2020

Impact of Sanctions and Awareness on Intention to Comply with Information Security

Kevin Fitzgerald
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

Kevin A. Fitzgerald

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Robert Levasseur, Committee Chairperson, Management Faculty
Dr. Kimberly Anthony, Committee Member, Management Faculty
Dr. Robert Kilmer, University Reviewer, Management Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2020

Abstract

Impact of Sanctions and Awareness on Intention to Comply with Information Security Policy

by

Kevin A. Fitzgerald

MPhil, Walden University, 2019

MBA, Southern Nazarene University, 2009

BS, Southern Nazarene University, 2006

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

August 2020

Abstract

Employees in higher education are likely to violate information security policies because of the open nature of academic institutions. Policy violations can lead to data breaches and identity theft that can cause harm to businesses and individuals. The purpose of this quantitative, correlational, cross-sectional study based on general deterrence theory and neutralization theory was to analyze the relationships between the independent variables, *severity of sanctions, vulnerability to sanctions, and awareness of consequences,* and the dependent variable, *intention to comply with information security policy*. Participants (n=100) who work in a higher education institution with an information security policy completed an online survey. Multiple linear regression analysis showed that all of the independent variables had a significant relationship with the dependent variable *intention*. *Severity* had the strongest relationship, followed by *awareness* and then *vulnerability*. Understanding the relationships between the *severity, vulnerability, awareness,* and the dependent variable *intention* may aid information security practitioners in creating programs that increase compliance with information security and decrease the number of data breaches. Decreasing the number of data breaches could reduce the incidents of identity theft, fraud, compromised medical records, and small business bankruptcies, thus contributing to positive social change.

Impact of Sanctions and Awareness on Intention to Comply with Information Security Policy

by

Kevin A. Fitzgerald

MPhil, Walden University, 2019

MBA, Southern Nazarene University, 2009

BS, Southern Nazarene University, 2006

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

August 2020

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Maintaining information security is vital for businesses in today's electronically based information economy. Organizational leaders must be diligent in defining and enforcing the policies and procedures for ensuring that sensitive information is not lost in a data breach. Employees are resistant to complying with information security policies (ISP) because they require extra effort and time (Lee, Lee, & Kim, 2016) and can impede work processes (Hwang, Kim, Kim, & Kim, 2017). The focus of this study was measuring the impact that sanction severity, sanction vulnerability, and awareness have on the intention to comply with information security policy (ISP) in higher education institutions and determining which factors had the most substantial impact. Increasing compliance with ISP could reduce the incidence of data breaches and the resulting damage.

In Chapter 1 of this proposal, I provide the background information on the topic, explain the theories associated with the study, and identify the gaps in the research that justify this study. This chapter contains a statement of the problem, the study purpose, the research questions, and hypotheses of the study. The chapter also contains an identification of the theoretical foundations used in the research model and an explanation of the nature of the study, as well as definitions, assumptions, scope, and delimitations. This chapter concludes with the significance of the study in addressing the research gap, improving practices, and positively impacting social change.

Background of the Study

Beccaria (1963) created general deterrence theory (GDT) in 1764. GDT is the basis for enforcement policies, such as information security policies (Boss, Galletta, Lowry, Moody, & Polak, 2015). Cheng, Li, Zhai, and Smyth (2014) found that sanctions had little or no effect on the intention to use the internet for personal reasons in the workplace. Johnston, Warkentin, and Siponen (2015) found that formal sanctions have no effect on the intention to comply with ISP and noted that there are inconsistent findings on the effect of formal and informal sanctions on compliance with ISP. Hedström, Karlsson, and Kolkowska (2013) noted that the severity of sanctions is not strongly correlated with ISP compliance.

Conversely, D'Arcy, Herath, and Shoss (2014) found that sanctions are effective in preventing cognitive rationalizations that lead to ISP violations. Sommestad, Hallberg, Lundholm, and Bengtsson (2014) noted that the perceived severity of penalties for failure to comply with ISP has a strong negative correlation with attitude toward violation, but a weak negative correlation with the intention to violate ISP. Unlike criminology studies that consistently support the idea that sanctions are an effective deterrent to deviant behavior (Ifinedo, 2014), there is a lack of agreement on the efficacy of sanctions in increasing ISP compliance (Goo, Yim, & Kim, 2014).

Sykes and Matza (1957) developed neutralization theory (NT), which indicates that individuals who choose to violate a behavioral norm will typically have some form of guilt and may justify the behavior using a neutralization technique. Barlow, Warkentin, Ormond, and Dennis (2013) found that employees often violate ISP even under the threat of sanctions because they use neutralization techniques to reduce the perception of negative consequences of deterrence. Bauer, Chudzikowski, and Bernroider (2017) found that members of an organization use neutralization to justify violating ISP and suggested the need for more research on how individuals use neutralization to justify policy violations. Studies conducted by Cheng, Li, Li, Holm, and Zhai (2013) and Cheng et al. (2014) found that employees think about neutralization more than they think about sanctions.

Barlow, Warkentin, Ormond, and Dennis (2018) found correlations between the use of neutralization and non-compliance with ISP and noted that anti-neutralization messages reduced non-compliance. Klockars (1974) extended NT with the metaphor of the ledger, where the violator believes that the cumulative value of good actions can outweigh the cumulative value of bad actions. Teh, Ahmed, and D'Arcy (2015) found correlations between the use of the metaphor of the ledger neutralization technique and violating ISP.

Researchers have questioned if there is any conclusive evidence that can be used to design information security awareness programs that are effective (Bauer et al., 2017). Han, Kim, and Kim (2017) found that while there is abundant research on information security technology, research on employee behavior is scant. D'Arcy et al. (2014) noted that knowledge of the factors that influence the decision to comply or not comply with ISP is incomplete and that there had not been enough studies on information security, especially as it relates to the connection between information security awareness and ISP compliance behavior. More research that explores the factors affecting compliance with ISP (Ifinedo, 2014), and the gap in the literature on the reasons individuals choose not to comply with ISP (Siponen & Vance, 2014), is necessary.

I conducted this study to address gaps in the literature on the most effective means of enforcing ISP. Determining a more effective means of enforcing ISP compliance is important given that managing employees in a way that encourages compliance with ISP is the most difficult part of maintaining information technology security (Hwang et al., 2017). Understanding what motivates individuals to comply with ISP could lead to programs and policies that encourage compliance and reduce the number of data breaches.

Problem Statement

Over 3,100 data breaches occurred in the United States between 2005 and 2012, resulting in over 510 million records with personal information being obtained by unauthorized individuals (Holtfreter & Harrington, 2015). Leaders in institutions of higher education have experienced frequent and damaging data breaches (Al-diabat, 2018) with a university in Texas having approximately 200,000 student records with social security numbers being illegally accessed and a university in California exposing the names and social security numbers of 98,000 students (Kam & Katerattanakul, 2014). Higher education institutions are susceptible to data breaches because of the open nature of academic institutions (Weidman & Grossklags, 2018). Research has revealed that nearly a third of users in higher education have opened emails with malicious attachments (Rajab & Eydgahi, 2019). Organizations have implemented security, education, awareness, and training (SETA) programs and ISP in an attempt to prevent data breaches, but organizational leaders still find that over 50% of breaches are caused by employees not complying with ISP (D'Arcy & Greene, 2014).

When unauthorized individuals gain access to data, they may use the data to commit crimes (Teh et al., 2015) such as identity theft, which is the act of using another person's identity to commit fraud (Holtfreter & Harrington, 2015). When data breaches involved the theft of medical records, sensitive information (Kuo, Ma, & Alexander, 2014) such as social security numbers, and indications of mental illness, AIDS, or cancer (Li & Slee, 2014) can be made public and expose the victims to serious harm (Kuo et al., 2014). Organizations suffer financial loss (Clapper & Richmond, 2016) and damage to their reputations (Hedström et al., 2013) when data breaches occur. The average cost of a data breach is $6.5 million, and the financial damage caused by data breaches can force small businesses to close (Clapper & Richmond, 2016).

The general problem is that data breaches can result in financial damage to organizations. The specific problem is the lack of knowledge of the relationships between deterrence and compliance, and awareness and compliance when employees in higher education decide not to comply with ISP. Han et al. (2017) found that while there is abundant research on information security technology, research on employee behavior is scant, and more research is needed to determine the factors that affect compliance with

ISP. More knowledge of the factors associated with compliance is needed (Humaidi & Balakrishnan, 2015) to address the gap in the research on why individuals choose to violate ISP (Siponen & Vance, 2010).

Purpose of Study

The purpose of this quantitative study was to measure the impact that sanction severity, sanction vulnerability, and awareness of the consequences have on the intention to comply with ISP. There were three independent variables: sanction severity, referenced in this study as *severity*, which is the harshness of the sanctions; sanction vulnerability, referenced in this study as *vulnerability*, which is the likelihood that sanctions will occur; and awareness of consequences, which is the knowledge that behavior affects the welfare of others, referenced in this study as *awareness*. The dependent variable was the intention to comply with ISP, referenced in this study as *intention*. Employees in the United States working in higher education institutions with an ISP completed a survey. I used multiple regression analysis to measure the relationships between the independent and dependent variables. Determining whether there are significant relationships between the independent variables and the dependent variable, and how much each of the independent variables explain the variation in the dependent variable *intention* could contribute to the knowledge of the antecedents that lead to ISP compliance. A greater understanding of the factors that lead to ISP compliance could enable information security officials to create policies, education, tools, and enforcement programs that would increase compliance with ISP and reduce the number of data breaches.

Research Questions and Hypotheses

RQ1: What is the relationship between *severity* and *intention*?

$H_0$1: There is no relationship between *severity* and *intention*.

H_a1: There is a relationship between *severity* and *intention*.

RQ2: What is the relationship between *vulnerability* and *intention*?

$H_0$2: There is no relationship between *vulnerability* and *intention*.

H_a2: There is a relationship between *vulnerability* and *intention*.

RQ3: What is the relationship between *awareness* and *intention*?

$H_0$3: There is no relationship between *awareness* and *intention*.

H_a3: There is a relationship between *awareness* and *intention*.

RQ4: What is the relationship between *severity*, *vulnerability*, and *awareness*, taken collectively, and *intention*?

$H_0$4: There is no relationship between severity, vulnerability, and awareness, taken collectively, and intention.

H_a4: There is a relationship between *severity*, *vulnerability*, and *awareness*, taken collectively, and *intention*.

A theoretical model of the relationships between the three independent variables *severity*, *vulnerability*, and *awareness*, and the dependent variable *intention* is shown in Figure 1.

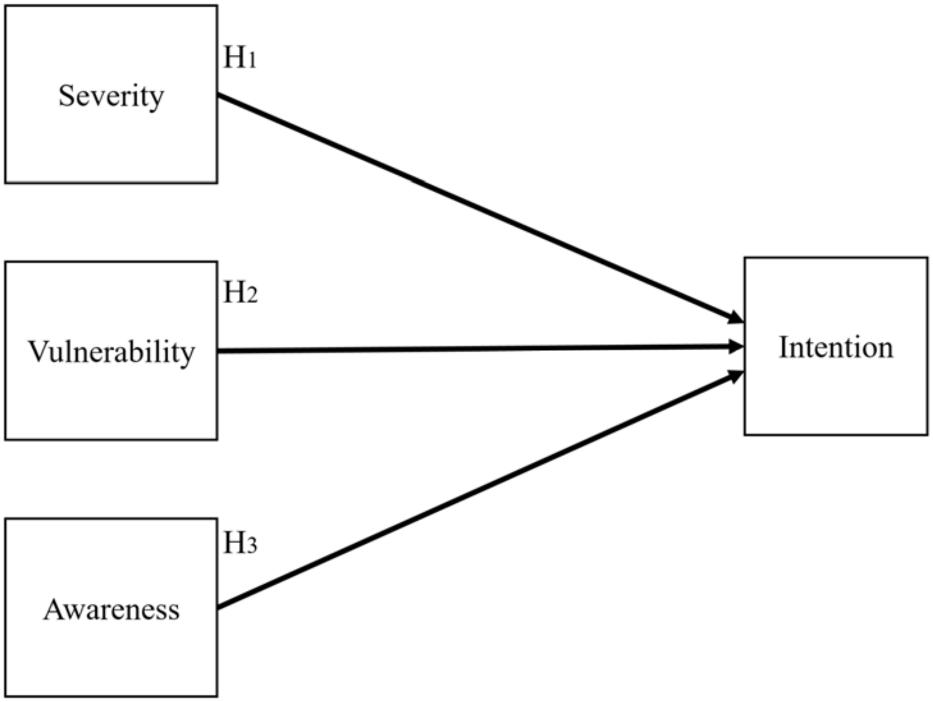


Figure 1. Conceptual Model of Hypotheses.

Theoretical Foundation

The theoretical framework for this study used GDT and NT. GDT (Beccaria, 1963) indicates that the threat of punishment deters crimes or violations of rules such as not complying with ISP (Johnston et al., 2015) and explains the processes used and behaviors expected in organizations that use the threat of sanctions to enforce ISP. The independent variables *severity* and *vulnerability* originate with GDT (Beccaria, 1963).

Researchers have defined awareness as knowing and understanding safe information security behavior (Parsons et al., 2017) or knowledge of information security policies (Safa, Von Solms, & Furnell, 2016). The origin of the variable *awareness* in this study came from work done by Yazdanmehr and Wang (2016) in which they defined awareness as an understanding of how one's behavior affects the well-being of others. Two other studies used similar descriptions. Dang-Pham and Pittayachawan (2015) defined awareness as knowledge of the severity and vulnerability of a threat to an organizational asset. Yang and Lee (2016) defined awareness as the knowledge of the damage that a data breach could cause to information systems.

