RCT) has its background in criminology but can be applied to the field of information security. Vance and Siponen (2012) used RCT to investigate

how an end-user decides to commit a security violation. Ajzen's theory of reasonable action (TRA) was also considered, but the major significance that self-efficacy lent to TRA was to form TPB as a critical component of this research (Madden, Ellen, & Ajzen, 1992).

Within an ISA program, the principles of protection motivation, self-determination, deterrence, and rational choice theories can all be found. In the form of security policy violation penalties and fear of job loss, the underpinnings of deterrence and protection motivation can be found. In the training for acceptable use policies, roles/responsibilities, and incident response, self-determination and rational choice behaviors are formed. As these components are part of the larger ISA, the TPB represents the best fit to measure the effectiveness of the ISA on behavior and also aids in avoiding confounding variables.

ISA Research

Information awareness programs are a critical component of overall information security; technology without ISA is not a fully encompassed plan. The universality of information systems (IS's), along with the ever-increasing need for the systems to be ubiquitous, has resulted in amplified vulnerability to risk. As a result, organizations have advocated for more defensive ISA programs (Mejias, 2012). ISA is commonly defined as an organizational process that aims at educating end-users in its procedures regarding the protection of the digital assets (Takebayashi, Tsuda, Hasebe, & Masuoka, 2013; Wheeler & Swick, 2011; Whitman & Mattord, 2011). As the word *awareness* implies, an ISA program is designed to create an organizational culture of proactive secure computing. In the ongoing effort to secure digital assets, the end-user occupies the role of both friend and foe. Security awareness is a process that seeks to change individual perceptions, values, attitudes, behavior, norms, work habits, and organizational culture and structures in order to secure vital personal information (Tsohou et al., 2015).

Predicting end-user behavior within the domain of information technology has been accomplished in multiple studies (Cheung & Vogel, 2013; Kahn et al., 2011; Mathieson, 1991; Safa et al., 2015). Mathieson's (1991) was one of the first studies that sought to predict end-user intention in the context of information systems. In his research, he compared the technology acceptance model (TAM) and TPB for their ability to predict user intention and how such intention translates into behavior. The research found that both models can be used to predict intention but that TPB provided more specific information. Ifinedo (2012) used the TPB constructs of self-efficacy, attitude, subjective norms, and perceived control, combined with the protection motivational theory, to discover if they positively influence compliance with security policy. Wilson and Warkentin (2013) used TPB to illustrate that deterrence alone is not enough to curb intentional employee computer abuse and that TPB can be used as a predictor, or antecedent, of behavior. Nasri and Charfeddine (2012) studied the behavioral adoption of Internet banking in Tunisia using TPB and TAM, which confirmed the efficacy of the two theories in measuring the problem.

Summary

This chapter was dedicated to developing and supporting Ajzen's theory of planned behavior as a useful tool for measuring the effectiveness of ISA programs on end-user behavior. The three constructs of PBC, ATT, and SN were explained using prior research examples. Last, examples of research using TPB were provided to illustrate its pertinence to the research done in this dissertation.

Chapter III: Methods

Introduction

The purpose of this chapter is to describe the research methods that were employed to study the effectiveness of ISA programs on end-user security behavior. The chapter will discuss the specific steps in the research: research design, population and sample, instrumentation development and design, data collection, data analysis, validation, personnel, budget, and timeline.

Research Design

The research was designed in concert with the organization being studied in order to best protect the respondents and the organization. Another goal of involving the organization was to certify that the data collected would be of later use to their decision-making. The following is a listing of the research design:

1) Sign MOU with organization (appendix A).
2) Develop a survey based upon current research and the literature review.
3) Review questions with a dissertation committee.
4) Review questions with expert panel.
5) Meet and discuss logistics and the survey with the organization.
6) Adjust questions as needed (final copy appendix B).
7) Place questions into an online survey tool.
8) Organization will forward survey link to staff on my behalf (appendix C).
9) Human subjects review (approval in appendix D)
10) Respondents will be given one week to take the survey. A reminder went out on day 4.

11) Data review.

12) Findings and conclusions.

13) Defend dissertation. Upon approval, present/discuss findings with study organization.

Population and Sample

The target population for this study met the Gartner Group definition of a midsize organization (Gartner, 2014). The company in this study has multiple locations, approximately 400 end-users, and revenue of more than $50 million (but less than $1 billion) all under one leadership organization. An ISA program is in place at the company, and respondents who indicated that they had not been organizationally security-trained were removed from the study. The survey population was randomly sampled from a 400 end-user pool. Participant demographic data was classified according to gender, tenure at organization, education, years of computing experience, and other non-identifying background information.

Human Subject Approval

This study sampled a midsize organization in order to study ISA and its behavioral effects. Since the study concerned human behavior, it required review and approval of the EMU Human Subjects Review. The survey contains a very clear consent form, and sample respondents will take it of their own free will (appendix E). Any data that identify the participant or organization will not be collected, since anonymity is critical to the research. To further protect the respondents, a memorandum of understanding (MOU) was signed with the study organization (appendix A). The data were encrypted in processing, transfer, and at rest.

Data Collection/Analysis

The survey will be delivered electronically via SurveyMonkey®, a web-based collection tool. The collected data will then be placed into the Statistical Package for the Social Sciences (SPSS) for analysis. The imported data will then be vetted to remove nonresponsive answers and respondents who had not had security training. The constructs analyzed in the next section were designed to confirm reliability and validity. A cover letter was included with the survey URL to instruct respondents on their roles, assure them anonymity, and explain the research goals as they relate to data collection.

Validation

According to Straub (1989), instrument validation consists of content validity, construct validity, and reliability. As stated by Straub, Boudreau, and Gefen (2004), "Without solid validation of the tools that are used to gather data on which findings and interpretations are based, the very scientific basis of the profession is threatened." The following portions of this section will explain how this study has met these standards.

Content validity is defined as providing adequate coverage of the subject being studied. This includes measuring the correct items to form constructs that meet the study question (Polit & Beck, 2006). The operational validity of the experimentation was illustrated by a complete literature review and past research. To provide more validity, the survey was presented and altered based upon feedback from two outside sources. The first step was meeting with the organization's Vice President of Technology and Security. This meeting was two-pronged: first, to ensure that the organization was comfortable with the questions asked, and second, to ensure that the survey gathers information that is relevant and helpful to the company. The panel and the organization had similar feedback, as both felt that the survey measured security awareness and that a few of the questions were invalid since employees had no choice but to comply. For example, in one instance the survey asked if the respondent would use complex passwords when, in fact, the installed system does this by default. Consequently, the question was changed to “I am capable of guarding passwords as guided by my organization.” Two members of the panel mentioned that a similar study on security situational awareness would also be helpful and could be included in the study. However, it was decided to not extend the study and to save that research for another time. Such characteristics provided the study with content validity (Straub, Boudreau, & Gefen, 2004). Panel comments can be found in table 2 below.

Table 2

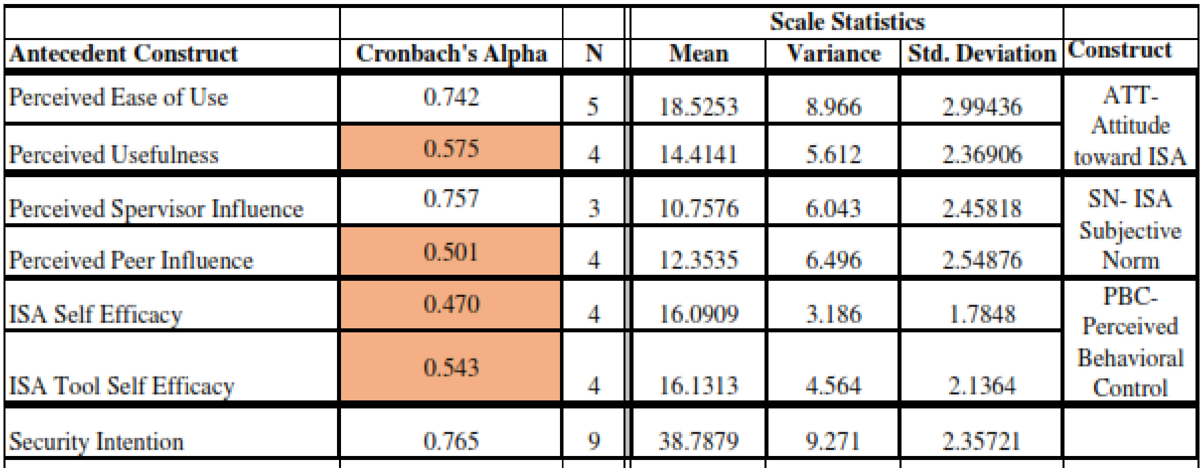
Listing of Security Panel Comments

	Title	Partial listing of comments
Expert 1	Data Security Analyst, Senior	• Some questions out of date • Should mobile security be included • Remove questions that corporate security should handle • Long survey • Definitions of ISA are accurate
Expert 2	Adjunct Professor IA; 15 years corporate experience	• Questions do capture ISA • Questions on survey response (did not know survey was electronic delivery) • Questions are direct an easily read
Expert 3	Security Analyst	• Should you ask if people follow security guidance because it's the right thing to do? • "Shadow IT" – are people working around security policy/tools because it's too difficult • Agrees ISA is captured in questions
Expert 4	Security Engineer	• Agrees ISA is captured in questions • Would like to see a match between ISA and actual performance • Agrees questions are readable
Expert 5	Senior Information Security Intelligence and Forensics	• Agrees survey items will measure ISA • Perhaps more focus on policy and policy awareness could be done

Construct validity is defined as how accurately the experimental method measures the subject of the study. It is paramount that the items that form a construct have high interrelatedness, or internal consistency. A commonly accepted measure of internal consistency is Cronbach's alpha coefficient, when alpha registers 0.7 or above (Park & Chen, 2007; Cronbach & Meehl, 1955). Before executing Cronbach's alpha analysis, corrections were made to reverse-code items that were negatively worded so that a high value indicated the same type of response for every item. Table 3 illustrates that there were reliability problems with the survey, as Cronbach's alpha scores that are marked in orange were not acceptable; removing an item from perceived supervisor influence increased internal consistency.

Table 3

Cronbach Alpha Test for Reliability

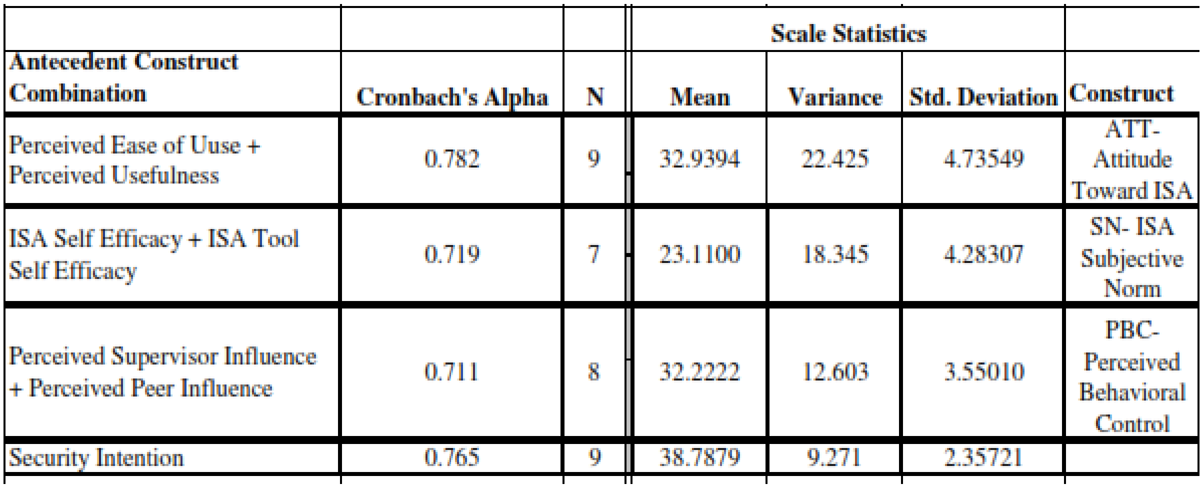


			Scale Statistics			
Antecedent Construct	**Cronbach's Alpha**	**N**	**Mean**	**Variance**	**Std. Deviation**	**Construct**
Perceived Ease of Use	0.742	5	18.5253	8.966	2.99436	ATT- Attitude toward ISA
Perceived Usefulness	0.575	4	14.4141	5.612	2.36906	
Perceived Spervisor Influence	0.757	3	10.7576	6.043	2.45818	SN- ISA Subjective Norm
Perceived Peer Influence	0.501	4	12.3535	6.496	2.54876	
ISA Self Efficacy	0.470	4	16.0909	3.186	1.7848	PBC- Perceived Behavioral Control
ISA Tool Self Efficacy	0.543	4	16.1313	4.564	2.1364	
Security Intention	0.765	9	38.7879	9.271	2.35721	

Other tests for reliability, such as test-retest or inter-rater, were not applicable to this study. A pilot study would have highlighted the issue and provided an opportunity to fine-tune the instrument. While this will be discussed in further detail in the results portion of this document, it is important to note that while the lack of reliability in the research method will result in the failure of one research goal, it does not impact the other. The first research goal of creating an overarching method to measure the effectiveness of ISA programs on end-user security behavior will need further prior research before release. The second research goal of studying the same question within a single organization can still be answered by combining the antecedents in each construct. The newly created variable will have seven items in common instead of four, and reliability increases because the antecedents are closely related. Table 4 illustrates the combined antecedent scores.

Table 4

Combined Antecedent Cronbach Alpha Scores



			Scale Statistics			
Antecedent Construct Combination	**Cronbach's Alpha**	**N**	**Mean**	**Variance**	**Std. Deviation**	**Construct**
Perceived Ease of Uuse + Perceived Usefulness	0.782	9	32.9394	22.425	4.73549	ATT- Attitude Toward ISA
ISA Self Efficacy + ISA Tool Self Efficacy	0.719	7	23.1100	18.345	4.28307	SN- ISA Subjective Norm
Perceived Supervisor Influence + Perceived Peer Influence	0.711	8	32.2222	12.603	3.55010	PBC- Perceived Behavioral Control
Security Intention	0.765	9	38.7879	9.271	2.35721	

Personnel, Budget, and Timeline

The personnel for this study included the expert panel of security professionals, the committee, and the investigator. The cost of SurveyMonkey® was $26/month for the data storage of 400 responses, and this represented the only out-of-pocket expense (www.surveymonkey.com, 2016).

Summary

This chapter presented the overall research procedures and the development of the survey. The survey was discussed in depth and was adapted from extant research. Reliability and validity were discussed and proven acceptable after minor changes.

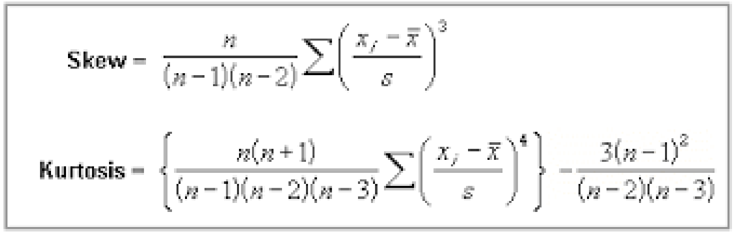
Chapter IV: Results

Introduction

The purpose of this chapter is to provide the detailed statistical analysis collected in the research survey tool. The data were pre-screened for reliability and validity in Chapter III; thus, this section will start with quantitative data analysis. The survey was administered through an online tool and investigated the effects of information security awareness on end-user security behavior in a midsize company. The survey was reviewed by an expert panel composed of several information security experts. The survey population was composed of full-time employees at a local midsize company. The survey was available for response over a one-week period. The organization has requested anonymity in this process.

Normality

Skewness and kurtosis were analyzed to review for normally distributed data and to ensure data statistical assumptions are acceptable (Grinnekk & Unrau, 2005). Using SPSS and the formulas in Figure 4, the test results revealed that some of the data in the main study were skewed outside the normal range of -1 and 1 (Mrdia, 1970). Further, kurtosis of items also ranged outside the acceptable range -1.96 and 1.96 to achieve $p < 0.05$ (NCBI, 2016).



$$\text{Skew} = \frac{n}{(n-1)(n-2)}\sum\left(\frac{x_j-\bar{x}}{s}\right)^3$$

$$\text{Kurtosis} = \left\{\frac{n(n+1)}{(n-1)(n-2)(n-3)}\sum\left(\frac{x_j-\bar{x}}{s}\right)^4\right\} - \frac{3(n-1)^2}{(n-2)(n-3)}$$

Figure 4. Formulas for skewness and kurtosis.

There were five items in total that needed to be transformed. To address these issues, transformations of affected variables were performed using Box-Cox so that assumptions of normality would be acceptable when conducting data analyses (Kline, 2011). After testing for normal distribution in the transformed items, skewness and kurtosis were all acceptable. This is illustrated in table 5 and figure 5 below.

Table 5

Transformed Data

		SN	**PBC**	**ATT**
N	**Valid**	**99**	**99**	**99**
Skewness		-0.166	0.236	-0.019
Std. Error of Skewness		0.243	0.243	0.243
Kurtosis		0.832	-0.453	-0.147
Std. Error of Kurtosis		0.481	0.481	0.481

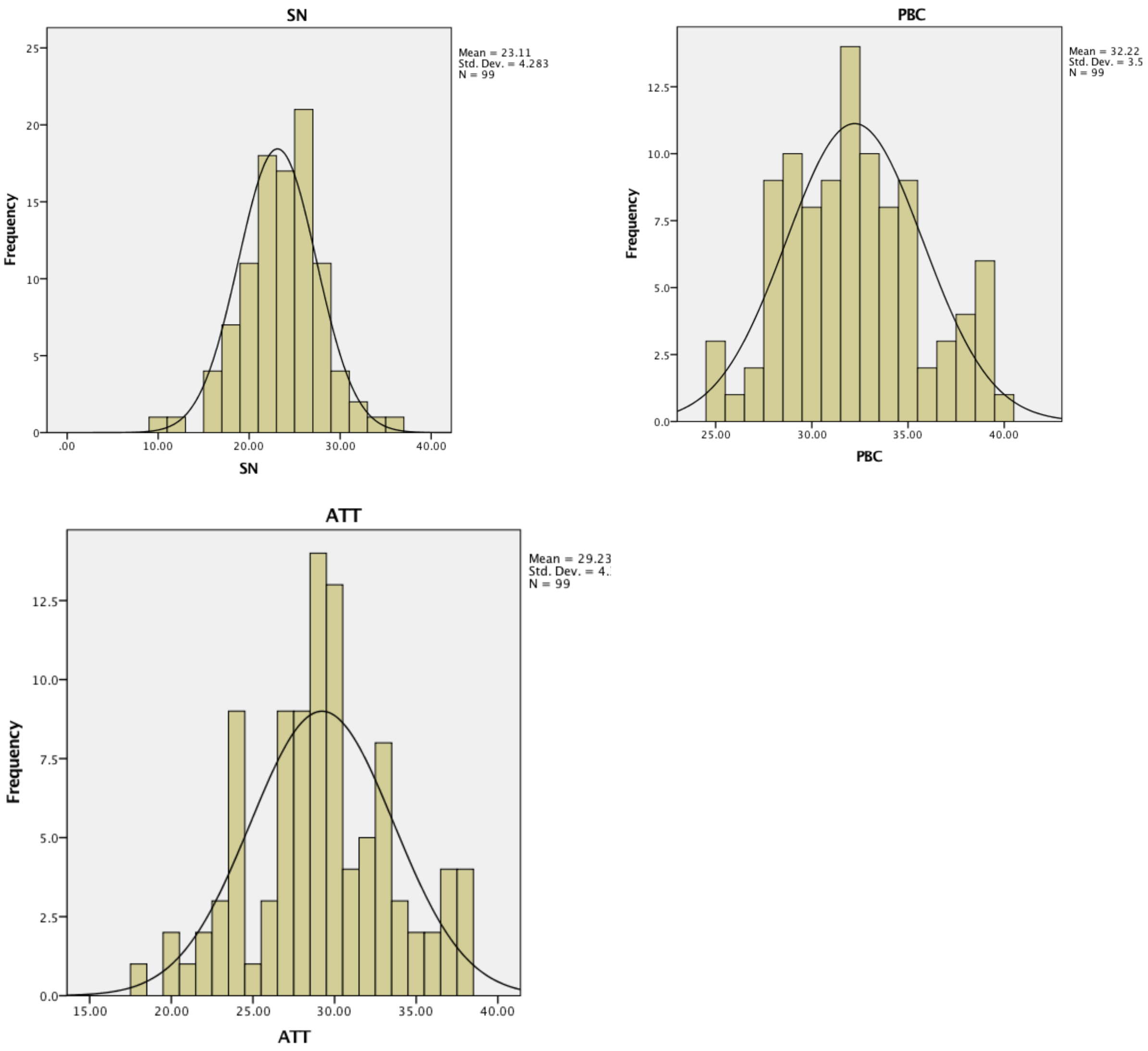


Figure 5. Histogram images of data distribution.

Completion Rates

The survey was provided to a population of 400 professionals who work with digital data on a daily basis, and only voluntary involvement was expected. The survey link and request was sent from a source internal to the organization so that participants were aware of it being a legitimate request. A copy of the letter can be found in Appendix C. One hundred and nine individuals responded to the survey; however, ten skipped questions or answered that they had not received corporate security training. As the study focuses on the effects of information security training on secure end user behavior, security training is a key measurement 99/400 or 24.75%.

Demographics

This study collected the following demographic characteristics: age, gender, and education level. In discussion with the Vice President of Technology and Security, a key demographic item was learned. All employees work with digital data on a daily basis as each employee is assigned a computer upon start date. Tables 6 and 7 below illustrate demographic data of the respondents to the survey.

Table 6

Demographic Information, Gender, and Age Frequency Report

What is your gender?

		Frequency	Percent	Cumulative Percent
Valid	Female	60	60.6	60.6
	Male	39	39.4	100
	Total	99	100	

What is your age?

		Frequency	Percent	Cumulative Percent
Valid	19-30	15	15.2	15.2
	31-40	25	25.3	40.4
	41-50	26	26.3	66.7
	50-60	20	20.2	86.9
	60 and above	13	13.1	100
	Total	99	100	

Table 7

Demographic Information, Education Report

What is the highest level of education you have completed?				
		Frequency	Percent	Cumulative Percent
Valid	Graduated from high school	11	11.1	11.1
	Graduated from 2-year college	3	3	14.1
	Graduated from college	36	36.4	50.5
	Completed graduate school	49	49.5	100

The remainder of item level frequencies can be found in Appendix F.

Data Analysis

Multiple linear regression (MLR) was used to test the relationships between the independent variables and the dependent variable. Studies have found that Likert scales, such as the instrument in this study, can be analyzed using parametric procedures under certain conditions. The scale has to be a true Likert scale and thus made of multiple items that all measure the same construct. Skewness and kurtosis must also be addressed and proven to be within acceptable levels. Thus, when these constraints are met, parametric statistical procedures can be used (Lix, Keselman, & Keselman, 1996; Lubke & Muthen, 2004; Choehn et al., 2013).

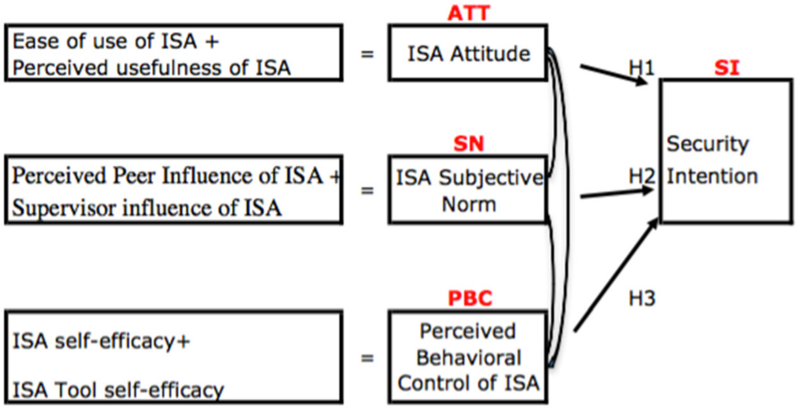


Figure 6. The corrected reliable hypothesis table (antecedents changed for validity).

H: There is a significant relationship between ISA and security behavior.

H₀: There is no significant relationship between ISA and security behavior.

The first model created was used to measure the effect of ISA SN, ATT, and PBC on secure behavior. The constructs were composed of multiple items using a five-scale response level. Tables 7 and 8 show the outcome of the analysis.

Table 8

Model Summary (N = 99)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.674	0.455	0.437	2.62439

Predictors: (Constant), PBC, SN, ATT

Table 9

Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	16.542	2.623		6.307	0
	ATT	0.094	0.079	0.118	1.189	0.238
	SN	-0.011	0.063	-0.013	-0.173	0.863

PBC	0.587	0.097	0.595		6.02	0.032

A Dependent Variable: SI
95.0% Confidence Interval for B

MLR results, as illustrated in Tables 8 and 9, indicate a moderate influence of the predictors on the dependent variable. This can be seen in the R^2 predicating that ATT, SN, and PBC cause 45.5% change in SI, while R, at .674, indicates an acceptable level of quality in the prediction. Only PBC proved to be significant at 0.032, after setting alpha at 1-.95 = .05, while SN and ATT would not be significant at 90% confidence interval. The shortcomings are most attributable to not having enough survey items in each construct and will be adjusted in future research. We must fail to reject the null hypotheses that there is no significant relationship between ISA and security behavior. The ISA variable, in order to match the TPM model, must show significance in ATT, PBC, and SN on change in SI. In this study, only PBC is significant. As there is no significance, there is as much probability of chance causing change in behavior as there is ATT, PBC, and SN.

H1: There is a significant influence of ISA ATT on end-user intention (behavior).

As seen in table 10 and figure 7, the correlation between ATT and SI is r = .496 and is significant at the 0.01 level. Therefore, we reject the null hypothesis, as there is a significant influence on SI by ATT.