NT (Sykes & Matza, 1957) explains how individuals justify violating rules such as not complying with ISP by nullifying the societal norm against committing the violation (Kim, Yang, & Park, 2014). The metaphor of the ledger neutralization technique developed by Klockars in 1974 indicates that a person will balance bad acts with good acts (Klockars, 1974). In the study of ISP compliance, the individual may use the metaphor of the ledger technique to justify violating ISP (Teh et al., 2015) by putting non-compliance on the bad side of the ledger and efficient execution of job duties on the good side of the ledger.

General Deterrence Theory

The origin of GDT comes from the writings of Cesare Beccaria, published in 1764 (Beccaria, 1963). Jeremy Bentham also contributed to GDT in the late 1700s (Johnston et al., 2015). GDT indicates that a person will compare the potential gains from committing a criminal act to the potential punishment they might receive for committing the act and rationally choose an action based on the opportunities for gain and the risk of sanctions (Barlow et al., 2013; Hedström et al., 2013; Johnston et al., 2015; Lowry, Posey, Bennett, & Roberts, 2015).

Beccaria detested the use of torture as a way of punishing criminals and asserted that the purpose of sanctions was not to make criminals pay for their crimes, because there was no way to undo a crime or bring back one who had been murdered (Beccaria, 1963). Instead, Beccaria (1963) proposed that the purpose of sanctions was to deter the criminal, and other potential criminals, from committing crimes in the future. Beccaria wrote that there are three elements of punishment. The first is the harshness or severity of the punishment, the second is the likelihood or vulnerability of the punishment, and the third is the time between the crime and the punishment, which is called the celerity of the sanction (Beccaria, 1963). While researchers initially used GDT in the study of criminology (Cheng et al., 2013; Lebek, Uffen, Neumann, Hohler, & Breitner, 2014), GDT has been used in many studies on ISP violation (Barlow et al., 2013; Boss et al., 2015; Cheng et al., 2014; Han et al., 2017). Past studies have found inconclusive evidence to support the GDT model in ISP compliance (Han et al., 2017; Hedström et al., 2013; Ifinedo, 2016). Chapter 2 contains more details about GDT and studies based on the theory.

Neutralization Theory

Sykes and Matza (1957) developed NT as a way of explaining delinquent behavior. The basis for existing theories on delinquent behavior was the assumption that individuals committed deviant acts because of an inverted moral code and disdain for societal norms (Sykes & Matza, 1957). Sykes and Matza found that delinquents had the same moral code as other citizens, but were able to nullify feelings of guilt by justifying deviant behaviors using neutralization techniques.

The first version of NT defined five techniques for neutralization that included denial of responsibility, denial of injury, denial of the victims, condemnation of the condemners, and appeal to higher loyalty (Sykes & Matza, 1957). Researchers added other techniques such as the defense of ubiquity technique (Coleman, 1987), the defense of necessity technique (Minor, 1981), and the metaphor of the ledger technique added by Klockars in 1974 that explained that individuals sometimes justify deviant acts by claiming that a large number of good deeds compensates for a small number of bad deeds.

In this study on sanctions, awareness, and compliance, the metaphor of the ledger was the mechanism that explains how individuals justify non-compliance with ISP. Siponen and Vance (2010), Barlow et al. (2013), Kim et al. (2014), Cheng et al. (2014), and Barlow et al. (2018) found positive correlations between the use of neutralization techniques and non-compliance with ISP. Teh et al. (2015) found that individuals with low organizational commitment were more likely to use neutralization techniques than individuals with high organizational commitment. Chapter 2 contains a detailed explanation of neutralization techniques and studies that used the theory.

Nature of the Study

The study was a quantitative correlational study with multiple regression analysis using the IBM Statistical Package for the Social Sciences (SPSS) program. Research questions about the strength of the relationship between independent variables and a dependent variable often require the use of multiple regression to answer (Tonidandel, LeBreton, & Johnson, 2009). Participants provided data in an anonymous online survey. Anonymous surveys increased the likelihood that valid information was obtained from the participants (Fox, Murray, & Warm, 2003). The survey contained questions developed and validated in previous studies conducted by Herath and Rao (2009) and Yazdanmehr and Wang (2016) and measured the three independent variables, *severity*, *vulnerability*, and *awareness*, and the dependent variable *intention*. Herath and Rao provided permission to use the survey questions that measure *severity, vulnerability,* and *intention* in the study, and Yazdanmehr and Wang provided permission to use the questions that measure *awareness*. Copies of the written consent for the instrument are in Appendix A. Chapter 3 contains details about validation of the instruments.

The sample was a random selection of 100 employees in the United States working in higher education institutions who self-report as working in an organization with an ISP. I determined the appropriate sample size for the study using the G*Power program. The inputs were set to (a) an alpha level of .05 so that the possibility of a Type I error is less than 5%, (b) a power of .80, (c) three predictors, and (d) a medium effect size. While the results of the G*Power analysis indicated that the sample size should be 77, self-reported data about complying with policies is likely to be skewed (Barlow et al., 2013) and therefore a larger sample was necessary to ensure the power of the statistical analysis. I analyzed the data using multiple regression to determine which of the independent variables explained the most variation in the independent variable. Multiple regression provides robust statistical power for skewed data sets of 100 samples when there are fewer than five variables (Allison, 1999). Consequently, the sample size for the research was 100.

Definitions

Awareness: The knowledge that one's behavior affects the well-being of others (Yazdanmehr & Wang, 2016). Awareness is an independent variable in this study.

Data breach: An event where confidential, protected, or sensitive data becomes available to individuals not authorized to possess or view the data, thus compromising the integrity and availability of the data (Sen & Borle, 2015).

Fear Appeal: A message that informs a person they must conduct or not conduct an act, and that there is a punishment for not complying (Rogers, 1975). In the context of this study, the fear appeal is the message received by the individual via SETA that explains that ISP is required and that there are potential sanctions for failing to comply with ISP.

Information system security: Protecting an organization's information through the use of technical systems, proper procedures, and behavior management (Dhillon & Torkzadeh, 2006).

Information security policy: A high-level document that identifies the organization's goals, priorities, and intentions for the management of information security, and the responsibilities, rights, and roles of individuals in pursuit of security goals (Stahl, Doherty, Shaw, & Janicke, 2014).

Intention: The motivation an individual has to perform a particular behavior (Ajzen, 1991). Typically, the stronger the intention a person has to execute a behavior, the more likely the individual will perform that behavior (Ajzen, 1991). Intention is the dependent variable in this study.

Protection motivation theory: Protection motivation theory indicates that the motivation to protect oneself is driven by the perceived severity of a threat, the likelihood that the event associated with the threat will occur, the perceived efficacy of the recommended solution, and the perceived efficacy of the individual to use the recommended solution (Rogers, 1975).

Security education, training, and awareness program (SETA): Programs that explain the appropriate procedures and potential sanctions for not complying for not following the appropriate procedures (Posey, Roberts, & Lowry, 2015)

Severity: The harshness of the punishment administered for violating a law or rule (Beccaria, 1963). Severity is an independent variable in this study.

Vulnerability: The likelihood that an individual will be caught when violating a law or rule (Beccaria, 1963). Vulnerability is an independent variable in this study.

Assumptions

This study included several theoretical, topical, and methodological assumptions. The primary theoretical assumption was that a behavioral theory such as protection motivation theory, explains the individual's reaction to ISP enforcement. The topical assumption was that participants understand what an ISP is and know if they are complying with it or not. Finally, it was logical to assume that an individual's *intention* to comply with ISP is unlikely to affect the policy-driven sanction variables *severity* and *vulnerability,* or an individual's *awareness* of how behavior affects others. Consequently, in this study, I assumed that the independent variables have a causal relationship with the dependent variable.

Methodological assumptions are that anonymous data gathering will encourage participants to answer survey questions honestly (Bélanger, Collignon, Enget, & Negangard, 2017) and mitigate the possibility of self-reporting bias. The last assumption was that the analysis conducted by the researchers that developed the instrument questions was conducted as stated and accurately represents a validation process that ensures that the instrument questions accurately measure the constructs defined in the study (Herath & Rao, 2009; Yazdanmehr & Wang, 2016).

Scope and Delimitations

This study addressed the factors that affect employees' decision to comply or not comply with ISP in higher education institutions. Participants were adults in the United States working in a higher education institution. The participants worked in an organization with ISP; they were aware of ISP, were competent to comply, and had behavioral control. Participants were not members of vulnerable populations.

Consequently, the results cannot be generalized to vulnerable populations or cultures or countries outside the United States.

I used GDT and NT in this study to investigate how a person responds to SETA messages containing a fear appeal about potential sanctions for non-compliance. Researchers have used other theories to investigate ISP compliance. The theory of organizational justice explains how individuals react to ISP based on fairness and equity (Li, Sarathy, Zhang, & Luo, 2014). Rational choice theory indicates that individuals are rational and will consider the benefits and costs of different options and choose based on economic gain (Kim et al., 2014). Researchers have used the Big Five personality traits to measure how individuals react to sanctions based on agreeableness, conscientiousness, and neuroticism, which are indications of stability, and openness and extroversion, which are indications of plasticity (Johnston, Warkentin, McBride, & Carter, 2016). Researchers have found protection motivation theory an excellent model for predicting how individuals will make decisions about complying with ISP (Crossler & Bélanger, 2014; Posey et al., 2015; Torten, Reaiche, & Boyle, 2018; Yang & Lee, 2016). I did not examine the theories just mentioned or other behavioral theories such as the theory of planned behavior, social bond theory, the technology acceptance model, or the theory of reasoned action in this study.

Limitations

The data were gathered using a self-reported survey and might be affected by common methods bias from self-reporting (Warkentin, Johnston, Shropshire, & Barnett, 2016). Common methods bias causes the participants to provide false answers to questions about compliance behavior (Lebek et al., 2014). Anonymous online surveys can decrease anxiety and increase the likelihood that participants will respond honestly (Fox et al., 2003).

Data were collected using a seven-point Likert scale, which may reduce the statistical power of the analysis because while these scales are numerical, the difference between 1-*Strongly Agree*, and 2-*Agree*, is not necessarily the same as the difference between 2-*Agree*, and 3-*Somewhat Agree.* Therefore these scales do not meet all of the requirements of interval data (Warner, 2013). Sufficient sample size was ensured so that the analysis was valid (Williams, Gómez Grajales, & Kurkiewicz, 2013). The data analysis could have revealed multicollinearity between variables (Warner, 2013), but this was not the case. I used SPSS 25 to measure the variance inflation factor. The value of less than 3.33 found is acceptable (Petter, Straub, & Rai, 2007).

While correlation does not necessarily imply a causal relationship, it is highly unlikely that the dependent variable *intention* is affecting the independent variables *severity* and *vulnerability* to sanctions, or *awareness.* One might make a counterargument that groups of people over time behaving in a non-compliant manner might cause an institution to change policy. However, this study examined the knowledge and *intention* of individuals at a specific point in time. In this study, I assumed that the relationship between the independent variables and the dependent variable is causal.

Significance of the Study

This study was significant because there is a lack of knowledge of the factors that influence people to follow ISP. Han et al. (2017) found that while there is abundant research on information security technology, research on employee behavior is scant. More research is needed to understand better why individuals do not comply with ISP (Siponen & Vance, 2014) because the current knowledge of the factors that influence information security behavior is incomplete (Chen, Wu, Chen, & Teng, 2018; D’Arcy et al., 2014).

Significance to Theory

There has been much research on information security technology, but little on employee behavior as it relates to ISP compliance (Han et al., 2017). There is a lack of agreement on the efficacy of sanctions in increasing ISP compliance (Goo et al., 2014). Researchers have found inconsistent results for the effect of sanctions on ISP compliance (Johnston et al., 2015) with Hedström et al. (2013) finding the severity of sanctions not strongly correlated with ISP compliance and D’Arcy et al. (2014) finding that sanctions are effective in preventing ISP violations. Research should be conducted to improve understanding of how the metaphor of the ledger neutralization technique is used to justify unsecure behavior (Cheng et al., 2014). This study on sanctions, awareness, and compliance made an original contribution to the gap in understanding behaviors associated with compliance with ISP because there have been no previous studies found where researchers measured the relationships between the independent variables *severity*, *vulnerability*, and *awareness*, and the dependent variable *intention*.

Significance to Practice

There is a lack of knowledge of the factors that influence people to follow or not follow ISP. GDT has been appropriated from criminology and applied to compliance (Cheng et al., 2014). The threat of formal sanctions has little effect on individuals who do not intend to comply with ISP (Johnston et al., 2015), nor does it have any effect on someone who believes they will not be caught (Chen, Ramamurthy, & Wen, 2012). Individuals tend to use neutralization techniques to justify non-compliance (Bauer et al., 2017), and the effects of neutralization are stronger than the effects of deterrence (Barlow et al., 2013). The metaphor of the ledger is a neutralization technique often used to justify non-compliance with ISP (Teh et al., 2015).

Recent work has indicated that SETA programs are too focused on the how of ISP, and not enough on the why (Arachchilage & Love, 2014). Awareness programs that focus on the damage caused by data breaches may offset the metaphor of the ledger technique such that individuals would more highly value the risk mitigation of compliance than the ability to complete work more quickly through non-compliance. Information security practitioners could use the results of this study to improve ISP and SETA programs. SETA programs that clearly define ISP may minimize the risk of data breaches and direct users in protecting an organization’s information assets (Ritzman & Kahle-Piasecki, 2016).

This study on sanction, awareness, and compliance may contribute significantly to information security theory and practices by providing more information about the reasons why employees in higher education institutions do not comply with ISP. The results of this study provided more information about the effects that sanctions and awareness of the consequences have on the intention to comply with ISP. More information about the reasons that employees in higher education choose to follow or not follow ISP and an understanding of the relative strengths of those reasons could aid information security practitioners in creating security compliance programs and training. Better training and compliance programs that explain the consequences of data breaches may encourage individuals to comply with ISP, which may reduce the frequency of data breaches.

Significance to Social Change

This study may cause positive social change by providing information that could enable information security practitioners to create programs that could increase compliance with ISP and reduce the number of data breaches. Improving SETA efforts may increase compliance with ISP and reduce the risk of data breaches (Ritzman & Kahle-Piasecki, 2016). Reducing the number of data breaches may contribute to positive social change by reducing the frequency of the negative impacts that data breaches have on individuals and organizations.

Data breaches lead to identity theft (Holtfreter & Harrington, 2015), and the exposure of sensitive information such as medical records (Kuo et al., 2014). Reducing the number of data breaches may reduce the negative impact that data breaches have on individuals and organizations. Individuals could benefit from a reduction in the frequency of identity theft and fraud. Having fewer data breaches could reduce the number of compromised electronic medical records systems, which can cause the publication of patients' medical records. Implementing programs that encourage practices that make data more secure could reduce instances of identity theft, compromised medical records, and small business bankruptcy.

Summary and Transition

In Chapter 1, I introduced the topic of the study and why it is important to individuals, organizations, and society. This chapter contained an explanation of the general problem of data breaches and the personal and financial damage they can cause, the specific problem of non-compliance with ISP, and the quantitative correlational nature of the study. Chapter 1 also included a statement of the research questions, hypotheses, and purpose of the study.

The chapter continued with behavioral theories examined in the study and identification of theories assumed to explain behaviors associated with the study. I have provided definitions of uncommon terms used in the proposal and explained the assumptions, limitations, and delimitations of the study. Chapter 1 concluded with the identification of the significance to the gap in the literature, and an explanation of the significance to the advancement of theory, significance to practitioners, and significance to positive social change. The next chapter contains the theoretical foundations and a detailed literature review that covers the studies conducted in the last few years that used similar variables, approaches, and topics.

Chapter 2: Literature Review

The general problem is the financial and personal damage caused by data breaches to organizations and individuals. The specific problem is the lack of understanding of the relationships between deterrence and compliance, and awareness and compliance, when employees in higher education decide not to comply with ISP. More knowledge of the factors that affect compliance with ISP is needed (Humaidi & Balakrishnan, 2015) to address the gap in the research (Siponen & Vance, 2010). The purpose of this study was to measure and rank the strength of the relationship between deterrence factors and compliance, and awareness and compliance.

Johnston et al. (2015) found that formal sanctions have no effect on the intention to comply with ISP, and noted that there are inconsistent findings on the effect of formal and informal sanctions on compliance with ISP. Hedström et al. (2013) noted that the severity of sanctions is not strongly correlated with ISP compliance. Conversely, D'Arcy et al. (2014) found that sanctions are effective in preventing cognitive rationalizations that lead to ISP violations.

Chapter 2 contains an overview of the theories and variables addressed in this study and a description of the process used in the literature search to ensure that all relevant articles have been discovered and incorporated. The chapter contains a discussion of the theories that support the hypotheses in the study, a review of how these theories have been used in similar studies in the past, and an explanation of how the theories support the variables used in the study. Finally, the chapter concludes with a justification for the research and the methods used to analyze the data.

Literature Search Strategy

I limited the literature search to peer-reviewed articles published within the last five years and used these search terms: information security, information security policy, compliance, awareness, general deterrence theory, intention to comply, deterrence theory, higher education, neutralization, and metaphor of the ledger. I conducted searches in the ABI/INFORM Complete, Business Source Complete, Emerald Management, ProQuest Computing, SAGE Premier, Science Direct, and Google Scholar databases. Automated searches for key terms created in Google Scholar Alerts, Mendeley / Elsevier, and Science Direct / Elsevier provided weekly suggestions. Citation chaining searches performed for the articles considered relevant to the study revealed applicable articles from the early part of this century that were not found in search engines.

I obtained seminal articles for behavioral theories by identifying references in recent articles and then buying copies of the articles and books from Amazon and other sources. The Klockars (1974) book *The Professional Fence* was only available as a used item. The Beccaria (1963) book *On Crimes and Punishment* was still available new. Other seminal works by Rogers (1975), Rogers (1983), Ajzen (1985), Fishbein (1975), and Sykes and Matza (1957) were found online after extensive internet searches.

Theoretical Foundation

GDT (Beccaria, 1963) and NT (Sykes & Matza, 1957) formed the theoretical foundation of the study. GDT explains how the organizational leaders enforce ISP, and NT explains how a person justifies non-compliance with ISP. A behavioral theory such as protection motivation theory (Rogers, 1975) or the theory of planned behavior (Ajzen, 1985) explains the cognitive process that a person conducts when forming an intention to comply or not comply with ISP after being threatened with GDT sanctions. A person that chooses not to comply with ISP may use a neutralization technique to mitigate the guild associated with non-compliance.

General Deterrence Theory

Information security policies are the first step an organization takes in developing procedures for protecting the organization's information (Ritzman & Kahle-Piasecki, 2016). While many chief information officers believe that employees present a higher risk to data than hackers (Barlow et al., 2013), getting employees to follow ISP is one of the most difficult tasks an information technology department faces (Hwang et al., 2017). The challenge of enforcing ISP has led many organizations to turn to GDT and use the threat of sanctions to encourage employees to adhere to ISP requirements (Barlow et al., 2013). GDT comes from the field of criminology and has been used in many studies on ISP compliance (Barlow et al., 2013; Chen et al., 2012; Cheng et al., 2013). The three elements of sanctions are severity, vulnerability, and celerity (Beccaria, 1963).

The concept of using the threat of punishment to deter crimes or violations of rules originated in work done by Cesar Beccaria and Jeremy Bentham in the late 1700s (Johnston et al., 2015). When an individual is threatened with punishment, the threat is evaluated based on the severity or harshness of the punishment that will be administered for committing the violation, the vulnerability or likelihood that a violation will be detected, and the celerity or length of time between committing the violation and the administration of the punishment (Cheng et al., 2014; Crossler et al., 2013; Johnston et al., 2015; Lowry et al., 2015). GDT indicates that a person will make a rational decision when considering violating a rule. If the individual perceives that the punishment is severe, the risk of being caught is high, and that punishment will be delivered quickly, the person may decide that the risks outweigh the benefits of violating the rule and will choose not to commit the violation (Barlow et al., 2013; Cheng et al., 2014; Johnston et al., 2016; Lowry et al., 2015). SETA and GDT are the organization's attempt to influence individuals to follow policy. Organizational leaders use SETA to create awareness of the requirements of ISP and the potential sanctions for non-compliance, and expect individuals to weigh the consequences of violating ISP and choose to follow ISP to avoid sanctions.

Clapper and Richmond (2016) conducted a study with small business owners in North Carolina based on GDT. The variables that represented sanction severity and sanction vulnerability were operationalized as threats to the business and not the individual (Clapper & Richmond, 2016). The researchers did not find any significant correlation between knowledge, communication, normative beliefs, perceived vulnerability, or perceived cost with the intention to comply with payment card industry policies (Clapper & Richmond, 2016).

Behavioral Theories that Connect Deterrence to Intention

In the previous section, I have explained how organizational leaders use SETA to create awareness and GDT to influence individuals to follow ISP. Several theories can explain how an individual may react to the introduction of ISP and form an intent. Protection motivation theory, the theory of planned behavior, and the technology acceptance model are the most frequently used theories in information security research (Lebek et al., 2014). Researchers have found protection motivation theory an excellent model for predicting how individuals will make decisions about their intention to comply with ISP (Crossler & Bélanger, 2014; Posey et al., 2015; Torten et al., 2018; Yang & Lee, 2016). Protection motivation theory indicates that an individual responds to a threat by appraising the severity and certainty of the threat, and by appraising the individual's capacity to cope with the threat (Rogers, 1975). The theory of planned behavior indicates that intention can be predicted based on attitude, social norms, and behavioral control (Ajzen, 1991; Boss et al., 2015; Safa et al., 2015; Warkentin et al., 2016). The technology acceptance model indicates that an individual's current usage and intention for future usage of a technology is influenced by perceived usefulness and ease of use (Davis, 1989).

An individual may form an intention to violate ISP that is not malicious. Barlow et al. (2013) noted that research had defined three types of ISP violations: passive, volitional, and malicious. Employees must be aware of ISP to make a volitional choice to violate it (Moquin & Wakefield, 2016). Violations of ISP that result from a lack of training, human error, or negligence of ISP are passive violations (Barlow et al., 2013). The conscious intention to violate ISP is a volitional choice (Johnston et al., 2016), but may not be malicious (Barlow et al., 2013; Johnston et al., 2016; Lowry et al., 2015). Malicious activities include fraud and theft of confidential data (Bauer et al., 2017). Non-malicious security violations are intentional, self-benefiting, and voluntary, but may still cause damage or increased security risk (Guo, Yuan, Archer, & Connelly, 2011). Non-malicious activities include sharing passwords, not logging out from a computer when leaving the work area (D’Arcy et al., 2014; Teh et al., 2015), copying sensitive data to a non-encrypted portable storage device, and sharing sensitive data with non-employees (Teh et al., 2015). Individuals may make a volitional but non-malicious choice to violate ISP because it makes task completion more convenient.

D’Arcy et al. (2014) conducted a study with a broad sample from diverse organizations and then repeated the study in 2018 with a more limited sample from a single organization. This confirmed that volitional, but not malicious, violations of ISP occur because of security-related stress. D’Arcy and Teh (2019) conducted a similar study utilizing coping theory and affective events theory, and found again that security-related stress caused employees to conclude that ISP would prevent them from completing tasks in a timely manner.

The process of considering threats and coping abilities may lead an individual with no intended malice to the conclusion that violating ISP is the best decision. While the individual may think the decision is the best course of action, they are often aware that the action is a violation and may feel the need to justify the action to mitigate guilt or fear of social rejection (Barlow et al., 2013; Bauer et al., 2017). NT explains the process of justifying violations of ISP (Barlow et al., 2013; Bauer et al., 2017; Kim et al., 2014; Sommestad et al., 2014), and is discussed in the next section.

Neutralization Theory

Sykes and Matza developed NT in 1957 as an alternative to other theories of the day that explained deviant behavior (Sykes & Matza, 1957). The prevailing idea was that juvenile delinquents committed crimes because they had a value system that was the opposite of the average middle-class, law-abiding citizen and because they had been raised in an environment where societal norms were detested (Sykes & Matza, 1957). Contrary to these conclusions, Sykes and Matza (1957) found that delinquents experienced shame and guilt, admired honest people, and were opposed to stealing from sacred institutions such as churches indicating that the delinquents had a moral code similar to other citizens and that they were not raised to detest social norms.

Sykes and Matza (1957) noted that societal rules have exceptions, such as the concept that killing is wrong unless during wartime. The idea that one could justify a societal wrong given the circumstances led the researchers to the development of NT. NT indicates that individuals can justify a deviant act in the same way that society justifies societal wrongs (Sykes & Matza, 1957). Neutralization can occur before or after a deviant act, and increases the chance that the individual will commit the act again (Minor, 1981).

Sykes and Matza (1957) defined five techniques for neutralization that a person will use to mitigate guilt and social rejection:

1. The denial of responsibility: The delinquent feels forced into committing the act because of external forces.
2. The denial of injury: Acts may be illegal but are not wrong if no one was hurt, such as acts of vandalism, borrowing without permission, or getting into a fight with a person who agrees to fight.
3. The denial of the victim: The delinquent condemns the victim as a wrongdoer who deserved to be punished, or as a member of a deviant subculture such as LGBTQ individuals.
4. The condemnation of the condemners: The delinquent claims that the people accusing him or her of a crime are hypocrites, criminals, or motivated by personal gain or spite.
5. The appeal to higher loyalties: The delinquent belongs to a subgroup such as a family, gang, or circle of friends who needed the delinquent to commit the crime against society to benefit the subgroup.

This study referenced the metaphor of the ledger, a technique where the individual maintains a mental ledger with good acts on one side and bad acts on the other (Klockars, 1974). The person justifies bad acts if they have done more good acts than bad acts (Klockars, 1974). Individuals who violate ISP may use the metaphor of the ledger to justify their actions by concluding that the good act of quickly completing job tasks outweighs the bad act of non-compliance (Bauer et al., 2017; Cheng et al., 2013; Hepler, 2015; Sommestad et al., 2014). Information security practitioners may be able to mitigate justification via the metaphor of the ledger by providing information to the individual that changes the values of the acts on the ledger.

Researchers have started to find support for the concept that individuals use neutralization techniques to justify non-compliance with ISP in recent studies. Silic, Barlow, and Back (2017) examined the use of shadow IT usage, which is the use of any hardware or software for business purposes that were not approved and prescribed by IT and formal policy. The results indicated found that employees used the systems because they made the accomplishment of work tasks easier (Silic et al., 2017). The researchers conducted a field survey with managers in an American insurance company, a French toll road management company, a Croatian Bank, and a European IT company. The results indicated that individuals used the defense of necessity neutralization technique and the denial of injury neutralization technique to mitigate the shame from informal sanctions and that the metaphor of the ledger technique was used to justify the intention to use shadow IT systems (Silic et al., 2017).