Table 10

Pearson Correlation of ATT on SI

		ATT	SI
ATT	Pearson Correlation	1	.496**
	Sig. (2-tailed)		0
	N	99	99

SI	Pearson Correlation	.496**	1
	Sig. (2-tailed)	0	
	N	99	99

** Correlation is significant at the 0.01 level (2-tailed).

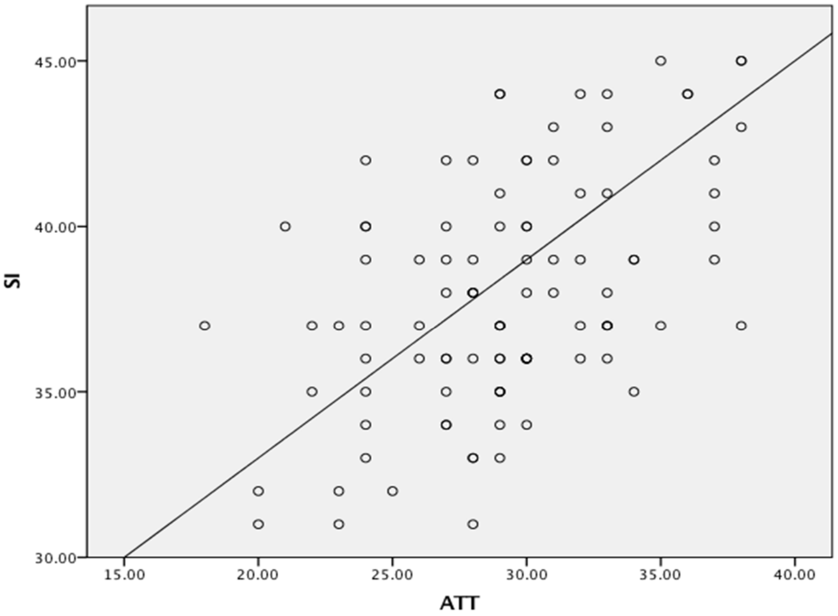


Figure 7. Pearson Correlation scatterplot SI/ATT

H2: There is a significant influence of ISA SN on end-user intention (behavior).

As seen in the Table 11 and Figure 8, the correlation between SN and SI is r = .124 and is not significant. Therefore, we fail to reject the null hypothesis, as there is not significant influence on SI by SN.

Table 11

Pearson Correlation of SN on SI

		SI	SN
SI	Pearson Correlation	1	0.124
	Sig. (2-tailed)		0.223
	N	99	99
SN	Pearson Correlation	0.124	1

Sig. (2-tailed)	0.223	
N	99	99

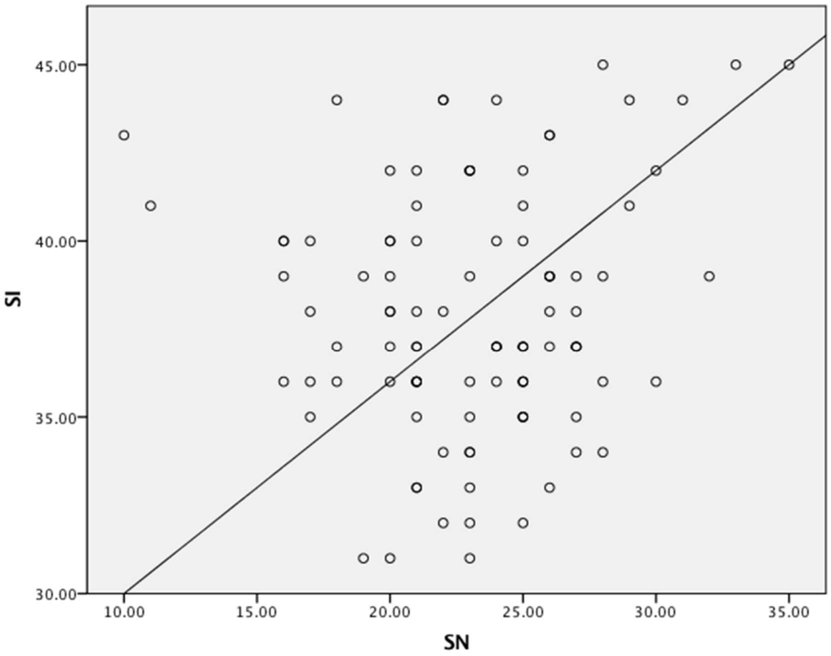


Figure 8. Pearson Correlation scatterplot SI/SN

H3: There is a significant influence of ISA PBC on end-user intention (behavior).

As seen in Table 12 and Figure 9, the correlation between PBC and SI is r = .668 and is significant at the 0.01 level. Therefore, we reject the null hypothesis, as there is a significant influence on SI by ATT.

Table 12

Pearson correlation of PBC on SI

		SI	PBC
SI	Pearson Correlation	1	.668**
	Sig. (2-tailed)		0
	N	99	99
PBC	Pearson Correlation	.668**	1
	Sig. (2-tailed)	0	
	N	99	99

** Correlation is significant at the 0.01 level (2-tailed).

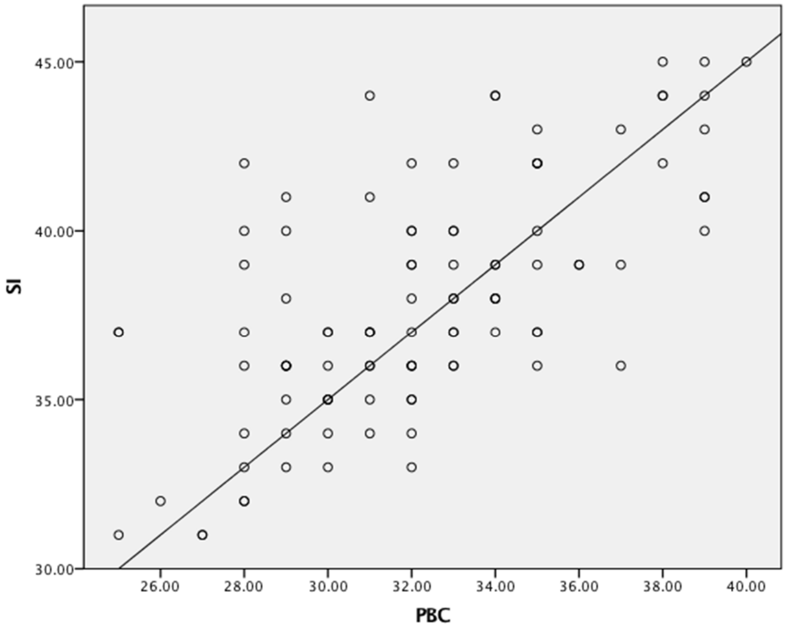
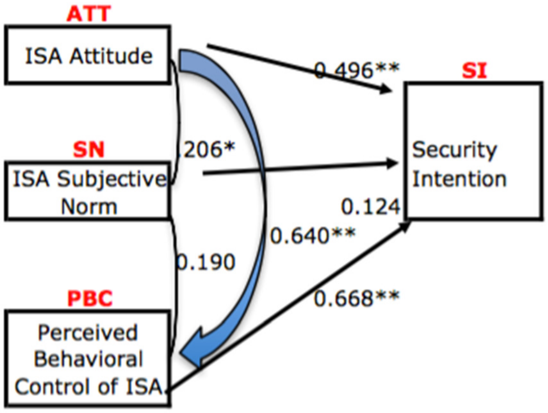


Figure 9. Pearson Correlation scatterplot SI/PBC

As Figure 10 indicates, there is very little correlation between each of the independent variables. The only moderate correlation ATT and PBC as r = 0.640. Also, there is no significance in the correlation between SN and SI nor SN and PBC.



** Correlation is significant at the 0.01 level (2-tailed).
** Correlation is significant at the 0.05 level (2-tailed).

Figure 10. Correlations of all studied constructs

Chapter V: Conclusion

This final chapter is divided into two sections: summary discussion and future research conclusions. The summary discussion section will provide a brief overview of the research, study background, and discussion of the findings of the study. The future research/conclusion section will provide analysis on the data collected and application in the research field. This section also illustrates the need for the continuation of this research agenda and the importance of further investigation.

Summary Discussion

This study examined the effectiveness of information security awareness (ISA) programs on end user security behavior. Past research emphasized the relevance of attitudes and behavior of individuals in relation to protecting information systems, a module that required far more than technological input (Brdiczka et al, 2012; Crossler et al., 2013; Dhillon, Syed, &Pedron, 2016; Hsu, Shih, Hung, & Lowry, 2015). Additionally, past research illustrates that information security awareness programs (ISA) are the common security bridge between technical and human factor in data risk mitigation. ISA is commonly defined as an organizational process that aims at educating end-users in its procedures regarding the protection of the digital assets (Takebayashi, Tsuda, Hasebe, & Masuoka, 2013; Wheeler & Swick, 2011; Whitman & Mattord, 2011). As the word *awareness* implies, an ISA program is designed to create an organizational culture of proactive secure computing, a culture of security. In the ongoing effort to secure digital assets, the end-user occupies the role of both friend and foe. Security awareness is a process that seeks to change individual perceptions, values, attitudes, behavior, norms, and work habits in an effort to secure vital personal information (Tsohou et.al, 2015). Within the individuals security behavior in an organization, the collective security culture of the organization is revealed. Therefore, this study examined ISA effectiveness on end-user behavior to help create future footholds of research, frameworks for securing human behavior. It is imperative to good security that an understanding of the human components, as well as technical solutions, are necessary to a secure organization.

Some of the more difficult and pervasive aspects of entering into the world of technology relates to the protection of digital assets by the very people who help create them, the end-user in an organization. Current research demonstrates that security is not simply a technology problem, but is primarily a people problem caused by malicious intent, carelessness, or accident (Desman, 2013; Kim, Lee, Chun, & Benbasat., 2014; Peltier, 2013; Whitman & Mattord, 2013).

Cybercriminals have a penchant for utilizing any method that tricks end-users into breaking their security practice. They have little regard for the feelings of safety by end-users in their quest to hack into heretofore considered safe systems. Cybercriminals employ a wide variety of hacking methods from pushing malware download on to unsuspecting consumers, phishing email, even going so far as to pay vulnerable customer service workers who have access to personal data. Again, ISA programs are designed to alleviate cybercriminal activity and create wanted secure behavior. Instances of stolen data and accidental data loss created the underlying theme of this study. Understanding the attitudes (ATT), subjective norms (SN), and perceived behavioral control (PBC) that motivate the behavior behind user adoption of ISA (Bandura, 1977; Ajzen, 1985; Mann, 2012) aid in understanding a culture where risk of data loss can occur.

Due to the loss of data from cybercrime and cybercriminals, in addition to accidental losses, human resources involved in the cyber world require the analysis presented in this study in order to establish policies, procedures, and practices mitigating data loss (Takebayashi, et al., 2010). Data loss can lead to lost revenue, lost jobs, lack of trust in essential digital processes, and even lost identity. Therefore, understanding and investigating the causes of end-user behavior was critical to finding a successful strategy for preventing further data loss. ISA is the widely accepted strategy for end-user security behavior while TPB is broadly accepted as a tool for predicting behavior. By applying TPB in connection to ISA strategies preventing data loss, new security methods, frameworks, technologies, and policies were suggested through the research presented in the study. However, as the data demonstrated, relying solely upon technology to deter human interference with data loss places abnormal stressors on the systems meant to protect end-users from data loss. Too-heavy reliance upon technological deterrents as the demand for information and its transmission has increased the exposure of sensitive data to cyber security risks. Since ISA programs are widely accepted as the primary tool for mitigating end-user security risks, researching the effectiveness of ISA in developing appropriate end-user security behavior was critical to developing new security methods, frameworks, technologies, and policies The variety of problems created by cybercriminals established the need for grasping attitudes and behaviors that laid the foundation for security breaches. The research from this analysis indicated that both technological and human strategies must be employed in the development of an information security awareness (ISA) program for organizational protection.

By creating a positive culture that promotes desired security behavior through appropriate technology, security policies, and an understanding of human motivations, ISA programs are becoming the norm for organizational end-user risk protection (Peltier, 2013; Tsohou, Karyda, Kokolakis, & Kiountouzis, 2015; Vroom & Solms, 2004). The data collected through the analysis of this study illustrated that ISA programs may be an effective manner to build desired end-user security behavior.

Since the turn of the twenty-first century, information accessibility increased incrementally, often at a speed far more rapid than ISA programs or the average consumer could prevent cybercrime. As the continuing need to prevent cybercrime increases, so does the need to increase security. In order for organizations to diminish risk, it is paramount to start security at the human level and align with technical solutions. It is critical to understand human behavior and drive a secure culture into the organization.

Since information security (IS) has its basis in human behavior, then the behavior controlling IS finds its paradigm firmly grounded in the psychological and sociological behavior of the individuals associated with IS (D'arcy et al., 2009; Ahmed et al., 2012). The acceptance of effective ISA programs bridges the gap between end-users and technology (Ahmad et al., 2012; Balerek et al., 2012; Desman, 2013). Any organization applying the innovative techniques in its technological component must provide its end-users with secure guidance on expected behavior. End-users have an expectation of a strong and more than adequate ISA program for their protection. Effective ISA programs that follow with action not merely technical jargon, find that end-users have a more cooperative attitude toward the organization and belief in its policies (Peltier, 2011). In other words, actions that influence the ATT, SN, and PBC of end-users create an organizational culture based on collective individual behavior that results in lower risk to data theft or loss. The problem that this study aimed at delineating concerned the manner and effectiveness of an ISA in risk management and how these ISA policies related to human weaknesses and strengths. By building on the research of psychosocial behavior (Stanton et al., 2005) and leveraging established TPB tools (Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1975), this study illustrated the correlation between using ISA programs to help mitigate security attacks through the illumination of relevant human behavior. This was accomplished by using a survey that asked questions around ISA and also the respondent's behavior in security situations.