Literature Review

Researchers have used GDT in many information security research studies (Bauer & Bernroider, 2017; Chen et al., 2018; Dang-Pham & Pittayachawan, 2015; Han et al., 2017). Cheng et al. (2013) used GDT, the social control concept, and social bonding theory to create a research model that measured the relationship between IS security policy violation intention and several independent variables. The social control concept developed by Ross in 1896 supported formal social controls that include enforcement and laws, and informal social controls that include traditions, customs, morality, and norms (Cheng et al., 2013). The formal control elements of social control and the constructs of GDT supported the hypothesis that perceived vulnerability and perceived severity would be negatively correlated with intention to violate ISP (Cheng et al., 2013). The researchers used a scenario-based instrument to survey 185 Chinese employees, and the results supported vulnerability to sanctions, but not severity of sanctions (Cheng et al., 2013). The study revealed that informal sanctions are more effective than formal sanctions (Cheng et al., 2013), and this could be interpreted to mean that people would rather be punished than feel embarrassed or socially ostracized.

Foth (2016) used the theory of planned behavior and GDT in a theoretical model to evaluate compliance with ISP by gender with 349 female participants and 204 male participants in German hospitals. While Germany has strict laws governing the privacy of medical records, more accidental and intentional data breaches have occurred in German hospitals than similar institutions in other countries (Foth, 2016). Foth (2016) found no correlation between severity of sanctions and intention to comply with ISP for men or women, but found a correlation between vulnerability of detection and intention in both groups (Foth, 2016). Findings for the theory of planned behavior variables and intention to comply were different based on gender causing Foth (2016) to advocate tailoring SETA programs for the different genders.

Ifinedo (2016) used GDT, rational choice theory, and organizational climate perspective to create a research model that showed that top management support and beliefs, cost-benefit analysis, sanction severity, and detection probability would affect compliance with ISP. Hovav and D'Arcy (2012) provided support for GDT though Ifinedo (2016) pointed out that most research that applied GDT to ISP compliance was inconclusive. Ifinedo (2016) surveyed 176 Canadian non-IS managers that were members of the Canadian Association of Information Technology Professionals, and professionals connected to the researcher by LinkedIn. The results indicated that vulnerability was not correlated with compliance, top management support and beliefs were correlated at a low level; cost-benefit analysis was correlated at a medium level, and sanction severity was correlated at a strong level (Ifinedo, 2016). Ifinedo (2016) claimed to have measured compliance and not just the intention to comply, but conducted a survey and did not directly observe the participants. Social desirability bias would encourage participants to report socially desirable traits of compliance (Lebek et al., 2014).

Bulgurcu, Cavusoglu, and Benbasat (2010) found correlations between vulnerability of resources and beliefs about outcomes that included benefits, cost, sanction vulnerability, sanction severity, and work impediment. They found beliefs about outcomes correlated with beliefs about consequences in terms of the benefit of compliance with ISP, cost of compliance, and the cost of non-compliance. The researchers found beliefs about consequences correlated with attitude, normative beliefs, and self-efficacy, and found attitude, normative beliefs, and self-efficacy correlated positively with the intention to comply with ISP (Bulgurcu et al., 2010).

Kajzer, D'Arcy, Crowell, and Striegel (2014) examined the effect that deterrence language in information security messages had on individuals based on the Big Five personality traits in a study with 293 computer users using an online survey. The results indicated that message believability, persuasiveness, and the probability that a message could influence behavioral change toward information security differed depending on the type of message and the personality of the person receiving the message (Kajzer et al., 2014). Johnston et al. (2015) examined the effect that messages had on the intent to comply with ISP and determined that messages with informal threats of sanctions were correlated with the intention to comply with ISP, but messages with formal threats of sanctions were not. Many researchers have examined the relationship between extrinsic and intrinsic sanctions, and the intention to comply with ISP but have found mixed results.

Aurigemma and Mattson (2017) examined how the elements of GDT affected ISP compliance intent when moderated by an attitude developed from previous punitive experiences. The first part of the theoretical model measured the correlations between certainty and attitude, severity and attitude, and a combination of certainty and severity with attitude in groups that had previous experience with punishment, and a group that had no experience with punishment (Aurigemma & Mattson, 2017). The second part of the model depicted hypothesized correlations between subjective norms and intent, perceived behavioral control and intent, and attitude and intent (Aurigemma & Mattson, 2017). In the last part of the model, the researchers predicted a correlation between the independent variables subjective norms and perceived behavioral control and the dependent variable intent. The authors also tested an alternative model where attitude was treated as an independent variable instead of a moderating variable (Aurigemma & Mattson, 2017).

The researchers surveyed a sample of 239 Department of Defense employees governed by the same ISP. Covariance-based structural equation modeling provided results that supported the hypothesized relationships in the primary model between the elements of GDT and attitude, between attitude and intent, and between subjective norms and intent in both groups (Aurigemma & Mattson, 2017). Perceived behavioral control was correlated with intent in the group that had a previous punishment experience, but not in the group with no previous punishment experience.

Aurigemma and Mattson (2017) found significant relationships in the alternative model for both groups between the independent variables attitude, subjective norms, and perceived behavioral control and the dependent variable intention. The researchers found the combination of severity and certainty correlated with intent in the group with a previous punishment experience, but not with the group with no previous punishment experience (Aurigemma & Mattson, 2017). They found no significant correlations between the dependent variables severity and certainty and the dependent variable intention in either group.

Choi and Song (2018) used social bond theory and the more developed social control theory to create a research model where they hypothesized that three of the elements of social control theory, commitment, belief, and attachment, would be correlated with deterrence, and that deterrence would be correlated with compliance with ISP. They operationalized commitment as the ambition and aspiration an employee has for the organization, attachment as the affection and respect an employee has for other employees, and belief as the conclusion that a specific act is ethically correct (Choi & Song, 2018). The researchers did not include involvement, the fourth element of social control theory in the study. The researchers surveyed 199 officials in public institutions in Korea and used partial least squares to analyze the data (Choi & Song, 2018). The results indicated that commitment and belief were significantly correlated with deterrence, but attachment was not correlated with deterrence (Choi & Song, 2018). The researchers found a correlation between deterrence and compliance with ISP.

Merhi and Ahluwalia (2019) used a survey instrument to query 133 employees in the education, financial, information technology, and retail industries in the South-Western United States. The researchers measured the correlations between the independent variables punishment severity and certainty of detection, and the mediating variables descriptive norms and moral norms (Merhi & Ahluwalia, 2019). Descriptive norms are an individual's beliefs about the actions that most other people will take in a specific situation, and moral norms are the implicit group understanding of what is right and wrong (Merhi & Ahluwalia, 2019). The researchers measured the correlations between the mediating variables descriptive norms and moral norms, and the dependent variable resistance to information security systems (Merhi & Ahluwalia, 2019). The authors also measured correlations between the control variables industry, job type, size, age, gender, education and experience, and the dependent variable resistance to information security systems (Merhi & Ahluwalia, 2019).

Partial least squares analysis revealed significant correlations between certainty of detection and both mediating variables, a significant correlation between punishment severity and description norms, but no significant relationship between punishment severity and moral norms (Merhi & Ahluwalia, 2019). Merhi and Ahluwalia (2019) found the mediating variables correlated with resistance to information security systems, but none of the control variables correlated with resistance to information security systems (Merhi & Ahluwalia, 2019). The researchers found descriptive norms to have a moderating effect on the mediating effect that moral norms had on the relationship between certainty of detection and resistance to information security systems (Merhi & Ahluwalia, 2019).

GDT appears in studies even when it is not identified as the GDT. Klein and Luciano (2016) created a research model that appears to be based on protection motivation theory, GDT, and other undefined theories related to the effort an individual is willing to put into safe behaviors, and the satisfaction they experience in the workplace. Klein and Luciano predicted there was a correlation between these constructs and safe online behaviors. The researchers validated an instrument with a sample of 135 Brazilian IT users using an online and paper-based questionnaire and conducted a final survey with 112 users. They found threat susceptibility and satisfaction correlated with safe behaviors at $p < .001$; threat severity correlated with safe behaviors at $p < .01$, and certainty of detection correlated with safe behaviors at $p < .05$ (Klein & Luciano, 2016). The hypothesis that severity of punishment would be correlated with safe behaviors was not supported (Klein & Luciano, 2016). The article described the basics of protection motivation theory and GDT and explained how the constructs of these theories had been used in other information security research but never referenced the theories by name. The word theory did not even appear in the article. The researchers measured safe online behaviors construct by asking the participants how they used email (Klein & Luciano, 2016). The results supported the hypothesized correlations between the constructs and safe behavior except severity of punishment.

Chen et al. (2018) investigated how elements of protection motivation theory and moral belief theory moderate the effect of sanctions on intention. The authors began by stating that the results from ISP studies with GDT have been inconsistent and that this may be caused by missing moderator values (Chen et al., 2018). The point of the study was to gain a better understanding of how moderating variables affect the relationship between severity and intention. The authors used two variables from protection motivation theory, response cost and self-efficacy, one variable from GDT, severity, and one variable from Moral Beliefs theory, descriptive norm, and theorized they would affect intention

The researchers hypothesized that severity would influence all other variables, and was would intention directly. Chen et al. (2018) also hypothesized that self-efficacy would influence the relationship between severity and intention and directly influence intention, that descriptive norms would influence the relationship between severity and intention and directly influence intention, and that response cost would influence the relationship between severity and intention, and directly influence intention. The authors used published survey instruments to create an online survey distributed by the Qualtrics survey company.

A sample of 406 employees in a mid-sized university in the northwest United States attempted the survey resulting in 231 usable responses. The analysis utilized SmartPLS 3.0 to measure Cronbach's alpha, confirmatory factor analysis, and discriminant validity, which all had acceptable values. None of the protection motivation theory variables moderated the relationship between sanctions and intention, and sanctions did not affect response cost. The findings supported all other hypothesized relationships. The authors listed inconsistent results in previous ISP studies with GDT as one of the justifications for conducting the study. The following section addresses the varying outcomes of previous studies about how GDT affects compliance with ISP.

Mixed Results in ISP Studies with General Deterrence Theory

The results from studies that measured the effect that deterrence has on compliance with ISP are mixed (Chen et al., 2018; Cheng et al., 2013; Han et al., 2017; Ifinedo, 2016). Barlow et al. (2013) found that neutralization techniques were stronger than the threat of sanctions in an online study about how messages influence intent with 90 full-time employees in the United States. In contrast, Moody and Siponen (2013) found that formal sanctions had a modest effect on the intention to violate internet usage policies in a study with 238 employees in Finnish service companies. Chen et al. (2012) used the vulnerability of threat as a moderating variable on the relationship between sanctions and intention, and rewards and intention in an internet-based field experiment with 50 employees from companies in the Midwest United States. The results indicated that the correlations were stronger when vulnerability was high (Chen et al., 2012).

Hovav and D'Arcy (2012) combined sanction severity and vulnerability into one construct and found a negative correlation with intention to misuse technology, such as not following ISP in a study with 228 employees from diverse environments and 183 employees that were also MBA students. However, in work done two years later with 539 computer-using professionals in the mid-Atlantic region of the United States, D'Arcy et al. (2014) found no direct connection between sanctions and the intention to violate ISP and noted that this finding was contrary to work done previously. Ifinedo (2014) used sanction vulnerability and severity as control variables in a study with 124 managers in the United States and found no correlation between the GDT variables and intention in the full model, but did find a small correlation between the GDT variables and intention when removing other variables from the theory of planned behavior that had a stronger correlation with intention.

Rajab and Eydgahi (2019) measured the constructs of GDT, protection motivation theory, the theory of planned behavior, and organizational theory to see if they were correlated with the intention to comply with ISP. The sample consisted of 206 employees at a university in the Midwest United States (Rajab & Eydgahi, 2019). The results indicated no significant correlations between the GDT constructs and intention to comply, nor any of the constructs from the theory of planned behavior or organizational theory and intention to comply (Rajab & Eydgahi, 2019). The authors concluded that the protection motivation theory is the best theory for explaining the behavioral mechanisms associated with the intention to comply with ISP (Rajab & Eydgahi, 2019).

While there is a history of contradictory findings for the effects that sanctions have on the intention to comply with ISP, the differences in findings for the individual constructs of GDT reveal a more detailed picture of how individuals respond to the threat of sanctions. In the next section, I discuss the findings of studies that measured the correlation between severity and vulnerability, and intention.

Sanction Severity Versus Sanction Vulnerability

An examination of the ISP studies conducted in the previous seven years revealed that researchers measured the correlations between sanction vulnerability and intent to comply or similar variables, and sanction severity and intent to comply or similar variables separately. Of the studies examined in this literature review, researchers in seven studies found differences in the correlations between the independent variables sanction severity and sanction vulnerability, and the dependent variable the intention to comply with ISP. In three of the studies, researchers found correlations between sanction vulnerability and intent but found no correlation between sanction severity and the intention to comply with ISP. The results in three of the studies indicated correlations between sanction severity and intent or a similar variable, but no correlation between and sanction vulnerability and intent. One researcher found different results for samples in two countries.

Cheng et al. (2014) found a correlation between vulnerability, sanctions, and the intention to comply with ISP, but no correlation between severity of sanctions and the intention to comply with ISP in a study with Chinese employees in telecom and financial organizations. In contrast, Cheng et al. (2013) found a correlation between sanction severity and the intention to comply with ISP but found no correlation between sanction vulnerability and the intention to comply with ISP. Foth (2016) found a correlation between sanction vulnerability and the intention to comply but no correlation between sanction severity and the intention to comply among German nurses and doctors. In contrast, Ifinedo (2016) found a correlation between sanction severity and intention to comply, but no support for the correlation between sanction vulnerability and intention to comply. Li et al. (2014) found support for a correlation between vulnerability and the intention to comply, but no correlation between sanction severity and the intention to comply with ISP. Contrary to these findings, Yang and Lee (2016) conducted a study with hospital employees in Korea and found a correlation between sanction severity and the intention to protect healthcare information, but did not find a correlation between sanction vulnerability and the intention to protect healthcare information.

An additional set of contrary findings in the results of these studies becomes evident when examining the results of work done by Hovav and D’Arcy in 2012. In a study that used samples from the United States and Korea, Hovav and D’Arcy (2012) found a negative correlation between sanction vulnerability and the intent to misuse technology in Korea, but not in the United States. They found sanction severity negatively correlated with the intention to misuse technology in the United States, but not Korea (Hovav & D’Arcy, 2012). One might assume that these results indicate some connection between the type of society and the response to sanction severity versus sanction vulnerability. The correlation between vulnerability and the intention to comply with ISP appeared to be more common in collectivist societies such as Korea or China as is seen in the studies done by Cheng et al. (2013), and Yang and Lee (2016). The correlation between severity and the intention to comply appeared to be more common in individualist societies such as the United States or Germany, as is seen in studies done by Foth (2016), and Li et al. (2014). The data in Table 1 shows that there is no pattern to the results. Ifinedo (2016) conducted a study in Canada and found a correlation between sanction severity and the intention to comply, but no correlation between sanction vulnerability and the intention to comply. Cheng et al. (2014) found correlations in the opposite direction with a sample from China.

Table 1

Differing Results for Studies with Intention, and Vulnerability and Severity

Vulnerability but not severity	Severity but not vulnerability
China - (Cheng et al., 2014)	China - (Cheng et al., 2013)
Korea - (Hovav & D'Arcy, 2012)	U.S. - (Hovav & D'Arcy, 2012)
Germany - (Foth, 2016)	Canada - (Ifinedo, 2016)
U.S. - (Li et al., 2014)	Korea - (Yang & Lee, 2016)

As has been discussed, researchers have found mixed results when comparing sanctions to the intention to comply. While most of these studies have operationalized sanctions by using sanction vulnerability and sanction severity, the concept of sanctions includes the aspect of celerity (Barlow et al., 2013), which is not often seen in studies (Lowry et al., 2015). I discuss the aspects of deterrence celerity in the next section.

Deterrence Celerity in General Deterrence Theory Studies

The celerity component of GDT represents the speed with which sanctions are administered after a violation of a law (Beccaria, 1963), or in the case of ISP studies, the violation of ISP (Cheng et al., 2014; D'Arcy & Herath, 2011; Johnston et al., 2015). Classic GDT states that all three elements, severity, vulnerability, and celerity, are required to maximize the effect of deterrence (Bulgurcu et al., 2010). Given that individuals tend to value short-term gains and costs over long-term gains and costs, researchers have suggested that ISP violation sanctions be administered immediately following a violation to increase the effectiveness of the sanctions (Tsohou, Karyda, Kokolakis, & Kiountouzis, 2015). Celerity is rarely included in ISP studies (D'Arcy & Herath, 2011; Johnston et al., 2015; Lowry et al., 2015). Celerity may be left out of studies because of work done by researchers in the field of criminology who questioned the efficacy of celerity in enforcing behavior and suggested that it is more suited to animal behavior than it is to human behavior (Johnston et al., 2015).

Several studies have measured celerity with no significant results. D'Arcy and Herath (2011) stated they could find no ISP studies that included celerity, and Johnston et al. (2015) noted that while there had been a few ISP studies that included celerity, the studies had found no significant relationship between celerity and compliance. Johnston et al. used celerity as a component of messages that warned users about the sanctions associated with violations of ISP but found no correlation between the celerity component and intention to comply. Lowry et al. (2015) measured the effect that celerity had on the reactive computer abuse, but found no significant correlation. D'Arcy et al. (2014) used celerity as a control variable in a study that examined the effects that security-related stress had on the intention to violate ISP, but found no correlation for celerity.

Alshare, Lane, and Lane (2018) conducted a study with 195 employees at a Midwestern university in the United States and measured deterrence celerity and severity along with organization security culture, privacy, responsibility and the three elements of organizational justice, to determine if these factors were correlated with violation of ISP. Multiple regression analysis revealed statistically significant correlations between the dependent variable and celerity and severity (Alshare et al., 2018). They found all of the other independent variables correlated with violations of ISP except for interactional justice (Alshare et al., 2018).

Cheng et al. (2014) measured the effects of sanction severity and vulnerability but did not include celerity. Bulgurcu et al. (2010) suggested that studies that examine how users perceive the cost of non-compliance should measure celerity. While the lack of significant results has led ISP researchers to suggest that more studies should include celerity as an independent variable, I did not include celerity in this study due to the lack of support for the construct in studies that use GDT, and the inability to map GDT celerity to the threat appraisal in protection motivation theory.

The Questionable Use of Sanctions in ISP Enforcement

GDT from criminology explains the processes that organizational leaders assume will occur when using sanctions to enforce ISP. Security leaders in organizations have reacted to the possible violation of ISP by stating that sanctions will be administered to violators (Barlow et al., 2013; Cheng et al., 2014; Johnston et al., 2016, 2015), including the threat of termination (Cheng et al., 2014). Research shows that an authoritarian approach does not always provide the desired results (Barlow et al., 2013; Cheng et al., 2013; D’Arcy et al., 2014; Posey, Roberts, Benjamin, & Hightower, 2014). The threat of sanctions has no effect on an individual who believes they will not be caught (Chen et al., 2012), and formal sanctions have little effect on individuals who have no intention to comply with ISP (Johnston et al., 2015), or employees with no intention to commit acts that deviate from policies (Li et al., 2014). Strong formal sanctions may cause an individual to react negatively to the threat of sanctions and adopt behaviors that increase risk (Posey et al., 2014). Users may justify non-compliance by rationalizing that the threat is low (Goo et al., 2014), using moral reasoning (Barlow et al., 2013), or using mechanisms such as neutralization techniques to justify non-compliance (Goo et al., 2014; Kim et al., 2014).

This study addressed a gap in the literature on the effectiveness of using deterrence to enforce ISP policies (Crossler, Long, Loraas, & Trinkle, 2014; Goo et al., 2014; Ifinedo, 2016; Siponen & Vance, 2014). The GDT supports the first two independent variables in the conceptual model shown in Figure 1. I hypothesized that the independent variables s*everity, vulnerability,* and *awareness* would influence the dependent variable *intention* and that taken collectively, the three independent variables would have different levels of influence on the dependent variable.

When a person violates a norm, they will experience some form of guilt and will be motivated to mitigate the guilt (Sykes & Matza, 1957). Prior to work done by Sykes and Matza (1957), the prevailing theory was that delinquents who violated social norms or committed crimes had an inverted moral code that was the opposite of the prevailing society (Sykes & Matza, 1957). Sykes and Matza found that delinquents had the same moral code as others, but were able to justify delinquent acts using various techniques. An individual might justify stealing from a store if they perceived the store owner to be dishonest, but the same individual would never steal from a church (Sykes & Matza, 1957). In the first case, the individual can justify the act, but in the second case, they cannot. Sykes and Matza pointed out that being unable to justify stealing from a respected institution such as a church indicated that the person had a similar moral code to others and that being able to justify stealing from the store did not indicate that the person had an inverted moral code, but instead was able to justify the act. NT can explain the cognitive processes that occur when an individual decides to violate ISP. (Barlow et al., 2013; Bauer & Bernroider, 2017; D'Arcy & Teh, 2019; Teh et al., 2015). I 7explain how NT relates to ISP compliance in the following section.

Neutralization Theory

Piquero, Tibbetts, and Blankenship (2005) examined NT as a theory that could explain unethical decisions in pharmaceutical marketing (Siponen & Vance, 2010). The results indicated that participants used the belief that the government overstated the dangers of a drug to neutralize the guilt associated with continuing to market the drug even though it was about to be recalled by the Food and Drug Administration (Piquero, Tibbetts, & Blankenship, 2005). Siponen and Vance referenced the work done by Piquero et al. in a 2010 study that was the first use of neutralization in a study involving ISP (Lebek et al., 2014). Siponen and Vance (2010) found that individuals used neutralization techniques to reduce the perception of harm when choosing to violate ISP. Barlow et al. (2013), Cheng et al. (2013), Cheng et al. (2014), Goo et al. (2014), Kim et al. (2014), Teh et al. (2015), Bauer and Bernroider (2017), Barlow et al. (2018), and D'Arcy and Teh (2019) found that individuals use neutralization techniques to justify non-compliance with ISP. D’Arcy and Teh posited that neutralization had been adapted to ISP studies because it explains how a person uses psychological control to alleviate the stress caused by ISP by having an emotionally based coping response.

Extending Neutralization Theory with the Metaphor of the Ledger

Other researchers have developed additional neutralization techniques since Sykes and Matza published the original five techniques in 1957. Coleman added the defense of ubiquity neutralization technique to NT in 1987. Individuals who claim that everyone is committing the deviant behavior; therefore, the act is acceptable are using the defense of ubiquity technique. Minor added the defense of necessity neutralization technique to NT in 1981, which is used to justify deviant behavior by claiming that one must commit the behavior to survive in competitive situations. The metaphor of the ledger neutralization technique developed by Klockars in 1974 is specifically relevant to the topic of ISP compliance.

The metaphor of the ledger is a neutralization technique that is used by individuals to justify non-compliance with ISP (Bauer et al., 2017; Cheng et al., 2013; Hepler, 2015; Sommestad et al., 2014). Klockars introduced the concept of the metaphor of the ledger in 1974 in the book *The Professional Fence*. Klockars was able to get a fence, which is a criminal that traffics in stolen goods, to allow Klockars to observe and interview him for over a year. At one point, the fence explained to Klockars that even though he had committed many crimes, he had also done many good deeds and that a tally of the good and bad deeds showed that the fence had committed more good than bad and was therefore morally justified (Klockars, 1974).

In the case of non-compliance with ISP, individuals may use the metaphor of the ledger to justify non-compliance by concluding that the positive aspect of completing job tasks efficiently outweighs the negative aspect of non-compliance with ISP (Bauer et al., 2017; Cheng et al., 2013; Hepler, 2015; Sommestad et al., 2014). Barlow et al. (2013) found that when individuals made deliberate decisions about ethical situations, they often made unethical decisions based on the reasoning that it was a reasonable action to violate ISP when it improved work performance. Violating ISP included writing down passwords or using unencrypted data storage. Goo et al. (2014) found that employees intentionally ignore ISP and ignore deterrence efforts by the organization because they are prioritizing work over security and find ISP requirements a hindrance to work accomplishment.

Tarafdar, D'Arcy, Turel, and Gupta (2015) noted that medical doctors often find IT security tasks to be impossible and that the stress caused by security tasks leads medical personnel to conclude that they should violate ISP to be more productive. Employees and other company insiders are the greatest threat to data, yet they create threats to data in an attempt to increase productivity (Tarafdar et al., 2015). Teh et al. (2015) argued that employees used the metaphor of the ledger by putting work accomplishment on the good side of the ledger and non-compliance on the bad side of the ledger and that the good deed of accomplishing work outweighed the bad deed of non-compliance with ISP.

As has been discussed, several researchers have argued that individuals use the metaphor of the ledger neutralization technique to justify non-compliance with ISP. Barlow et al. (2013) tested various forms of neutralization, and while the results indicated that several neutralization techniques were correlated with the intention not to comply with ISP, the correlation between the use of the metaphor of the ledger technique and non-compliance was not significant. In contrast, Kim et al. (2014) found a correlation between non-compliance and seven of the eight neutralization techniques, including the metaphor of the ledger.

Criticism of Neutralization

While there has been support for the use of neutralization in criminal and ISP studies, Minor (1981) stated that there are flaws in the way neutralization techniques have been applied to delinquent behavior and the way neutralization techniques have been measured. Minor suggested that Cohen (1955) overstated the difference in moral codes held by delinquents and non-delinquents and that Sykes and Matza's (1957) overstated the similarities in moral codes held by delinquents and non-delinquents. He found that there was a correlation between accepting excuses for deviant behavior and subsequent deviant acts implying that neutralization was an antecedent of deviant acts as opposed to deviant acts being an antecedent of neutralization in a study with 478 college students at the University of Maryland. Minor found denial of responsibility, denial of the victim, appeal to higher loyalties, and defense of necessity positively correlated with the intention to commit deviant acts (Minor, 1981).

Minor (1981) also commented that the definition of the denial of the victim neutralization technique was flawed because the technique could mean that the victim deserved any injury caused by the crime, or it could mean that the victim was unknown to the criminal. These two forms of victim denial are entirely different, and the difference in the meanings has led some ISP researchers such as Siponen and Vance (2010) and Teh et al. (2015) to drop the denial of the victim technique from ISP compliance research that included NT. Minor also criticized the Neutralization Index developed by Ball in 1973 for being unable to distinguish between an individual that is using neutralization to justify the breaking of a social norm versus an individual that has unconditional approval for an action that breaks a social norm.

ISP Studies with Neutralization

Kim et al. (2014) utilized planned action theory, rational choice theory, protection motivation theory, and NT in a study with 194 information technology employees in 32 companies across 10 industries. Kim et al. used a modern version of NT that included the metaphor of the ledger and defense of ubiquity, two techniques added to Sykes and Matza’s NT by other researchers. Analysis of the survey data found a negative correlation between seven neutralization techniques and intention to comply, and found a correlation between response-efficacy and intention, but not between self-efficacy and intention (Kim et al., 2014).