The creation of information security policies, standards, procedures, and guidelines is only the start of establishing effective information security programs. Technology plays a role, but is not as effective as a trained work force (Brdiczka et al., 2012; Crossler et al., 2013; Hsu et al., 2015; Dhillon et al., 2016). A well-built technical security architecture will be rendered less effective if there is no process in place to make certain that the end-users are made aware of their responsibilities with regard to information assets (Crossler et al., 2013). An ISA program encompasses end-user awareness, education, and training programs to address security practices, policies and tools. As this research illustrates, the next step is to create a culture of security within the organization built on ISA program and understanding security behavior.

Security policy is the foundation of an ISA program as it establishes practice, sets boundaries, and creates desired behavior. In most organizations, security policy guidelines and implementations are the responsibility of the information technology (IT) department and often a security executive. In particular, a security policy consists of a set of rules and practices that control how an organization protects and distributes its key information assets, striking a balance between security and usability (Safa et al., 2012). According to Peltier

(2013), a good security policy dictates user responsibility that includes threat reporting, identification of key information security personal, and deterrents for violations.

Security misbehavior is broadly understood as the set of end-users who violate organizational security policy, that leads to the loss of organizational assets. Users who engage in intentional misbehavior are either out for profit and/or destruction, and are labeled intentional malicious insiders. End-users who unintentionally neglect to follow policy and engage in behaviors which result in asset loss or risk are categorized as unintentional insider threats (Whitman & Mattord, 2011).

Inappropriate modification of data, altering access to data and the availability of systems, copying software, selling organizational IP property, and stealing corporate data as they leave for other jobs are a few examples of intentional undesired behaviors. Providing a strong ISA program will not halt misbehaviors, and as the study's data demonstrated, a weak ISA program could lead to such behavior (Siponen, 2014). Unintentional undesired behavior such as understanding and being capable of following security policy and practice, but failing to do so can also lead to loss of organizational assets (Guo, 2010). Unintentional undesired behavior can also be caused by lack of knowledge or efficacy. Sustaining both intentional and unintentional loss is a weak ISA program. However, with proper training, educated end-users assume clearer understanding of individual responsibilities behind the establishment of effective ISA (Peltier, 2013; Tsohou et al., 2015; Vroom & Solms, 2004). The research in this study built on the importance of an ISA program and outlined the need to study behavior to create the security minded culture that will further protect organizational digital assets.

Future Research/Conclusion

The rapid advancement of technology places a continued burden on ISA policy makers and programs to prevent cybercrime and cybercriminals seeking to misuse, steal, and sell data for unintended reasons. Maintaining advances in IS systems requires more than just technology, it also requires understanding human behavior. A combination of technical skills in conjunction with academic research into understanding the attitudes (ATT), subjective norms (SN), and perceived behavioral control (PBC) of behavior comprises an intrinsic part of amending the problem. Individuals or groups involved in cybercrime do so for a variety of reasons, most of which are intertwined with attitudes of greed and an overall lack of concern for those they damage. End-users who make mistakes that lead to data loss are often the result of poor ISA programs. Researchers continue to discover the underlying behaviors that lay behind the increase of data loss as necessary ingredients to construct IS systems formulated to combat data loss. This research starts an agenda into that field and provides many footholds for future research. More specifically, the research agenda being formed in this study is human behavior factors in information assurance. The first step into this agenda was to step and look at ISA and secure behavior. This study showed that there is a correlation between ISA programs and behavior, but will need further tuning on the survey tool to arrive at significant conclusions.

The research in this study focused on the end-user ATT, SN, and PBC involved in ISA programs that constructs the behaviors that led to compliance of information security guidelines, practices, and policies. Current behavioral research in information security relies heavily on TPB constructs as a precursor to behavior. The hypothesis of the research conducted by Hu, Kuamg, Lu, and Wu (2014) utilized ATT in the study of software piracy in

China and the United States, demonstrating that the attitude toward software privacy was positively related to piracy intent. More specifically, they analyzed software cost, punishment severity, and punishment certainty as antecedents to attitudes that subsequently contribute to intent. Not only did their study exhibit that antecedents influence attitude, but they also found that attitude had the largest influence on piracy intent. In a study by Siponen, Mahmood, and Pahinila (2014), these researchers found that that security compliance was positively influenced by ATT, SN, and PBC. Furthermore, these constructs could be cultivated into a culture by executive-level influence. The outcome of these two studies alone indicated that TPB constructs are a major component of either cybercriminal behavior or conversely, compliance led by a security culture created by the behaviors of peers and by those in charge. Researchers cannot dismiss this aspect of behavior, particularly in light of the fact that the cyber world is not going to disappear, therefore data loss too will escalate accordingly without further constructive analysis. This research added to the work above by showing that end-user security behaviors are modified by ISA programs. Furthermore, the study illustrated why technical reliance for secure the organization is toxic and will lead to data loss.

Information awareness programs are a critical component of overall information security; technology without ISA is not a fully encompassed plan. The universality of information systems in combination with the on-going requirements for these systems to be highly accessible, creates the requisite application of newer, more innovative security. As a result, organizations have advocated for more impactful ISA programs (Mejias, 2012). ISA in its definitive and systematic place in technology must be inculcated in end-user procedures in order for their protection of all things digital (Takebayashi, Tsuda, Hasebe, & Masuoka, 2013; Wheeler & Swick, 2011; Whitman & Mattord, 2011). This study illustrated that the impact of ISA programs on behavior is critical to making protection more successful. In the ongoing effort to secure digital assets, the end-user occupies the role of both friend and foe. Security awareness is a process that seeks to change individual perceptions, values, attitudes, behavior, norms, work habits, within an organizational culture in order to secure vital information (Tsohou et al., 2015). As the statistical analysis in this study indicated attitude, intent, ease of use, self-efficacy, and peer influence relate directly to security intent. The significance of the data collected self-advocates the importance of understanding TPB constructs in the ever-increasing cyber world where security cannot be ignored as the Internet and its multitude of growing components is a world that is here to stay.

Keeping abreast of and ahead of data loss behavior was the vital component behind this research. Utilizing a mid-size organization with technology as one of its primary and significant factors endowed the study with the parameters required to help establish the paradigm of developing and maintaining ISAs proved essential. End-users, by definition all who use the internet with its growing necessity in everyday lives, must become and be more aware of the negativity of IT as well as its benefits. However, without ongoing research and study of secure behavior, data loss will rise far more rapidly than those who rely only on technology. Bandura's (1977) theoretical premise of attitude and its effect on behavior resides comfortably in association with Azjen's (1985) TPB as behavior predictors of ISA effectiveness to the use and/or misuse the digital world we live in.

Providing analytical data supported through this quantitative study lays the foundation for further ongoing research aimed at enhancing knowledge of the behaviors of those charged with securing the data in their hands against the ultimate benefits, and dangers, of the information highway. The twenty-first century's innovation and love affair with technology will not cease in spite of the exponential growth of cybercrime, thus it is imperative to understand the way ISA programs influence the behavior of the end-user in charge of digital assets. Behavior, trust, security, and innovative ISAs must be the underpinnings attached to security in the world of information technology and cyber growth. Armed with a solid ISA program and an understanding of human behavior an organization can create a culture of security. A culture where security is inclusive of all organizational employees and technical solutions. The organization will reach a higher level of security where behaviors can be predicated and expected.

References

Ahmad, A., Maynard, S. B., & Park, S. (2012). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing,* 1–14.

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

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior.* Englewood Cliffs, NJ: Prentiss-Hall.

Alfawaz, S., Nelson, K., & Mohannak, K. (2010, January). Information security culture: A behaviour compliance conceptual framework. In *Proceedings of the Eighth Australasian Conference on Information Security, Volume 105* (pp. 47–55). Australian Computer Society, Inc.

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567–575.

Armitage, C. J., Norman, P., Noor, M., Alganem, S., & Arden, M. A. (2014). Evidence that a very brief psychological intervention boosts weight loss in a weight loss program. *Behavior Therapy*, *45*(5), 700–707.

Aurigemma, S., & Panko, R. (2012, January). A composite framework for behavioral compliance with information security policies. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 3248–3257). IEEE.

Babbie, E. R. (1990). *Survey research methods*. Belmont, CA: Wadsworth Pub. Co.

Balcerek, B., Frankowski, G., Kwiecień, A., Smutnicki, A., & Teodorczyk, M. (2012). Security best practices: Applying defense-in-depth strategy to protect the NGI_PL. In *Building a National Distributed e-Infrastructure–PL-Grid* (pp. 128–141). Springer Berlin Heidelberg.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191.

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist*, *37*(2), 122.

Bandura, A. (1986). The explanatory and predictive scope of self-efficacy theory. *Journal of Social and Clinical Psychology*, *4*(3), 359–373.

Bandura, A. (1989). Human agency in social cognitive theory. *American Psychologist*, *44*(9), 1175.

Bandura, A. (2006). Guide for constructing self-efficacy scales. *Self-efficacy Beliefs of Adolescents*, *5,* 307–37.

Bandura, A. (2012). On the functional properties of perceived self-efficacy revisited. *Journal of Management*, *38*(1), 9–44.

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.

Brdiczka, O., Liu, J., Price, B., Shen, J., Patil, A., Chow, R., & Ducheneaut, N. (2012, May). Proactive insider threat detection through graph learning and psychological context. In *Security and Privacy Workshops (SPW), 2012 IEEE Symposium on* (pp. 142–149). IEEE.

Brahme, A. M., & Joshi, S. B. (2013). A review of cyber crime: An ever-growing threat and its influence on society & IT sector. *International Journal of Managment, IT and Engineering*, *3*(7), 534–545.

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).*

Caprara, G. V., Vecchione, M., Alessandri, G., Gerbino, M., & Barbaranelli, C. (2011). The contribution of personality traits and self-efficacy beliefs to academic achievement: A longitudinal study. *British Journal of Educational Psychology*, *81*(1), 78–96.

Clarke, M. (2011). The role of self-efficacy in computer security behavior: Developing the construct of computer security self-efficacy (CSSE). *ProQuest LLC*.

CNSS https://www.cnss.gov/CNSS/index.cfm

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, 189–211.

Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2013). *Applied multiple regression/ correlation analysis for the behavioral sciences*. Routledge.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, *39*, 447–459.

Cheung, R., & Vogel, D. (2013). Predicting user acceptance of collaborative technologies: An extension of the technology acceptance model for e-learning. *Computers & Education*, *63*, 160–175.

Chu, K. (2013, January 9). Dun & Bradstreet fined, four sentenced in China. *The Wall Street Journal Online*. Retrieved from http://www.wsj.com/news/articles/SB10001424127887323482504578230781008932240?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424127887323482504578230781008932240.html.

Cronbach, L. J., & Meehl, P. E. (1955). Construct validity in psychological tests. *Psychological Bulletin*, *52*(4), 281.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101.

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.

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643–658.

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.

Deci, E. L., & Ryan, R. M. (2012). Overview of self-determination theory. In *The Oxford handbook of human motivation* (pp. 85–107). New York, NY: Oxford University Press.

Desman, M. B. (2013). *Building an information security awareness program*. CRC Press.

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security*, *56*, 63–69.

Fabozzi, F. J., Focardi, S. M., Rachev, S. T., & Arshanapalli, B. G. (2014). Building and testing a multiple linear regression model. In *The basics of financial econometrics: Tools, concepts, and asset management applications*, 81–102.

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

Furnell, S., & Moore, L. (2014, May). End-user security: No longer a matter of choice? In *Proceedings of 13th Annual Security Conference, Las Vegas, Nevada* (pp. 22–24).

Gandhi, M. (1939). *The collected works of Mahatma Gandhi*.

Gartner --http://www.gartner.com/newsroom/id/2156915, retrieved 2013

Ghaisas, S., Motwani, M., Balasubramaniam, B., Gajendragadkar, A., Kelkar, R., & Vin, H. (2015, August). Towards automating the security compliance value chain. In *Proceedings of the 2015 10th Joint Meeting on Foundations of Software*

Engineering (pp. 1014–1017). ACM.

Ghasemi, A., & Zahediasl, S. (2012). Normality tests for statistical analysis: A guide for non-statisticians. *International Journal of Endocrinology and Metabolism*, *10*(2), 486–489. http://doi.org/10.5812/ijem.3505.

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users: A study of perceptions of the adequacy of security. *Information & Management*, *20*(1), 13–27.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*(2), 203–236.

Guo, K. (2010). *Information systems security misbehavior in the workplace: The effects of job performance expectation and workgroup norm.*

Grinnell Jr., R. M., & Unrau, Y. (2005). *Social work research and evaluation: Quantitative and qualitative approaches*. Cengage Learning.

Hair, J. F. (2009). *Multivariate data analysis*. Works.bepress.com

Harris, K., Jerome, N., & Fawcett, S. (1997). Rapid assessment procedures: A review and critique. *Human Organization*, *56*(3), 375–378.

Hendre, A., & Joshi, K. P. (2015, June). A semantic approach to cloud security and compliance. In *2015 IEEE 8th International Conference on Cloud Computing* (pp. 1081–1084). IEEE.

Holden, R. J., & Karsh, B. T. (2010). The technology acceptance model: Its past and its future in health care. *Journal of Biomedical Informatics*, *43*(1), 159–172.

Huffman, A. H., Whetten, J., & Huffman, W. H. (2013). Using technology in higher education: The influence of gender roles on technology self-efficacy. *Computers in Human Behavior*, *29*(4), 1779–1786.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, *54*(6), 54–60.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615–660.

Hu, X., Kuang, W., Lu, B., & Wu, G. (2014). Inside the minds of software pirates: A comparison study of American and Chinese pirates. In *The Eighth China Summer Workshop on Information Management (CSWIM 2014*; p. 59).

Hsu, J. S. C., Shih, S. P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research*, *26*(2), 282–300.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95.

Ifinedo, P. (2013). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition *Psychological Review*, *84*(2), 191–215.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69–79.

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, *25*(3), 231–251.

Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security, 61*, 46–58.

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, *5*(26), 10862.

Kim, T. H., Lee, J. N., Chun, J. U., & Benbasat, I. (2014). Understanding the effect of knowledge management strategies on knowledge management performance: A contingency perspective. *Information & Management*.

Kline, R. B. (1998). *Principles and practice of structural equation modeling*. New York: The Guilford Press. Retrieved August 15, 2016, from https://statistics.laerd.com/spss-tutorials/multiple-regression-using-spss-statistics.php.

Lee, J., & Suh, E. (2013). An Empirical Study of the Factors Influencing Use of Social Network Service. In *PACIS* (p. 181).

Liaw, S. S., & Huang, H. M. (2013). Perceived satisfaction, perceived usefulness and interactive learning environments as predictors to self-regulation in e-learning environments. *Computers & Education*, *60*(1), 14–24.

Lix, L. M., Keselman, J. C., & Keselman, H. J. (1996). Consequences of assumption violations revisited: A quantitative review of alternatives to the one-way analysis of variance F test. *Review of Educational Research, 66*(4), 579–619.

Lubke, G. H., & Muthén, B. O. (2004). Applying multigroup confirmatory factor models for continuous outcomes to Likert scale data complicates meaningful group comparisons. *Structural Equation Modeling, 11*(4), 514–534.

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.

Mann, M. I. (2012). *Hacking the human: Social engineering techniques and security* *countermeasures*. Gower Publishing, Ltd.

Marakas, G., Johnson, R., & Clay, P. F. (2007). The evolving nature of the computer self-efficacy construct: An empirical investigation of measurement construction, validity, reliability and stability over time. *Journal of the Association for Information Systems*, *8*(1), 2.

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

Maynard, M. T., Mathieu, J. E., Rapp, T. L., & Gilson, L. L. (2012). Something(s) old and something(s) new: Modeling drivers of global virtual team effectiveness. *Journal of Organizational Behavior, 33*(3), 342–365.

McKeachie, W., & Svinicki, M. (2013). *McKeachie's teaching tips*. Cengage Learning.

Mejias, R. J. (2012, January). An integrative model of information security awareness for assessing information systems security risk. In *System Science (HICSS), 2012 45th Hawaii International Conference* on (pp. 3258–3267). IEEE.

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, *34*, 47–66. Retrieved August 14, 2016, from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3693611/

Nachtigall, C., Kroehne, U., Funke, F., & Steyer, R. (2003). Pros and cons of structural equation modeling. *Methods Psychological Research Online, 8*(2), 1–22.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815–825. NSA http://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Pahnila, S., Karjalainen, M., & Siponen, M. (2013). *Information security behavior: Towards multi-stage models*.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). A study of information security awareness in Australian government organisations. *Information Management & Computer Security, 22*(4), 334–345.

Peltier, T. R. (2013). *Information security policies, procedures, and standards: Guidelines for effective information security management*. CRC Press.

Pillai, D., & Andley, P. (2010). Information security threats. *Compendium of Papers 2009–10*, 58.

Piper, W. (2005). *The little engine that could.* Penguin

Polit, D. F., & Beck, C. T. (2006). The content validity index: Are you sure you know what's being reported? Critique and recommendations. *Research in Nursing & Health, 29*(5), 489–497.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816–826.

Rogers, E. M. (2010). *Diffusion of innovations*. Simon and Schuster.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65–78.

Shannon, K. (2011, April 11). Breach in Texas comptroller's office exposes 3.5 million social security numbers, birth dates. *The Dallas Morning News*. Retrieved from http://www.dallasnews.com/news/state/headlines/20110411-breach-in-texas-comptrollers-office-exposes-3.5-million-social-security-numbers-birth-dates.ece.

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

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34*(3).

Stajkovic, A. D., & Luthans, F. (1998). Self-efficacy and work-related performance: A meta-analysis. *Psychological Bulletin*, *124*(2), 240.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124–133.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, 147–169.

Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *The Communications of the Association for Information Systems, 13*(1), 63. www.surveymonkey.com, accessed 2016.

Takebayashi, T., Tsuda, H., Hasebe, T., & Masuoka, R. (2010). Data loss prevention technologies. *Fujitsu Scientific and Technical Journal*, *46*(1), 47–55.

Tamjidyamcholo, A., Bin Baba, M. S., Tamjid, H., & Gholipour, R. (2013). Information security—Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language. *Computers & Education, 68*, 223–232.

Tan, M., & Teo, T. S. (2000). Factors influencing the adoption of Internet banking. *Journal of the AIS, 1*(1es), 5.

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research, 6*, 144–176.

Teh, P. L., Ahmed, P. K., & D'Arcy, J. (2015). What drives information security policy violations among banking employees? Insights from neutralization and social exchange theory. *Journal of Global Information Management (JGIM)*, *23*(1), 44–64.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems, 24*(1), 38–58.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3), 190–198.

Vance, A., & Siponen, M. T. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing (JOEUC)*, *24*(1), 21–41.

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.

Viduto, V., Maple, C., Huang, W., & López-Peréz, D. (2012). A novel risk assessment and optimization model for a multi-objective network security countermeasure selection.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*(3), 191–198.

Vygotsky, L. S. (1980). *Mind in society: The development of higher psychological processes*. Harvard University Press.

Weems, G. H., & Onwuegbuzie, A. J. (2001). The impact of midpoint responses and reverse coding on survey data. *Measurement and Evaluation in Counseling and Development*, *34*(3), 166.

Whitman, M. E., & Mattord, H. J. (2012). Threats to information security revisited. *Journal of Information System Security*, *8*(1).

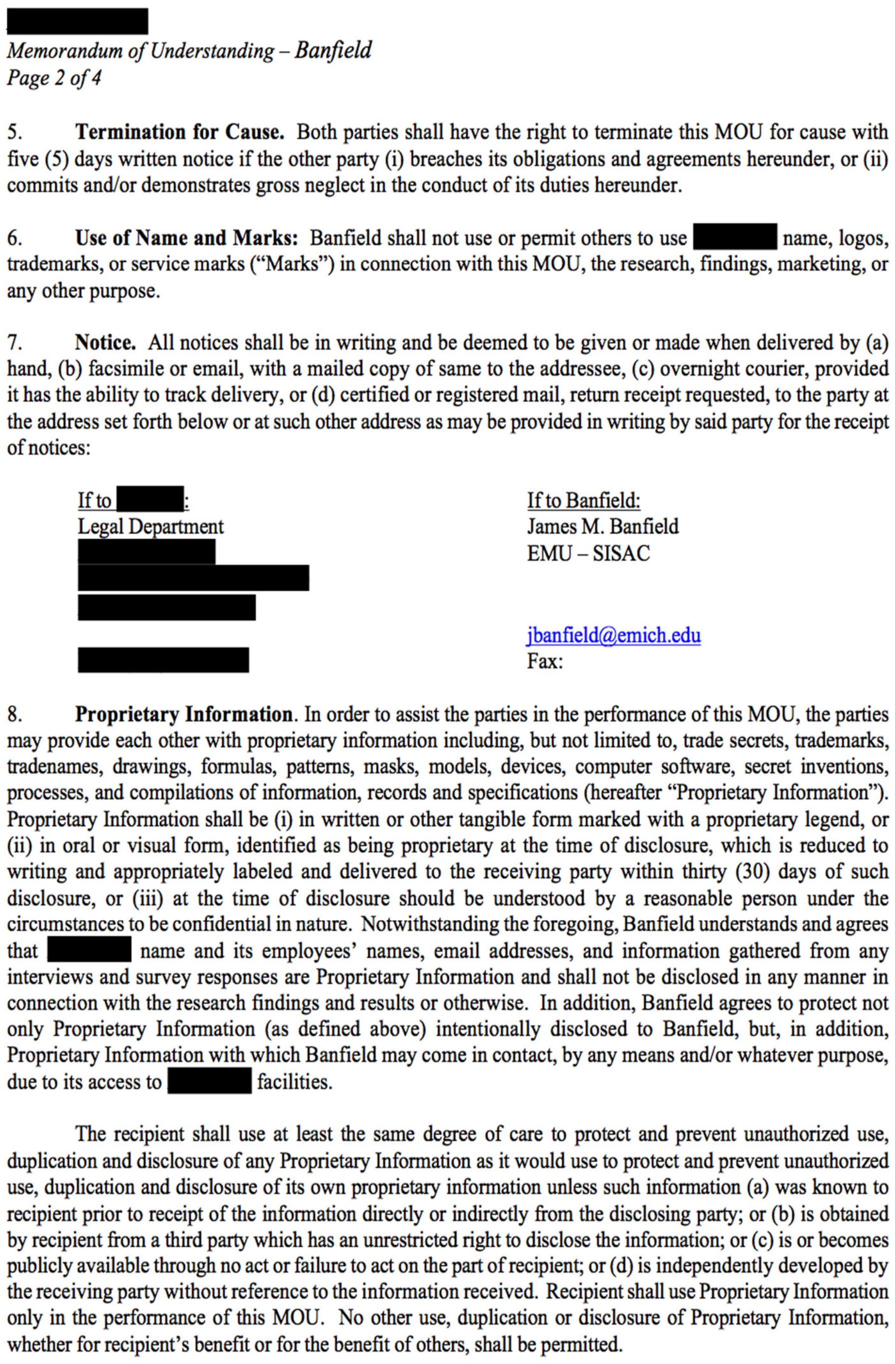
Whitman, M., & Mattord, H. (2011). *Principles of information security*. Cengage Learning.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, *37*(1), 1–20.

Younis, M. Y. A., & Kifayat, K. (2013). Secure cloud computing for critical infrastructure: A survey. *Liverpool John Moores University, United Kingdom, Tech. Rep*. problem. *Decision Support Systems*, *53*(3), 599–610.

Zimmerman, B. J. (2000). Self-efficacy: An essential motive to learn. *Contemporary Educational Psychology*, *25*(1), 82–91.

Appendix A: MOU



[redacted]
Memorandum of Understanding – Banfield
Page 2 of 4

5. **Termination for Cause.** Both parties shall have the right to terminate this MOU for cause with five (5) days written notice if the other party (i) breaches its obligations and agreements hereunder, or (ii) commits and/or demonstrates gross neglect in the conduct of its duties hereunder.

6. **Use of Name and Marks:** Banfield shall not use or permit others to use [redacted] name, logos, trademarks, or service marks ("Marks") in connection with this MOU, the research, findings, marketing, or any other purpose.

7. **Notice.** All notices shall be in writing and be deemed to be given or made when delivered by (a) hand, (b) facsimile or email, with a mailed copy of same to the addressee, (c) overnight courier, provided it has the ability to track delivery, or (d) certified or registered mail, return receipt requested, to the party at the address set forth below or at such other address as may be provided in writing by said party for the receipt of notices:

If to [redacted]:
Legal Department
[redacted]

[redacted]

If to Banfield:
James M. Banfield
EMU – SISAC

jbanfield@emich.edu
Fax:

8. **Proprietary Information**. In order to assist the parties in the performance of this MOU, the parties may provide each other with proprietary information including, but not limited to, trade secrets, trademarks, tradenames, drawings, formulas, patterns, masks, models, devices, computer software, secret inventions, processes, and compilations of information, records and specifications (hereafter "Proprietary Information"). Proprietary Information shall be (i) in written or other tangible form marked with a proprietary legend, or (ii) in oral or visual form, identified as being proprietary at the time of disclosure, which is reduced to writing and appropriately labeled and delivered to the receiving party within thirty (30) days of such disclosure, or (iii) at the time of disclosure should be understood by a reasonable person under the circumstances to be confidential in nature. Notwithstanding the foregoing, Banfield understands and agrees that [redacted] name and its employees' names, email addresses, and information gathered from any interviews and survey responses are Proprietary Information and shall not be disclosed in any manner in connection with the research findings and results or otherwise. In addition, Banfield agrees to protect not only Proprietary Information (as defined above) intentionally disclosed to Banfield, but, in addition, Proprietary Information with which Banfield may come in contact, by any means and/or whatever purpose, due to its access to [redacted] facilities.