Cheng et al. (2014) addressed NT and GDT in a study with 112 employees in telecommunication and financial organizations in China that had internet policies that forbid personal use of the internet while working. The results of the study indicated that there was a positive correlation between seven specific neutralization techniques and the intention to use the internet for personal reasons (Cheng et al., 2014). The results also indicated there was a negative correlation between the knowledge that behavior would be detected and the intention to use the internet for personal reasons at work, and that the perception of benefits was positively correlated with the intention to use the internet for personal purposes at work (Cheng et al., 2014). The researchers did not find a negative correlation between sanctions and the intention to use the internet for personal reasons at work as hypothesized (Cheng et al., 2014). The study provided more evidence that sanctions and rewards are not effective means of enforcing IS policies, and the lack of support for sanctions is consistent with many, but not all, other studies that found that sanctions are not an effective means of enforcing behavior. Even though Cheng et al. found a negative correlation between detection certainty and personal use of the internet, they noted that the effect was much less than the relationships in the other hypotheses.

Barlow et al. (2013) used NT, GDT, and framing theory to investigate IT security communications to see if they could be framed in a way that discouraged non-compliance with ISP. The study utilized a scenario-based survey with 90 participants to assess the effectiveness of different types of communications in discouraging the use of neutralization techniques for excusing non-compliance with ISP (Barlow et al., 2013).

The results indicated that the defense of necessity neutralization technique was positively correlated with intention to violate ISP early, but that the denial of injury and metaphor of the ledger neutralization techniques were not (Barlow et al., 2013). The results also indicated that communication messages about sanctions and not using neutralization were equally effective in influencing users not to violate ISP (Barlow et al., 2013). The analysis indicated that the effects of NT overcome the impact of sanctions when individuals are considering volitional, but not malicious acts because the individual thinks they are doing the right thing after neutralizing the norm of complying with policies (Barlow et al., 2013).

Al-Mukahal and Alshare (2015) examined the factors that influenced ISP violations in organizations in Qatari. The authors hypothesized that awareness of ISP, clarity of ISP, and the positive impact of ISP would be negatively correlated with the number of policy violations, and that trust in employees would be positively correlated with the number of policy violations (Al-Mukahal & Alshare, 2015). They also hypothesized that high uncertainty avoidance would moderate the relationships hypothesized for awareness and clarity and that high collectivism would moderate the relationships for trust in employees and the positive impact of ISP (Al-Mukahal & Alshare, 2015).

Al-Mukahal and Alshare (2015) proposed that GDT and NT apply to ISP compliance research and referenced the metaphor of the ledger. The idea that individuals used neutralization techniques to justify non-compliance, and that awareness, clarity, and positive impact of ISP would reduce neutralization provided the basis for the hypotheses. Al-Mukahal and Alshare noted that work done by Siponen and Vance in 2010 had found that formal sanctions are ineffective in the enforcement of ISP and that neutralization was the strongest influence on the intention to violate ISP. The researchers used multiple regression to analyze data from an online survey conducted with 234 Qatari professionals who worked in organizations with an ISP. The results supported the hypothesized relationships except for the ones between awareness and the number of ISP violations, and the moderating effect that high uncertainty avoidance would have on the relationship between awareness and the number of ISP violations (Al-Mukahal & Alshare, 2015).

Teh et al. (2015) conducted a study based on NT and social exchange theory and tested the relationship between neutralization techniques and the volitional but not malicious decision to violate ISP with 228 randomly chosen employees in the Malaysian banking industry. The results supported the hypothesis that neutralization techniques would be positively correlated with the intention to violate ISP and that organizational commitment would be negatively correlated with the use of neutralization (Teh et al., 2015). The authors noted that the use of neutralization is more prevalent in employees with low organizational commitment and that the metaphor of the ledger technique was used to justify non-compliance because employees concluded that occasional non-compliance on the bad deed side of the ledger was by frequent ISP compliance on the good deed side of the ledger (Teh et al., 2015).

Bauer et al. (2017) conducted a qualitative study with three full-service banks in Central Eastern Europe and found that employees used the defense of necessity and appeal to higher loyalties neutralization techniques to justify violations of ISP that occurred while providing service to customers. Bauer et al. noted that employees found ISP an obstacle to achieving the organization's mission. The results of the study suggested improving SETA programs using Deming's plan, do, check, act model.

Bauer and Bernroider (2017) conducted a second study in a banking organization in Europe and used a qualitative case study approach to establish hypotheses relating to the theory of reasoned action, neutralization, and the intention to comply with ISP. The results of the study indicated that internal and external information influences information security awareness that in turn influences attitudes, social norms, and the use of neutralization techniques, which all affect the intention to comply with ISP. Bauer and Bernroider found that the neutralization techniques denial of responsibility, defense of necessity, denial of injury, and condemn the condemners were all being used by employees.

In a more recent study with 200 individuals in the United States who worked in an environment with computers and ISP, Barlow et al. (2018) found correlations between non-compliance with ISP and the use of neutralization techniques. The researchers employed an online factorial survey with scenarios and found connections between informational communication and compliance with ISP, and between anti-neutralization communication and compliance with ISP. They did not find support for a correlation between normative communication and ISP compliance (Barlow et al., 2018).

Willison, Warkentin, and Johnston (2018) used a scenario-based factorial survey with 968 full time working professionals in the United States from a wide variety of industries who used a computer and who were eligible for raises. The authors stated that they used the factorial survey to decrease issues of social desirability bias and to provide more information about the individual's decision making structure (Willison et al., 2018). The researchers used two concepts from organizational justice and hypothesized that an individual's perceptions of distributive injustice and procedural injustice would have a positive correlation with the intention to commit employee computer abuse (Willison et al., 2018). Distributive justice is the fairness of outcomes, while procedural justice is the fairness of processes (Willison et al., 2018). The researchers also hypothesized that three neutralization techniques, denial of injury, denial of the victim, and the metaphor of the ledger would moderate the relationship between perceptions of injustice and intention (Willison et al., 2018). The results did not support a connection between distributive injustice and intention but did support the correlation between procedural injustice and intention. The results also supported the hypotheses that the denial of the victim neutralization technique and the metaphor of the ledger technique would moderate the relationship between procedural injustice and the intention to commit computer abuse.

D'Arcy and Teh (2019) conducted a study using coping theory and affective event theory to measure hypothesized correlations between security-related stress and emotional reactions that could vary with time, emotional reactions and neutralization techniques, and neutralization techniques and compliance ISP compliance. The study was novel in the way the researchers used experience sampling methodology, an expensive research technique where participants completed surveys on Mondays, Wednesdays, and Fridays for three weeks (D’Arcy & Teh, 2019). Affective events theory indicates that workplace events and the emotional reactions that employees have to the events explain variation in attitudes and behaviors over time (D’Arcy & Teh, 2019). A recruiting firm solicited participants and received 305 responses, of which 201 were selected to be in the study with an outcome of 138 participants providing a total of 1058 usable surveys (D’Arcy & Teh, 2019).

The authors used hierarchical linear modeling to assess the relationships between the variables at multiple levels due to the nature of the non-independent data (D’Arcy & Teh, 2019). The results indicated significant positive relationships between security-related stress and the two emotional reactions frustration and fatigue, significant positive relationships between the emotional reactions and neutralization techniques, and a significant negative relationship between neutralization techniques and ISP compliance as hypothesized by the researchers (D’Arcy & Teh, 2019). A separate analysis was performed on groups with high frustration, low frustration, high fatigue, and low fatigue (D’Arcy & Teh, 2019). The researchers did not find a significant negative correlation between neutralization and ISP compliance in the low frustration group but found significant negative correlations between neutralization and ISP compliance for the other three groups.

I focus on acts where the individual has determined that security requirements are preventing them from accomplishing work tasks and have used a neutralization technique such as the metaphor of the ledger to justify non-compliance with ISP in this study. These individuals think they are acting in the best interest of the organization and have concluded that non-compliance is a normal act that is similar to acts by other individuals in the organization (Barlow et al., 2013). In recent work, researchers have found that the use of neutralization techniques is correlated with noncompliance (Barlow et al., 2018; Bauer et al., 2017) and that it tends to overcome the significance of sanctions (Barlow et al., 2013).

Given the inconsistent findings on the effectiveness of deterrence (Chen et al., 2018; Cheng et al., 2014; D'Arcy et al., 2014), a different technique is needed to offset the effects of neutralization techniques such as the metaphor of the ledger and lead the individual to the conclusion that non-compliance with ISP has a larger negative value on the ledger than the positive value of accomplishing work tasks. Yazdanmehr and Wang (2016) found that awareness of the damage caused to an organization by data breaches was an effective means for mitigating the effect that neutralization had on non-compliance with ISP. I discuss awareness of the consequences in the next section.

Awareness of the Consequences

There are multiple definitions for awareness in the context of information security, and researchers have operationalized the concept of awareness in various ways in information security studies. Many studies examined in this proposal define awareness as knowledge of information security practices. As such, researchers have defined information security awareness as the effort to bring attention to the importance of information security and encourage secure behavior (Tsohou, Karyda, Kokolakis et al., 2015), or as the knowledge of ISP and procedures (Safa et al., 2015, 2016), or the understanding of safe information security behaviors and the commitment to use best practices in information security (Parsons et al., 2017). Dang-Pham and Pittayachawan (2015) defined awareness as the knowledge of the severity and vulnerability of threats to organizational assets.

Awareness in any form is an essential aspect of information security. An employee must be aware of a requirement before they can comply with it (Moquin & Wakefield, 2016) and employees that are not aware of ISP may violate ISP (Siponen & Vance, 2014). Chen et al. (2018) found that employees must be educated to be aware of ISP and procedures, or they will refuse to change behaviors. Employees who are aware of ISP are less likely to violate ISP (Chu & Chau, 2014).

The cognitive process of responding to ISP cannot occur without awareness. The theoretical construct used in this proposal indicates that an individual becomes aware of ISP and potential sanctions via SETA and then reacts based on a behavioral theory such as protection motivation theory. The protection motivation theory process cannot occur without a fear appeal that makes the individual aware of the nature of the threat, the threat severity and certainty, and the recommended response (Rogers, 1975). There are more aspects of information security of which an individual can and should be aware.

Awareness should include knowledge of ISP practices, but should also include knowledge of the damage done by non-compliance with ISP. Al-Mukahal and Alshare (2015) noted that employees would not conform with ISP if they do not understand information security risks. Dang-Pham and Pittayachawan (2015) found that practitioners should put more emphasis on the severity of threats instead of the certainty of threats, and Han et al. (2017) argued that employees would have more intention to comply with ISP if they understand the benefits. Ma, Kuo, and Alexander (2016) and Sher, Talley, Yang, and Kuo (2017) both suggested that medical personnel would be more likely to comply with electronic medical records privacy policies if they were more aware of how policy violations caused damage to patients.

Arachchilage and Love (2014) made an assertion from their findings that sums up the previous suggestions; organizational leaders should focus more on the why of ISP compliance, and less on the how of ISP compliance. Users would be more likely to comply with ISP if the users of information systems were more aware of the consequences of data breaches to others. Researchers have called this type of awareness ISP-related awareness of the consequences (Yazdanmehr & Wang, 2016) and awareness of the consequences of security threats (Yang & Lee, 2016).

Yazdanmehr and Wang (2016) noted that employees must be aware of how security behavior affects the welfare of others and the overall organization and called this type of knowledge awareness of the consequences. This construct does not define awareness of the sanctions that could be applied for non-compliance, nor is it an awareness of ISP policies or procedures (Yazdanmehr & Wang, 2016). Yazdanmehr and Wang argued that the contemplation of ISP compliance is a cognitively elaborate process that considers personal norms and that an awareness of the consequences for non-compliance with ISP is required to enforce a moral obligation. An employee that does not understand how non-compliance with ISP can harm others may not realize that the decision has a moral element (Yazdanmehr & Wang, 2016). Similarly, Yang and Lee (2016) noted that the exposure of medical records can cause psychological damage to patients and that employees in health care organizations would be more likely to be attentive to ISP if they understood the damage that could be caused to patients if ISP is violated. In this study, I operationalized and measured the construct *awareness* based on the work done by Yazdanmehr and Wang.

Studies Utilizing Awareness of the Consequences

Yang and Lee (2016) used GDT and protection motivation theory to support the hypothesis that awareness, which was defined as being aware of the consequences of a security breach in terms of damage to the information systems and awareness of policy, would be positively correlated with threat severity, threat vulnerability, response-efficacy, and self-efficacy in a study with 222 Korean hospital employees. Yang and Lee also hypothesized that satisfaction with the security system would be positively correlated with response-efficacy and self-efficacy, and that self-efficacy, response-efficacy, threat vulnerability, and threat severity would influence induction control intention and self-defense intention, which are the two constructs in the intention to protect healthcare information. They hypothesized threat severity would be positively correlated with threat vulnerability, and self-efficacy would be positively correlated with response-efficacy. The results supported the hypotheses except for the correlations between awareness and vulnerability, vulnerability and induction control intention, and response-efficacy and induction control intention.

Researchers have conducted qualitative studies that support the importance of awareness of the consequences of a data breach (Connolly, Lang, Gathegi, & Tygar, 2017). Connolly et al. (2017) conducted nine interviews in the United States and 10 interviews in Ireland with individuals who worked in various industries. The results indicated that SETA increases security awareness and that awareness leads to compliant behavior. Connolly et al. concluded that information security programs should include awareness of security threats, and awareness of the consequences of security breaches, and noted that security incidents from real-life situations should be included in SETA.