The recipient shall use at least the same degree of care to protect and prevent unauthorized use, duplication and disclosure of any Proprietary Information as it would use to protect and prevent unauthorized use, duplication and disclosure of its own proprietary information unless such information (a) was known to recipient prior to receipt of the information directly or indirectly from the disclosing party; or (b) is obtained by recipient from a third party which has an unrestricted right to disclose the information; or (c) is or becomes publicly available through no act or failure to act on the part of recipient; or (d) is independently developed by the receiving party without reference to the information received. Recipient shall use Proprietary Information only in the performance of this MOU. No other use, duplication or disclosure of Proprietary Information, whether for recipient's benefit or for the benefit of others, shall be permitted.

In no event is the recipient authorized to duplicate or disclose Proprietary Information without the prior written approval of the disclosing party or to use Proprietary Information except for the purpose provided in this MOU. This clause shall be binding from the effective date of this MOU until five (5) years after termination of this MOU.

9. **Intellectual Property**. Neither party shall acquire, directly or by implication, any rights in any copyrighted works, patents and inventions and/or Proprietary Information of the other party developed, authored, conceived or reduced to practice by the other party hereunder.

10. **Entire Agreement**. This MOU constitutes the entire agreement among the parties, superseding all prior oral or written agreements, understandings, representations and warranties, and courses of conduct and dealing regarding the subject matter hereof. Except as otherwise provided herein, the provisions of this MOU may be amended, modified or waived only by a writing executed by each party hereto.

11. **Governing Law**. This MOU shall be governed by the laws of the State of Michigan, except its choice of law rules, and any dispute concerning the interpretation of this MOU or any allegation of breach of its provisions shall be resolved by judicial action brought in the courts of the State of Michigan and the parties hereby consent to the exclusive jurisdiction of such courts over any such disputes.

12. **Licensure/Nonprofit Status**. No party shall do anything that would jeopardize [redacted] licensure, accreditation, federal, state or local tax exemptions (including, without limitation, federal tax-exempt status as an organization described under Section 501(c)(3) of the Internal Revenue Code). Notwithstanding the other provisions of this MOU, if [redacted] is in jeopardy of the loss of any of the aforementioned licenses, accreditations or eligibilities as a result of this MOU, [redacted] shall have the right to immediately terminate this MOU.

13. **Expenses**. Each party hereto shall pay his, her or its own expenses in connection with the negotiation, execution and performance of this MOU, the transactions and purposes contemplated by this MOU and all things required to be done in connection with this MOU.

13. **Assignment**. This MOU may not be assigned in whole or in part by either party without the prior written consent of the other party.

14. **Waiver**. A waiver of any breach of any provision of this MOU shall not be deemed a waiver of such rights, nor shall the same be deemed to be a waiver of any subsequent breach, either of the same provision or otherwise.

15. **Severability**. The terms of this MOU are severable such that if any term or provision is declared by a court of competent jurisdiction to be illegal, void, or unenforceable, the remainder of the provisions shall continue to be valid and enforceable

16. **Relationship**. In performing any services herein specified, each party shall be acting as an independent contractor to the other. Nothing in this MOU shall be deemed to constitute, create, give effect to, or otherwise recognize a joint venture, partnership, or formal business entity of any kind, and the rights and obligations of the parties shall be limited to those expressly set forth herein.

17. **Specific Performance**. Each party acknowledges and agrees that the other party may be damaged irreparably if Sections 6, 8, or 9 of this MOU are not performed in accordance with its specific terms or otherwise is breached. Accordingly, each party agrees that, upon a proper showing of proof of entitlement

to such remedy, the other party shall be entitled to an injunction or injunctions to prevent the breach or further breach and to enforce specifically such terms, in addition to any remedy to which it may be otherwise entitled at law or in equity.

18. **Counterparts; Electronic Signature**. This MOU may be executed in two or more counterparts and by facsimile, PDF, .TIF, or other electronic signature, each of which shall be deemed an original but all of which together shall constitute one and the same instrument.

IN WITNESS WHEREOF, the parties hereto have executed this MOU as of the day and year first above written.

Accepted for:

[redacted]

____
(Authorized Signature)

____
(Printed Name)

____
(Title)

Accepted for:

____
(Authorized Signature)

James M. Banfield
____
(Printed Name)

Appendix B: Survey

The goal of this research survey is to better understand **information security awareness (security policy, practice, tools, procedure, resources, and culture)** effectiveness on secure behavior in mid-size organizations. A secondary focus is to create a tool that can be used to measure this relationship in other organizations.

Construct	**Variable Name**						
Demographic	D1	Age	Interval	19-30	31-40	41-50	51-60
	D2	Gender	M/F	Male	Female		
	D3	Education	Nominal	High School	College	Masters or above	
	D4	Working with others	Interval	1-2 hrs day	3-4 hrs day	more than 5 hrs day	
	D5	Received Corporate Security training	Nominal	Yes	No		
	Adapted from Taylor & Todd, 1995;Parsons, McCormac, Pattison, Butivicius, Jerram, 2014; Stanton et al., 2005; Davis 1989						
	** Likert Scale (1=Strongly disagree 2=disagree 3=neutral 4=agree 5=strongly agree)						
Perceived Ease of use (EU)	EU1	Following my corporate security policy is difficult for me					
	EU2	Following my corporate security policy is easy for me					

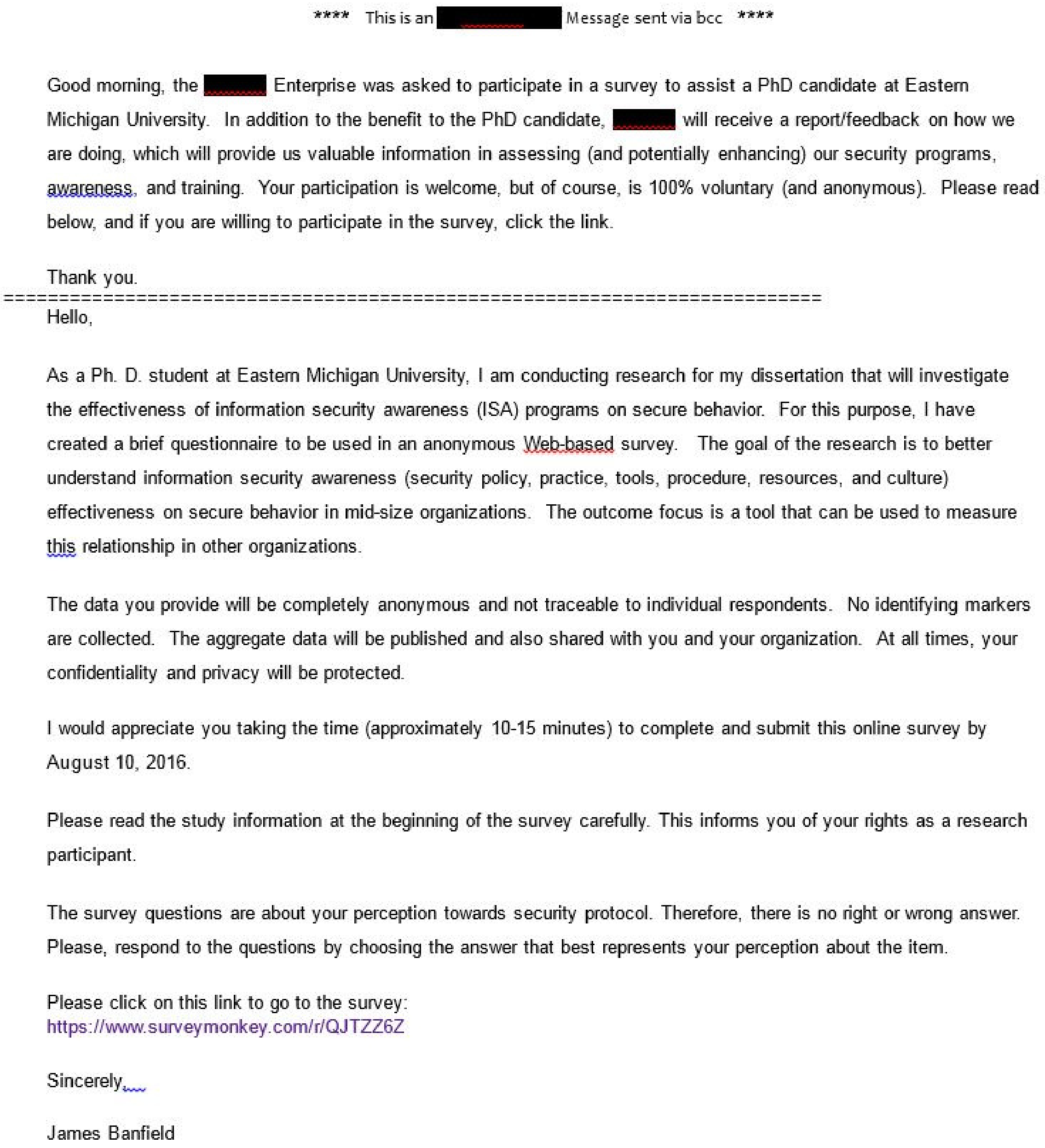
	EU3	Having a list of roles and responsibilities for security makes my role easier					
	EU4	Keeping up with corporate security training is not difficult					
	EU5	I find it easy to report activity that might cause data loss					
	Adapted from Taylor & Todd, 1995;Parsons, McCormac, Pattison, Butivicius, Jerram, 2014; Stanton et al., 2005; Davis, 1989						
Perceived usefulness of ISA (PU)	** Likert Scale (1=Strongly disagree 2=disagree 3=neutral 4=agree 5=strongly agree)						
	PU1	Being trained in organizational security practices will help my career					
	PU2	Being able to follow my organizational security policy is advantageous to me					
	PU3	Corporate security tools are not helpful to my job					
	PU4	My corporation could benefit from my understanding of our security practice					
	Adapted from Taylor & Todd, 1995;Parsons, McCormac, Pattison, Butivicius, Jerram, 2014; Stanton et al., 2005						
Perceived Supervisor Influence of ISA (SI)	** Likert Scale (1=Strongly disagree 2=disagree 3=neutral 4=agree 5=strongly agree)						
	SI1	I perform my role in security because management expects me to					

	SI2	I will use security tools because management requires it					
	SI3	Practicing good security is outlined as part of my job requirements					
	SI4	I follow good security practices because my supervisor does					
	Adapted from Taylor & Todd, 1995;Parsons, McCormac, Pattison, Butivicius, Jerram, 2014; Stanton et al., 2005						
	** Likert Scale (1=Strongly disagree 2=disagree 3=neutral 4=agree 5=strongly agree)						
Perceived peer influence of ISA (PI)	PI1	I would follow the corporate security policy if my co-workers told me it was important					
	PI2	I backup my local data mostly because others tell me it is important					
	PI3	I follow security practices that I read about on the Internet					
	PI4	I learn how to best protect data from my co-workers					
	Adapted from Taylor & Todd, 1995;Parsons, McCormac, Pattison, Butivicius, Jerram, 2014; Stanton et al., 2005						
	** Likert Scale (1=Strongly disagree 2=disagree 3=neutral 4=agree 5=strongly agree)						
ISA Self-efficacy (SE)	SE1	I am certain that I follow all of our organizational security practices					

	SE2	I am able to spot suspicious emails					
	SE3	I am adept at learning new security practices					
	SE4	I am aware of the security culture in my organization					
	Adapted from Taylor & Todd, 1995;Parsons, McCormac, Pattison, Butivicius, Jerram, 2014; Stanton et al., 2005						
	** Likert Scale (1=Strongly disagree 2=disagree 3=neutral 4=agree 5=strongly agree)						
ISA tool Self-efficacy (TSE)	TSE1	I am confident that I can use the security tools my organization has given me (anti-virus etc)					
	TSE2	I am capable of guarding passwords as guided by my organization					
	TSE3	I am able to learn new security tools/practices that pertain to my role					
	TSE4	I know what actions to take to remove a virus from my computer					
Security Intention (SINT)	Adapted from Taylor & Todd, 1995;Parsons, McCormac, Pattison, Butivicius, Jerram, 2014; Stanton et al., 2005						
	** Likert Scale (1=Strongly disagree 2=disagree 3=neutral 4=agree 5=strongly agree)						

	SINT2	I intend to make backup copies of my local files					
	SINT3	I intend to follow all security practice and policy					
	SINT4	I intend to be aware of secure procedures protecting digital data					
	SINT5	I will not share my password with anyone					
	SINT 6	I will not click on email attachments from unknown sources					
	SINT8	I will not access websites that are deemed inappropriate from my corporate provided systems (work computer, VPN,)					
	SINT9	I will not leave my work laptop physically unsecured when away from the office					
	SIN10	I will not post unapproved work data on social websites					
	SINT11	I will not "hack" into others computers					

Appendix C: Letter to Population



**** This is an [redacted] Message sent via bcc ****

Good morning, the [redacted] Enterprise was asked to participate in a survey to assist a PhD candidate at Eastern Michigan University. In addition to the benefit to the PhD candidate, [redacted] will receive a report/feedback on how we are doing, which will provide us valuable information in assessing (and potentially enhancing) our security programs, awareness, and training. Your participation is welcome, but of course, is 100% voluntary (and anonymous). Please read below, and if you are willing to participate in the survey, click the link.

Thank you.

==

Hello,

As a Ph. D. student at Eastern Michigan University, I am conducting research for my dissertation that will investigate the effectiveness of information security awareness (ISA) programs on secure behavior. For this purpose, I have created a brief questionnaire to be used in an anonymous Web-based survey. The goal of the research is to better understand information security awareness (security policy, practice, tools, procedure, resources, and culture) effectiveness on secure behavior in mid-size organizations. The outcome focus is a tool that can be used to measure this relationship in other organizations.

The data you provide will be completely anonymous and not traceable to individual respondents. No identifying markers are collected. The aggregate data will be published and also shared with you and your organization. At all times, your confidentiality and privacy will be protected.

I would appreciate you taking the time (approximately 10-15 minutes) to complete and submit this online survey by August 10, 2016.

Please read the study information at the beginning of the survey carefully. This informs you of your rights as a research participant.

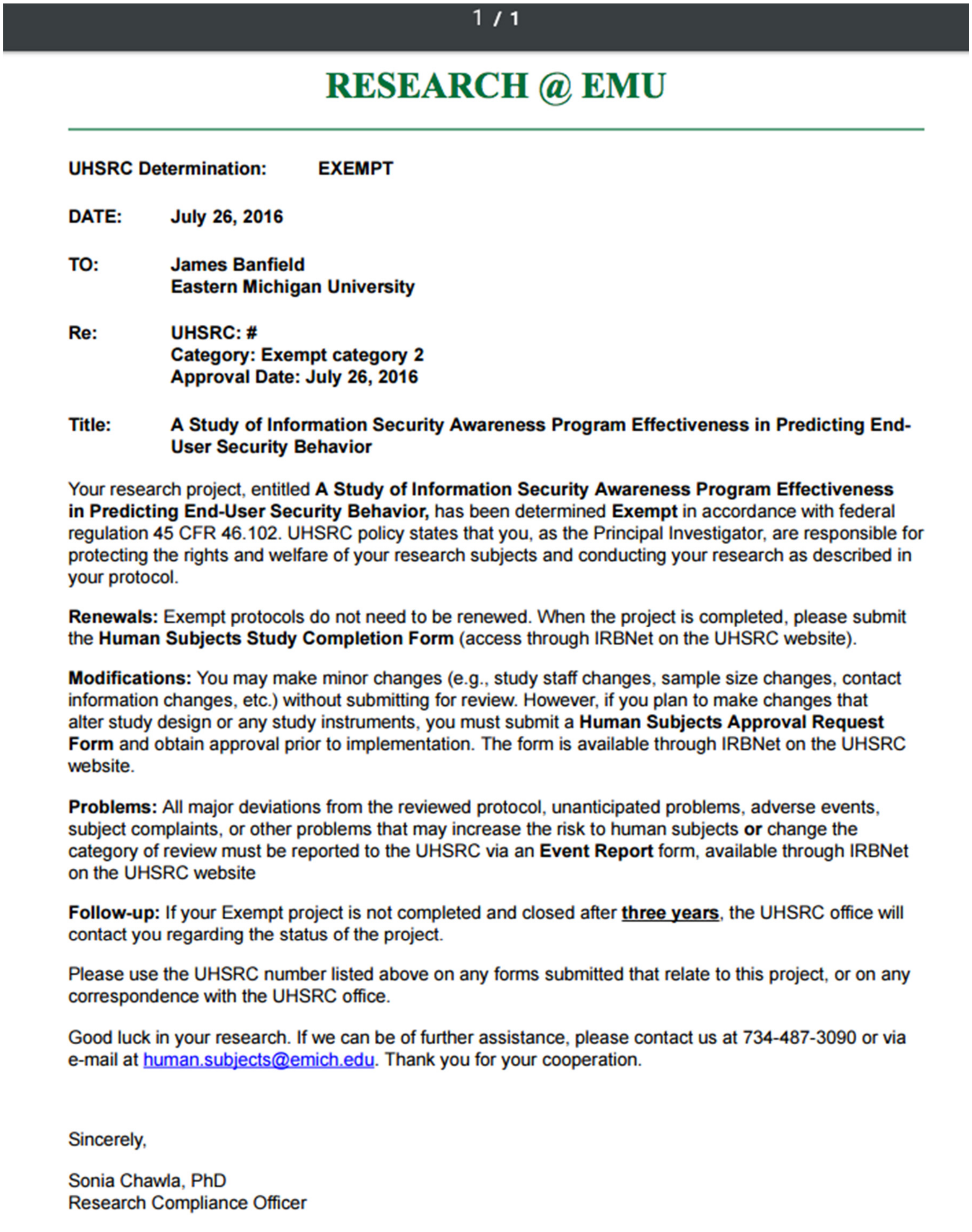
The survey questions are about your perception towards security protocol. Therefore, there is no right or wrong answer. Please, respond to the questions by choosing the answer that best represents your perception about the item.

Please click on this link to go to the survey:
https://www.surveymonkey.com/r/QJTZZ6Z

Sincerely,

James Banfield

Appendix D : Human Subjects



RESEARCH @ EMU

UHSRC Determination: EXEMPT

DATE: July 26, 2016

TO: James Banfield
Eastern Michigan University

Re: UHSRC: #
Category: Exempt category 2
Approval Date: July 26, 2016

Title: A Study of Information Security Awareness Program Effectiveness in Predicting End-User Security Behavior

Your research project, entitled **A Study of Information Security Awareness Program Effectiveness in Predicting End-User Security Behavior,** has been determined **Exempt** in accordance with federal regulation 45 CFR 46.102. UHSRC policy states that you, as the Principal Investigator, are responsible for protecting the rights and welfare of your research subjects and conducting your research as described in your protocol.

Renewals: Exempt protocols do not need to be renewed. When the project is completed, please submit the **Human Subjects Study Completion Form** (access through IRBNet on the UHSRC website).

Modifications: You may make minor changes (e.g., study staff changes, sample size changes, contact information changes, etc.) without submitting for review. However, if you plan to make changes that alter study design or any study instruments, you must submit a **Human Subjects Approval Request Form** and obtain approval prior to implementation. The form is available through IRBNet on the UHSRC website.

Problems: All major deviations from the reviewed protocol, unanticipated problems, adverse events, subject complaints, or other problems that may increase the risk to human subjects **or** change the category of review must be reported to the UHSRC via an **Event Report** form, available through IRBNet on the UHSRC website

Follow-up: If your Exempt project is not completed and closed after **three years**, the UHSRC office will contact you regarding the status of the project.

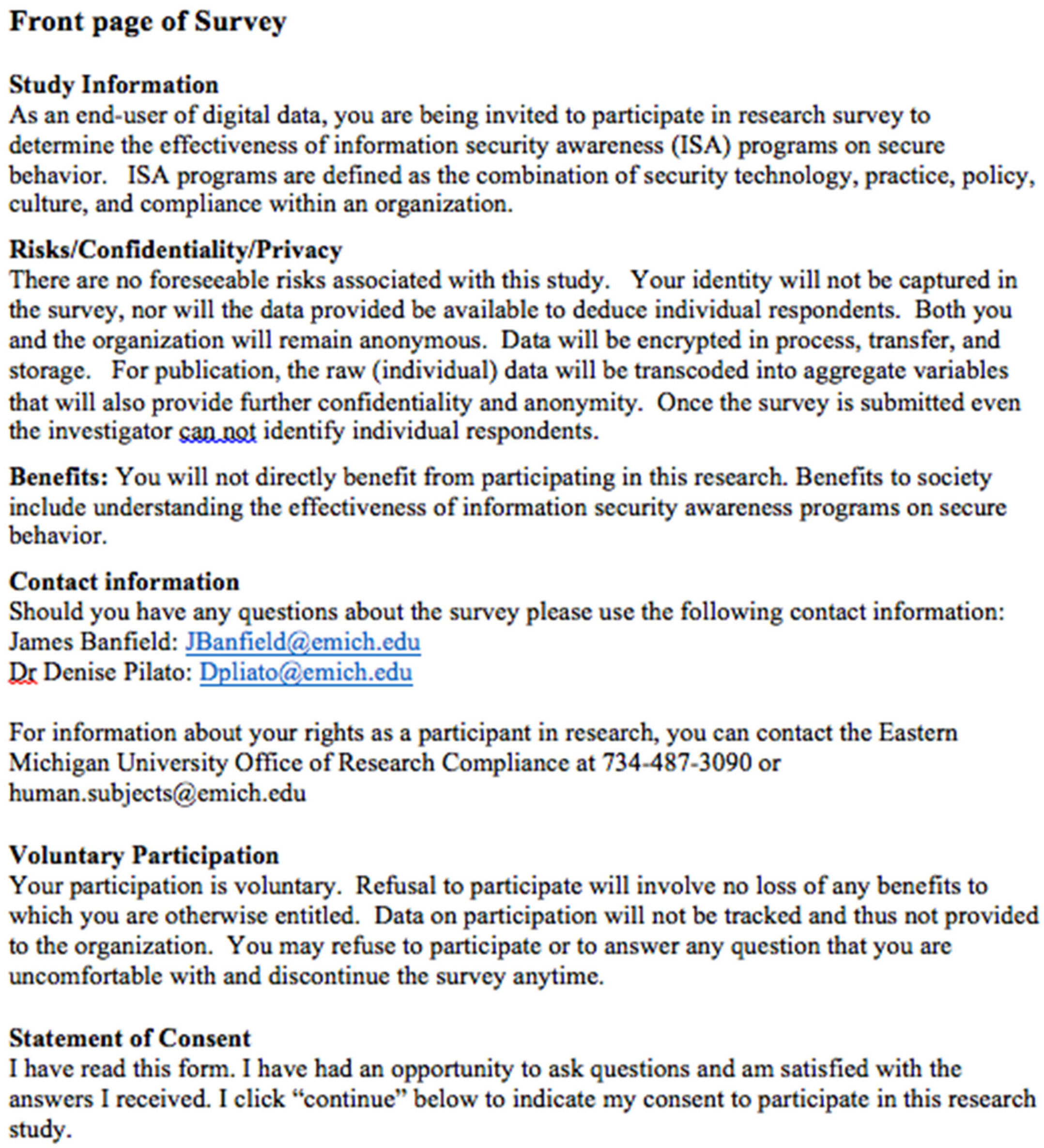
Please use the UHSRC number listed above on any forms submitted that relate to this project, or on any correspondence with the UHSRC office.

Good luck in your research. If we can be of further assistance, please contact us at 734-487-3090 or via e-mail at human.subjects@emich.edu. Thank you for your cooperation.

Sincerely,

Sonia Chawla, PhD
Research Compliance Officer

Appendix E : Consent Page



Front page of Survey

Study Information

As an end-user of digital data, you are being invited to participate in research survey to determine the effectiveness of information security awareness (ISA) programs on secure behavior. ISA programs are defined as the combination of security technology, practice, policy, culture, and compliance within an organization.

Risks/Confidentiality/Privacy

There are no foreseeable risks associated with this study. Your identity will not be captured in the survey, nor will the data provided be available to deduce individual respondents. Both you and the organization will remain anonymous. Data will be encrypted in process, transfer, and storage. For publication, the raw (individual) data will be transcoded into aggregate variables that will also provide further confidentiality and anonymity. Once the survey is submitted even the investigator can not identify individual respondents.

Benefits: You will not directly benefit from participating in this research. Benefits to society include understanding the effectiveness of information security awareness programs on secure behavior.

Contact information

Should you have any questions about the survey please use the following contact information:
James Banfield: JBanfield@emich.edu
Dr Denise Pilato: Dpliato@emich.edu

For information about your rights as a participant in research, you can contact the Eastern Michigan University Office of Research Compliance at 734-487-3090 or human.subjects@emich.edu

Voluntary Participation

Your participation is voluntary. Refusal to participate will involve no loss of any benefits to which you are otherwise entitled. Data on participation will not be tracked and thus not provided to the organization. You may refuse to participate or to answer any question that you are uncomfortable with and discontinue the survey anytime.

Statement of Consent

I have read this form. I have had an opportunity to ask questions and am satisfied with the answers I received. I click “continue” below to indicate my consent to participate in this research study.