Yazdanmehr and Wang (2016) hypothesized an ethical climate would influence ISP-related descriptive norms, injunctive norms, and subject norms and that the ISP-related norms would influence ISP-related personal norms, which in turn would influence ISP compliance behavior in a 2016 survey-based study with 201 Americans that worked in an organization with ISP. The authors also hypothesized that ISP-related ascription of personal responsibility would influence ISP-related personal norms and have a moderating effect on the relationship between ISP-related personal norms and IS compliance behavior (Yazdanmehr & Wang, 2016). Yazdanmehr and Wang hypothesized that ISP-related awareness of the consequences would influence ISP-related personal norms and have a moderating effect on the relationship between ISP-related personal norms and ISP compliance behavior. There was no support for the relationship between ISP-related descriptive norms and ISP-related personal norms, and no support for the moderating effect of ISP awareness of the consequences on the relationship between ISP-related personal norms and ISP compliance behavior. The results supported all other hypothesized relationships, and the support for the relationship between ISP-related awareness of the consequence and ISP-related personal norms was significant at p < .001.

The Impact of Awareness

Awareness was the third independent variable in the study. I hypothesized that *awareness* would explain the variance of *intention* and informally hypothesized that the relationship between *awareness* and *intention* would be stronger than the relationship between *severity* and *intention* and the relationship between *vulnerability* and *intention.* The results indicated *severity* had a stronger impact on *intention* than *awareness,* and *awareness* had a stronger impact on *intention* than *vulnerability.*

Sanctions tend not to affect individuals who justify non-compliance with ISP because they have little time to accomplish a task and consider compliance with ISP a barrier to task completion (Goo et al., 2014). Enforcing ISP requires us to defeat the allure of neutralization and offset the ledger by making the individual aware of the consequences of failure to comply with ISP. I argue that awareness, as defined by Yazdanmehr and Wang (2016), is the force that would change the values on the positive and negative sides of the ledger, so they are reversed. The person would now think the negative ledger value from not following rules and risking exposure of data is higher than the positive ledger value of doing the job efficiently and will choose to follow ISP.

Intention to Comply

The intention to comply with ISP was the dependent variable being measured in this study. However, there is much debate on the strength of the correlation between intention and behavior with Crossler et al. (2014) noting that intention data are less reliable than behavioral data. The theory of planned behavior predicts that intention leads to behavior (Ajzen, 1985), and the intention to perform an act has been strongly correlated with the performance of the act (Clapper & Richmond, 2016; Moody & Siponen, 2013). There are few studies where researchers measured behavior because it is expensive and difficult (Bélanger et al., 2017).

Observing Behavior

Studies in which behavior is directly observed are rare (Bélanger et al., 2017). Some ISP researchers such as Ifinedo (2014) and Sommestad et al. (2014) claimed to have measured behavior but did so by asking the user if they complied with ISP in a survey. Behavior data obtained in a survey may be flawed because of the tendency of self-report to cause common methods bias (Warkentin et al., 2016) or social desirability bias. Social desirability bias would encourage participants to provide false responses to questions about behavior (Lebek et al., 2014). The sensitive nature of security violations would discourage organizations from sharing quantitative information about violations (Lebek et al., 2014), and experiments that involve observation or electronic monitoring are difficult (Bélanger et al., 2017; Lebek et al., 2014).

Bélanger et al. (2017) used the theory of planned behavior and protection motivation theory to construct a research model that predicted the intention to comply with ISP and to predict that intention leads to compliance behavior. The study involved an experiment in a university where a notification was sent to users that they must begin using stronger passwords (Bélanger et al., 2017). The researchers used work done by Rogers in 1995 that categorized individuals based on the speed with which they adopt new technology innovations (Bélanger et al., 2017). Rogers used standard deviation from a normal distribution to divide adopters into innovators, early adopters, early majority, late majority, and laggards (Bélanger et al., 2017). Bélanger et al. condensed these five categories to three and labeled the first two as early conformers, labeled the second two as late conformers, and labeled laggards as non-conformers.

The researchers measured compliance behaviors by measuring the time between the notification and the time the user changed the password. The research model indicated that higher levels of the theory of planned behavior and protection motivation theory constructs would correlate with sooner adoption of strong passwords (Bélanger et al., 2017). The sample was composed of 535 participants in a university who were surveyed to measure the levels of the constructs in the research model and who were monitored to measure the behavior of switching to strong passwords (Bélanger et al., 2017). The results indicated that the intention to confirm early was highly correlated with early conformance behavior. Attitude was highly correlated with intention to conform early, while subjective norms and behavioral control were not (Bélanger et al., 2017). The researchers found organizational triggers correlated with ISP awareness, and ISP awareness, threat severity, and vulnerability were correlated with attitude (Bélanger et al., 2017).

Warkentin et al. (2016) conducted a longitudinal deception study and measured the response college students in the Southeast United States had to a fake virus threat. The researchers gave a presentation to 1800 college students and explained that a new computer virus called ZedCode was causing damage to computers and that the only way to prevent the virus from damaging computers was to install ZedAlert and run it once a week (Warkentin et al., 2016). The ZedAlert software reported the students' use of the software to a server and sent a survey to the student if they stopped using it. This experiment was a novel way of directly observing behavior.

Summary and Conclusions

This chapter contained a description of the variables used in this study, a description of the literature review search methods, and a review of past research that used similar theories and models. I have explained the research model and defined the theories that support the research model. The chapter also contained a justification for the research and the methods that were used to analyze the data.

Many ISP studies have used GDT with inconsistent results. Cheng et al. (2014) found that sanctions had little or no effect on the intention to use the internet for personal reasons in the workplace. More research is needed that explores the factors that affect compliance with ISP (Ifinedo, 2014), and the gap in the literature on the reasons that individuals choose not to comply with ISP (Siponen & Vance, 2014). D'Arcy et al. (2014) noted that knowledge of the factors that influence the decision to comply or not comply with ISP is incomplete and that there had not been enough studies on information security, especially as it relates to the connection between information security awareness and ISP compliance behavior.

Employees who chose not to comply with ISP may use neutralization techniques to overcome the remorse associated with violating norms. ISP researchers have identified neutralization as an important concept that needs further research. Bauer et al. (2017) and Bauer and Bernroider (2017) suggested that more research is needed on how neutralization techniques are used to justify non-compliance with ISP. Teh et al. (2015)

conducted an ISP compliance study with neutralization in Malaysia and suggested conducting further research in other cultures.

The following chapter contains a detailed description of the statistical methods and the rationale for the study. The chapter contains an explanation of the sampling procedures and justification for the data analysis plan. I conclude Chapter 3 by explaining the steps for screening data, discussing threats to internal and external validity, and providing the procedures for ensuring the ethical treatment of participants.

Chapter 3: Research Method

The purpose of this quantitative study was to improve the knowledge of the factors related to an individual's intention to comply with ISP. Improving the understanding of the antecedents that lead to ISP compliance could enable information security officials to increase compliance with ISP and reduce the frequency of data breaches. Reducing the number of data breaches may cause positive social change by reducing the personal and financial damage caused to individuals and organizations.

Chapter 3 contains the research design and rationale of the study, the methodology of the study, and a description of the sample population and sampling procedures. Also included are a definition of the instrument, explanation and justification of the data analysis plan, and a description of procedures for data screening. In addition, the chapter contains the research questions and hypotheses, followed by an explanation of issues that threaten the validity of the study. The chapter concludes with a description of the procedures used to ensure ethical practices followed by a summary of the chapter.

Research Design and Rationale

This study design had three independent variables and one dependent variable. GDT is the basis for the independent variables *severity* and *vulnerability*, and SETA programs is the basis for the independent variable *awareness*. The dependent variable was *intention*. The variables were measured at the individual level. The variables *severity, awareness,* and *intention* are interval and ranged on a 19 point scale from one to seven in increments of .0, .33, and .67 that was created by indexing the interval seven-point Likert data from the survey by using the means of the scores from the questions that represented each variable. The variable *vulnerability* was interval and ranged on a 13-point scale from one to seven in increments of .0 and .5 that was created by indexing the interval seven-point Likert data from the survey by using the means of the scores from the questions that represent *vulnerability*.

The study was a quantitative, non-experimental, correlational, cross-sectional design that quantified the participant's perceptions of *severity*, *vulnerability*, *awareness*, and *intention* using a survey. I analyzed the values for these variables using multiple regression to determine and rank the strength of the relationships between the variables. Quantifying the perceptions of the participants as variables and determining the strength of the influence between the variables using multiple regression revealed potential relationships between the independent variables *severity*, *vulnerability*, *awareness*, and the dependent variable *intention*, and the relative strengths of these relationships. Information security professionals could use the results to develop SETA programs that emphasize reasoning that will influence individuals to comply with ISP. In this study, I examined factors related to *intention*. Consequently, there were no moderating or mediating variables in the research design.

This research design was consistent with other studies that have investigated the factors related to information security compliance. Al-Mukahal and Alshare (2015) conducted a cross-sectional, non-experimental, correlational study based on GDT and NT with 234 employees in Qatari organizations with ISP. The authors used a survey to measure the participants’ perceptions of the independent variables awareness of ISP, clarity of ISP and positive impact of ISP, and the dependent variable, intention to violate ISP. The data were analyzed using multiple regression in SPSS, and the results indicated that awareness of ISP did not reduce the effects of neutralization, but that clarity of ISP and the positive impact of ISP did reduce the effects of neutralization (Al-Mukahal & Alshare, 2015). Alshare et al. (2018) measured the correlations between deterrence severity and violations of ISP, and between deterrence celerity and violations of ISP in an American university. The researchers gathered the data using an online survey and analyzed it using multiple regression in SPSS.

Anwar et al. (2017) conducted a cross-sectional, non-experimental, correlational study that used an anonymous online survey of 481 full and part-time employees in technology jobs to measure the constructs from protection motivation theory along with self-reported security behavior and several other constructs. The survey measured all responses using a seven-point Likert scale. The data were analyzed using regression in SPSS, and the results indicated that there were statistically significant differences in the computer skills, security self–efficacy, and self-reported security behavior of men and women (Anwar et al., 2017).

Tsai et al. (2016) conducted a cross-sectional, non-experimental, correlational study and utilized Amazon’s Mechanical Turk to conduct an online survey with 988 participants. The questions in the instrument used different scales depending on the question. The authors included a quality control question that had an obvious answer and used this question to determine if the participant had rushed through the survey selecting random answers (Tsai et al., 2016). The researchers analyzed the data using hierarchical regression and revealed that protection motivation theory self-efficacy, severity, and vulnerability were not correlated with the intention to use secure online practices, but that response-efficacy and response cost were correlated with the intention to use secure online practices (Tsai et al., 2016).

Belanger et al. (2017) conducted a cross-sectional, non-experimental, correlational study based on protection motivation theory and the theory of planned behavior and used an online survey with 535 participants. The survey contained statements about being an early adopter of information security practices, and the answers were based on a seven-point Likert scale that ranged from *strongly agree* to *strongly disagree* (Bélanger et al., 2017).

Methodology

The following section contains a description of the population, sampling process, and procedures for recruiting participants for the study. The section also contains an explanation of the source of the instrument, the justification for using the instrument, and how the constructs have been operationalized. I then provided and justified the data analysis plan and describe threats to validity and the mitigation techniques for these threats. The section concludes with an explanation of the procedures for protecting study participants and ensuring the ethical conduct of the study.

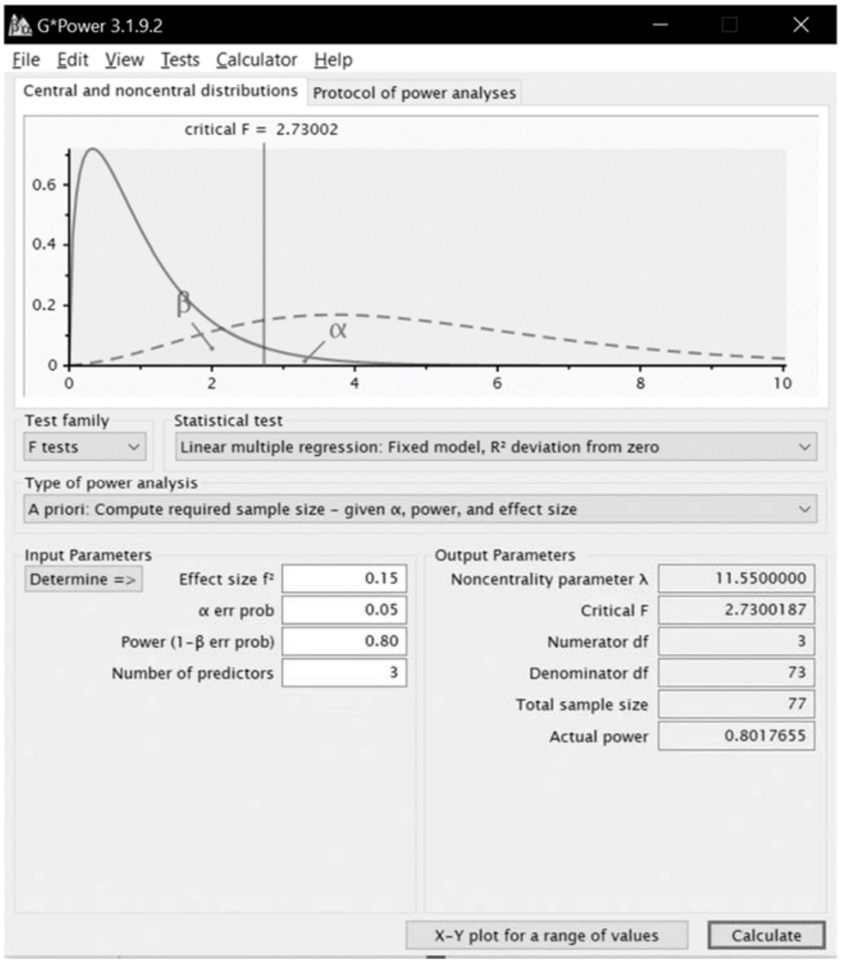
Population

The target population for this study was adults living in the United States who work in a higher education organization with an ISP. The survey solicitation targeted employees who lived in the United States, were 18 years old or older, and worked in the education industry as a university professor, administrator, or staff member. The survey contained screening questions designed to disqualify the participant if they did not match the target population. Consequently, to the best of my abilities, the sample did not include minors, facility residents, mentally disabled individuals, emotionally disabled individuals, pregnant women, my subordinates, students, or clients, individuals for whom English is a second language, individuals in crisis, or economically disadvantaged individuals. The selection and screening questions did not filter for participants over the age of 64 because the Walden institutional review board (IRB) determined that this excluded a potentially valuable population that did not need protection for a survey about the workplace. The screening questions filtered for employees of The University of Oklahoma since it was determined by the IRB that recruitment of participants at the same institution where I work would be coercion. The selection was random and did not collect information that would identify the participants so that all data were anonymous.