Appendix F: Item Level Frequency

A Study of Information Security Awareness Program Effectiveness in Predicting End-Use Security Behavior

1. Consent

Answer Options	Response Percent	Response Count
Yes	1	109
No	0	0
answered question	109	109
skipped question	0	0

2. What is your age?

Answer Options	Response Percent	Response Count
19-30	0.165	18
31-40	0.266	29
41-50	0.257	28
50-60	0.193	21
60 and above	0.119	13
answered question	109	109
skipped question	0	0

3. What is your gender?

Answer Options	Response Percent	Response Count
Female	0.615	67
Male	0.385	42
answered question	109	109
skipped question	0	0

4. What is the highest level of education you have completed?

Answer Options	Response Percent	Response Count
Graduated from high school	0.101	11
Graduated from 2 year college	0.028	3
Graduated from college	0.358	39
Completed graduate school	0.514	56
answered question	109	109
skipped question	0	0

5. How often do you work with other employees at the company?

Answer Options	Response Percent	Response Count
1-2 hours per day	0.321	35
3-4 hours per day	0.257	28
More than 5 hours per day	0.422	46
answered question	109	109
skipped question	0	0

6. Have you received corporate security training?

Answer Options	Response Percent	Response Count
Yes	0.963	105
No	0.037	4
answered question	109	109
skipped question	0	0

7. Following my corporate security policy is difficult for me

Answer Options	Response Percent	Response Count
Strongly disagree	0.272	28
Disagree	0.534	55
Nuetral	0.097	10
Agree	0.087	9
Strongly Agree	0.01	1
answered question	103	103
skipped question	6	6

8. Following my corporate security policy is easy for me

Answer Options	Response Percent	Response Count
Strongly disagree	0	0
Disagree	0.087	9
Nuetral	0.097	10
Agree	0.544	56
Strongly Agree	0.272	28
answered question	103	103
skipped question	6	6

9. Having a list of roles and responsibilities for security makes my role easier

Answer Options	Response Percent	Response Count
Strongly disagree	0	0
Disagree	0.049	5
Nuetral	0.214	22
Agree	0.553	57
Strongly Agree	0.184	19
answered question	103	103
skipped question	6	6

10. Keeping up with corporate security training is not difficult

Answer Options	Response Percent	Response Count
Strongly disagree	0	0
Disagree	0.068	7
Nuetral	0.165	17
Agree	0.534	55
Strongly Agree	0.233	24
answered question	103	103

skipped question	6	6

11. I find it easy to report activity that might cause data loss

Answer Options	Response Percent	Response Count
Strongly disagree	0.019	2
Disagree	0.049	5
Nuetral	0.252	26
Agree	0.427	44
Strongly Agree	0.252	26
answered question	103	103
skipped question	6	6

12. Being trained in organizational security practices will help my career

Answer Options	Response Percent	Response Count
Strongly disagree	0.01	1
Disagree	0.117	12
Nuetral	0.223	23
Agree	0.427	44
Strongly Agree	0.223	23
answered question	103	103
skipped question	6	6

13. Being able to follow my organizational security policy is advantageous to me

Answer Options	Response Percent	Response Count
Strongly disagree	0	0
Disagree	0.029	3
Nuetral	0.146	15
Agree	0.524	54
Strongly Agree	0.301	31
answered question	103	103
skipped question	6	6

14. Corporate security tools are not helpful to my job

Answer Options	Response Percent	Response Count
Strongly disagree	0.262	27
Disagree	0.427	44
Nuetral	0.223	23
Agree	0.078	8
Strongly Agree	0.01	1
answered question	103	103
skipped question	6	6

15. My corporation could benefit from my understanding of our security practice

Answer Options	Response Percent	Response Count
Strongly disagree	0.019	2

Disagree	0.058	6
Nuetral	0.291	30
Agree	0.447	46
Strongly Agree	0.184	19
answered question	103	103
skipped question	6	6

16. I perform my role in security because management expects me to

Answer Options	Response Percent	
Strongly disagree	0.029	3
Disagree	0.097	10
Nuetral	0.165	17
Agree	0.495	51
Strongly Agree	0.214	22
answered question	103	103
skipped question	6	6

17. I will use security tools because management requires it

Answer Options	Response Percent	Response Count
Strongly disagree	0.029	3
Disagree	0.058	6
Nuetral	0.117	12
Agree	0.515	53
Strongly Agree	0.282	29
answered question	103	103
skipped question	6	6

18. Practicing good security is outlined as part of my job requirements

Answer Options	Response Percent	Response Count
Strongly disagree	0.01	1
Disagree	0.068	7
Nuetral	0.097	10
Agree	0.427	44
Strongly Agree	0.398	41
answered question	103	103
skipped question	6	6

19. I follow good security practices because my supervisor does

Answer Options	Response Percent	Response Count
Strongly disagree	0.068	7
Disagree	0.184	19
Nuetral	0.427	44
Agree	0.223	23
Strongly Agree	0.097	10
answered question	103	103
skipped question	6	6

20. I would follow the corporate security policy if my co-workers told me it was important

Answer Options	Response Percent	Response Count
Strongly disagree	0.029	3
Disagree	0.107	11
Nuetral	0.262	27
Agree	0.398	41
Strongly Agree	0.204	21
answered question	103	103
skipped question	6	6

21. I backup my local data mostly because others tell me it is important

Answer Options	Response Percent	Response Count
Strongly disagree	0.087	9
Disagree	0.456	47
Nuetral	0.32	33
Agree	0.107	11
Strongly Agree	0.029	3
answered question	103	103
skipped question	6	6

22. I follow security practices that I read about on the Internet

Answer Options	Response Percent	Response Count
Strongly disagree	0.039	4
Disagree	0.291	30
Nuetral	0.311	32
Agree	0.291	30
Strongly Agree	0.068	7
answered question	103	103
skipped question	6	6

23. I learn how to best protect data from my co-workers

Answer Options	Response Percent	Response Count
Strongly disagree	0.058	6
Disagree	0.233	24
Nuetral	0.262	27
Agree	0.34	35
Strongly Agree	0.107	11
answered question	103	103
skipped question	6	6

24. I am certain that I follow all of our organizational security practices

Answer Options	Response Percent	Response Count
Strongly disagree	0	0
Disagree	0.087	9

Nuetral	0.175	18
Agree	0.612	63
Strongly Agree	0.126	13
answered question	103	103
skipped question	6	6

25. I am able to spot suspicious emails

Answer Options	Response Percent	Response Count
Strongly disagree	0	0
Disagree	0	0
Nuetral	0.049	5
Agree	0.563	58
Strongly Agree	0.388	40
answered question	103	103
skipped question	6	6

26. I am adept at learning new security practices

Answer Options	Response Percent	Response Count
Strongly disagree	0.01	1
Disagree	0.019	2
Nuetral	0.194	20
Agree	0.563	58
Strongly Agree	0.214	22
answered question	103	103
skipped question	6	6

27. I am aware of the security culture in my organization

Answer Options	Response Percent	Response Count
Strongly disagree	0	0
Disagree	0.078	8
Nuetral	0.068	7
Agree	0.621	64
Strongly Agree	0.233	24
answered question	103	103
skipped question	6	6

28. I am confident that I can use the security tools my organization has given me (anti-virus etc)

Answer Options	Response Percent	Response Count
Strongly disagree	0	0
Disagree	0.049	5
Nuetral	0.078	8
Agree	0.583	60
Strongly Agree	0.291	30
answered question	103	103
skipped question	6	6

29. I am capable of guarding passwords as guided by organization

Answer Options	Response Percent	Response Count
Strongly disagree	0	0
Disagree	0	0
Nuetral	0.039	4
Agree	0.369	38
Strongly Agree	0.592	61
answered question	103	103
skipped question	6	6

30. I am able to learn new security tools/practices that pertain to my role

Answer Options	Response Percent	Response Count
Strongly disagree	0	0
Disagree	0.01	1
Nuetral	0.107	11
Agree	0.583	60
Strongly Agree	0.301	31
answered question	103	103
skipped question	6	6

31. I know what actions to take to remove a virus from my computer

Answer Options	Response Percent	Response Count
Strongly disagree	0.049	5
Disagree	0.282	29
Nuetral	0.155	16
Agree	0.35	36
Strongly Agree	0.165	17
answered question	103	103
skipped question	6	6

32. I intend to make backup copies of my local files

Answer Options	Response Percent	Response Count
Strongly disagree	0.029	3
Disagree	0.184	19
Nuetral	0.301	31
Agree	0.262	27
Strongly Agree	0.223	23
answered question	103	103
skipped question	6	6

33. I intend to follow all security practice and policy

Answer Options	Response Percent	Response Count
Strongly disagree	0.01	1
Disagree	0	0
Nuetral	0.039	4

Agree	0.485	50
Strongly Agree	0.466	48
answered question	103	103
skipped question	6	6

34. I intend to be aware of secure procedures protecting digital data

Answer Options	Response Percent	Response Count
Strongly disagree	0	0
Disagree	0	0
Nuetral	0.107	11
Agree	0.515	53
Strongly Agree	0.379	39
answered question	103	103
skipped question	6	6

35. I will not share my password with anyone

Answer Options	Response Percent	Response Count
Strongly disagree	0	0
Disagree	0.01	1
Nuetral	0.01	1
Agree	0.233	24
Strongly Agree	0.748	77
answered question	103	103
skipped question	6	6

36. I will always log off or lockout my computer when it is unattended

Answer Options	Response Percent	Response Count
Strongly disagree	0.039	4
Disagree	0.165	17
Nuetral	0.126	13
Agree	0.398	41
Strongly Agree	0.272	28
answered question	103	103
skipped question	6	6

37. I will not click on email attachments from unknown sources

Answer Options	Response Percent	Response Count
Strongly disagree	0	0
Disagree	0.01	1
Nuetral	0.019	2
Agree	0.379	39
Strongly Agree	0.592	61
answered question	103	103
skipped question	6	6

38. I will not leave my work laptop physically unsecured when away from the office

Answer Options	Response Percent	Response Count
Strongly disagree	0.039	4
Disagree	0.087	9
Nuetral	0.058	6
Agree	0.427	44
Strongly Agree	0.388	40
answered question	103	103
skipped question	6	6

39. I will not post unapproved work data on social websites

Answer Options	Response Percent	Response Count
Strongly disagree	0	0
Disagree	0	0
Nuetral	0	0
Agree	0.184	19
Strongly Agree	0.816	84
answered question	103	103
skipped question	6	6

40. I will not "hack" into others computers

Answer Options	Response Percent	Response Count
Strongly disagree	0.01	1
Disagree	0.01	1
Nuetral	0	0
Agree	0.087	9
Strongly Agree	0.893	92
answered question	103	103
skipped question	6	6

Appendix G

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
What is your age?	109	1.00	5.00	2.8349	1.25841
What is your gender?	109	1.00	2.00	1.3853	.48892
What is the highest level of education you have completed?	109	1.00	4.00	3.2844	.93385
How often do you work with other employees at the company?	109	1.00	3.00	2.1009	.86007
Have you received corporate security training?	109	1.00	2.00	1.0367	.18889
Following my corporate security policy is difficult for me	103	1.00	5.00	2.0291	.90159

Following my corporate security policy is easy for me	103	2.00	5.00	4.0000	.85176
Having a list of roles and responsibilities for security makes my role easier	103	2.00	5.00	3.8738	.76286
Keeping up with corporate security training is not difficult	103	2.00	5.00	3.9320	.81964
I find it easy to report activity that might cause data loss	103	1.00	5.00	3.8447	.92628
Being trained in organizational security practices will help my career	103	1.00	5.00	3.7379	.96975
Being able to follow my organizational security policy is advantageous to me	103	2.00	5.00	4.0971	.74774
Corporate security tools are not helpful to my job	103	1.00	5.00	2.1456	.93313

My corporation could benefit from my understanding of our security practice	103	1.00	5.00	3.7184	.90117
I perform my role in security because management expects me to	103	1.00	5.00	3.7670	.99216
I will use security tools because management requires it	103	1.00	5.00	3.9612	.94891
Practicing good security is outlined as part of my job requirements	103	1.00	5.00	4.1359	.91874
I follow good security practices because my supervisor does	103	1.00	5.00	3.0971	1.03388
I would follow the corporate security policy if my co-workers told me it was important	103	1.00	5.00	3.6408	1.01802
I backup my local data mostly because others tell me it is important	103	1.00	5.00	2.5340	.90549

I follow security practices that I read about on the Internet	103	1.00	5.00	3.0583	1.00806
I learn how to best protect data from my co-workers	103	1.00	5.00	3.2039	1.09687
I am certain that I follow all of our organizational security practices	103	2.00	5.00	3.7767	.77879
I am able to spot suspicious emails	103	3.00	5.00	4.3398	.56972
I am adept at learning new security practices	103	1.00	5.00	3.9515	.75898
I am aware of the security culture in my organization	103	2.00	5.00	4.0097	.78584
I am confident that I can use the security tools my organization has given me (anti-virus etc)	103	2.00	5.00	4.1165	.74493

I am capable of guarding passwords as guided by organization	103	3.00	5.00	4.5534	.57272
I am able to learn new security tools/practices that pertain to my role	103	2.00	5.00	4.1748	.64818
I know what actions to take to remove a virus from my computer	103	1.00	5.00	3.3010	1.18681
I intend to make backup copies of my local files	103	1.00	5.00	3.4660	1.11861
I intend to follow all security practice and policy	103	1.00	5.00	4.3981	.66184
I intend to be aware of secure procedures protecting digital data	103	3.00	5.00	4.2718	.64465
I will not share my password with anyone	103	2.00	5.00	4.7184	.53169

I will always log off or lockout my computer when it is unattended	103	1.00	5.00	3.6990	1.15330
I will not click on email attachments from unknown sources	103	2.00	5.00	4.5534	.58959
I will not leave my work laptop physically unsecured when away from the office	103	1.00	5.00	4.0388	1.07487
I will not post unapproved work data on social websites	103	4.00	5.00	4.8155	.38976
I will not "hack" into others computers	103	1.00	5.00	4.8447	.55585
Valid N (listwise)	103				