Sampling and Sampling Procedures

The sampling strategy used a random probability sampling technique to select participants from a pool of individuals that match the criteria defined for the population. The Qualtrics survey company sent the solicitation to 1288 employees in the education industry and then filtered to include only participants that matched the desired sample population. Probability sampling provided a sample that is representative of the overall population and enabled the study to make inferences about the population (Burkholder, Cox, & Crawford, 2016). The criteria for the population were adults living in the United States who were not part of a vulnerable population and worked for a higher education institution with an ISP. The survey started by asking if the participant worked in a higher education organization with ISP. Participants that answered no were not part of the sample.

The G*Power program was used to determine the appropriate sample size for a study where the alpha level is .05, the power is .8, the desired effect size is medium at .15 (Cohen, 1992), and the number of predictors is three. Figure 2 shows the results and indicate that the sample size should be 77. The alpha level was set at .05. The power was set at .80, which is an appropriate level for general use (Cohen, 1992). Power levels lower than .80 increase the risk of a Type II error, and levels above .80 tend to result in sample sizes that are beyond the financial restrictions of the researcher (Cohen, 1992).


G*Power 3.1.9.2
File Edit View Tests Calculator Help
Central and noncentral distributions
Protocol of power analyses
critical F = 2.73002
0.6
0.4
0.2
0
0
2
4
6
8
10
β
α
Determine =>
X-Y plot for a range of values
Calculate

Test family: F tests

Statistical test: Linear multiple regression: Fixed model, R² deviation from zero

Type of power analysis: A priori: Compute required sample size – given α, power, and effect size

Input Parameters

Effect size f²	0.15
α err prob	0.05
Power (1–β err prob)	0.80
Number of predictors	3

Output Parameters

Noncentrality parameter λ	11.5500000
Critical F	2.7300187
Numerator df	3
Denominator df	73
Total sample size	77
Actual power	0.8017655

Figure 2. G*Power Results for Sample Size with a Medium Effect Size

While p-values have been used to measure and interpret the significance of research results, effect size is a more meaningful way of indicating the significance of an analysis (Coe, 2002). Cohen (1992) established the standard for effect sizes and defined a medium effect size as one that a careful observer would notice without conducting any analysis. He established a small effect size as one that was much smaller than medium but still meaningful, and a large effect size was set at the same distance above medium that small was below medium (Cohen, 1992). Detecting a small effect size with an alpha of .05, a power of .8 and three predictors would require a sample size of 550, which is beyond the financial scope of this study.

Other factors affect the sample size. The data from the dependent variable was skewed because of the nature of answering a question about violating a policy (Barlow et al., 2013), leading to the need for a larger sample (Allison, 1999). Multiple regression provides robust statistical power for data sets with skewed data for a data set of 100 samples and less than five variables (Allison, 1999). Consequently, the target sample size was 100.

Procedures for Recruitment, Participation, and Data Collection

The original recruitment protocol for the study involved contacting security officers at institutions of higher learning in the local region and asking them to forward an email invitation to participate in the study to employees at the institutions. However, the IRB determined this process to have a potential for bias and a sample that was not random. The second approach involved contacting dozens of higher education associations and asking them to agree to distribute the survey. When this failed, I examined similar Walden dissertations and found that other studies had utilized survey companies to find participants. The IRB and research committee approved this approach. Survey hosting cost $599.00, and each usable survey cost $30.00 for a total of $3,599 to obtain the minimum number of samples to complete the research. Data gathering started on February 12, 2020, and was completed on February 14, 2020.

Qualtrics sent invitations via email to participants in a group that has been determined to match the parameters required for the study. All data were anonymous and contained no demographic or identifying information for the participants. The survey started with the consent form. Participants answered each question using a seven-point Likert scale. The participants were able to stop the survey at any time if they decided not to participate.

Instrumentation and Operationalization of Constructs

I acquired the questions that measured the constructs *severity*, *vulnerability*, and *intention* from an instrument used by Herath and Rao in 2009 in an online survey with 78 employees in the western New York area who used computers and the Internet in their daily routine. Herath and Rao (2009) pretested the instrument with academic experts in the fields of management information sciences, sociology, and computer science. Experts from the banking industry and cybersecurity field who were working for the Federal Bureau of Investigation also validated the instrument. (Herath & Rao, 2009). Survey items were reworded, added, or deleted based on the results of the pretest (Herath & Rao, 2009).

The researchers conducted a pilot study with 25 employees and 23 students from a large American university in the northeast (Herath & Rao, 2009). They examined construct reliability, convergent validity, and discriminant validity to assess reflective constructs (Herath & Rao, 2009). The researchers assessed composite reliability scores, and all constructs exceeded the .70 threshold indicating that items were free from random error (Herath & Rao, 2009). They assessed convergent validity to ensure consistency across items by measuring how partial least squares indicators loaded on hypothesized factors. It was determined to be acceptable. The loadings were all significant at p < .001 and with magnitudes above .070. Herath and Rao (2009) assessed discriminant validity by measuring the square root of the average variance extracted, and ensuring they were larger than the absolute value of the inter-construct correlations. The correlations between the constructs were low enough to ensure that all constructs were distinct. Cronbach's alpha test confirmed the reliability of the test scale (Herath & Rao, 2009). Dr. Herath has provided written consent to use the questions from the instrument for this study in an email that is included in Appendix A.

I acquired the questions that measured *awareness* from a study conducted by Yazdanmehr and Wang in 2016 with an online survey with 201 participants in the United States who worked in organizations with ISP. The sample was random. The survey asked participants if they worked in an environment that had an ISP, and only those participants that responded in the affirmative were allowed to complete the survey. A random selection of participants pretested the questions through an online survey tool, and a pilot study was conducted with MBA students from an American university in the southwest (Yazdanmehr & Wang, 2016). Yazdanmehr and Wang (2016) validated the instrument by examining item reliability, composite reliability, convergent validity, and factor and cross loadings. The results indicated that cross correlations were smaller than the square root of the average variance extracted; all constructs' average variance extracted were higher than 0.5 indicating that the variance of the constructs was higher than error variance; all correlations between the constructs were small indicating they were distinct, and all items loaded highest on the intended constructs (Yazdanmehr & Wang, 2016). In addition, the researchers used Harman's one-factor test to determine if common method bias had affected the data set, and the results indicated that no single factor was found to explain the majority of variance (Yazdanmehr & Wang, 2016). They used the Marlowe-Crowne social desirability scale to examine the possibility that social desirability bias had influenced the data, but the results indicated there was no significant influence with $\beta = 0.01$, and $p > 0.1$ (Yazdanmehr & Wang, 2016). Dr. Yazdanmehr has provided written consent to use the questions from the instrument for this study. A copy of the written consent from Dr. Yazdanmehr is included in Appendix A.

The variables measured in the study were indexed from the scores of the survey questions associated with each variable as shown in Appendix C. Participants answered survey questions using a seven-point Likert scale that represents the level of agreement the participant had with a statement. The Likert scale had the following values:

1 – *Strongly disagree*

2 – *Disagree*

3 – *Somewhat disagree*

4 – *Neither agree nor disagree*

5 – *Somewhat agree*

6 – *Agree*

7 – *Strongly agree*

The first independent variable was *severity*. *Severity* represented the level of the participant's perception of the intensity of sanctions that the participant's organization would use to punish individuals who do not comply with ISP. The second independent variable, *vulnerability*, represented the participant's perception of the level of certainty that the participant's organization would punish individuals who do not comply with ISP. The third independent variable, *awareness*, represented the level of awareness the participant had about the damage caused to the organization and its employees by not complying with ISP. The dependent variable, *intention*, represented the level of intent the participant had to comply with ISP.

Data Analysis Plan

Data gathered in an online survey and analyzed using multiple regressions with IBM'S SPSS version 25 provided the statistical information used to determine the strength of the relationships between each of the independent variables and the dependent variable and address the four research questions. Multiple regression was the appropriate process for measuring the relationships between multiple independent variables and a single dependent variable (Nathans, Oswald, & Nimon, 2012) and can accurately analyze survey data even when the data are skewed (Norman, 2010). There were no covariates or confounding variables in the research model.

The data resulting from a survey of self-reported behavior was likely to be skewed (Barlow et al., 2013), and multiple regression analysis is most robust when the data are normally distributed and not skewed (Norman, 2010). The research model in this study contained less than five variables, and the sample size was 100. Data sets with at least 100 samples and less than five variables are appropriate for multiple regression even with skewed data (Allison, 1999)

Multiple regression is most robust when there is a normal distribution of errors in the data (Williams et al., 2013) such that the mean of the errors is zero (Durbin & Watson, 1950), known as homoscedasticity (Williams et al., 2013). However, multiple regression is still robust with larger sample sizes, even if errors are not normally distributed (Williams et al., 2013). Errors should have a finite and constant level of variance across all levels of the independent variables (Williams et al., 2013). A scatterplot of residuals revealed if the errors are not consistent (Fox, 1991), and the results indicated that the errors were consistent. If there had been heteroscedasticity, bootstrapping would have been used (Williams et al., 2013) to confirm the results provided by SPSS multiple regression.

Multiple regression assumes a linear relationship between all possible pairs of variables and that the variance of the dependent variable is homogenous across levels of the independent variables (Warner, 2013). I created scatterplots for all pairs of independent variables and the dependent variable to observe the spread of dots around the fit line. An even spread of data points around the fit line indicated that the relationships between the variable sets were linear (Warner, 2013).

Extreme outlying data can reduce the reliability of multiple regression. Cook’s distance was used to determine if outliers are affecting robustness (Williams et al., 2013), and the results indicated that no outliers were affecting the results. There were several options for addressing outliers that may have influenced the analysis. Outlying data could have been identified and assessed to determine if the data were extreme, and invalid data would have been removed.

Multicollinearity occurs when there is correlation between the independent variables (Allison, 1999). Multicollinearity increases the standard errors of the coefficients and reduces the accuracy of the analysis (Allison, 1999). I assessed multicollinearity by examining the variance inflation factors generated by SPSS (Williams et al., 2013). A variance inflation factor of less than 3.33 is considered acceptable (Petter et al., 2007), and the results were less than 3.33.

Multiple regression assumes that error terms in the model are independent and not correlated (Durbin & Watson, 1950). A violation of this assumption will not bias the coefficients but will cause the estimates to be inefficient (Williams et al., 2013). SPSS was used to perform the Durbin-Watson test to determine if errors are dependent (Chan, 2004; Garson, 2012). The Durbin-Watson coefficient *d* will range from zero to four (Chan, 2004). Coefficient *d* values near one indicate a negative correlation of the errors; *d* values near four indicate a positive correlation of the errors (Chan, 2004), and *d* values between 1.5 and 2.5 indicate no correlation of the errors (Garson, 2012). The results of the Durbin-Watson test indicated there was no correlation of the errors.

The research questions and hypotheses were as follows:

RQ1: What is the relationship between *severity* and *intention*?

$H_0$1: There is no relationship between *severity* and *intention*.

H_a1: There is a relationship between *severity* and *intention*.

RQ2: What is the relationship between *vulnerability* and *intention*?

$H_0$2: There is no relationship between *vulnerability* and *intention*.

H_a2: There is a relationship between *vulnerability* and *intention*.

RQ3: What is the relationship between *awareness* and *intention*?

$H_0$3: There is no relationship between *awareness* and *intention*.

H_a3: There is a relationship between *awareness* and *intention*.

RQ4: What is the relationship between *severity*, *vulnerability*, and *awareness*, taken collectively, and *intention*?

$H_0$4: There is no relationship between severity, vulnerability, and awareness, taken collectively, and intention.

H_a4: There is a relationship between *severity*, *vulnerability*, and *awareness*, taken collectively, and *intention*.

Research questions that ask how much each independent variable in a research model contributes the most to the variance of the dependent variable are often answered using standardized regression weights or part correlations (Tonidandel et al., 2009). Hypotheses one through three were that there is a relationship between each of the independent variables and the dependent variable, and the fourth hypothesis was that the independent variables taken collectively would have a relationship with the dependent variable. The alpha threshold for testing the hypotheses was .05. The null hypothesis was rejected if the *p*-value was lower than .05.

I considered other forms of analysis for this study. Spearman's coefficient has been recommended as a technique for measuring covariance (Warner, 2013). Spearman's rank correlation can only handle simple designs and is rarely used (Norman, 2010). Studies have shown that analyses using Pearson's correlation and Spearman's correlation tend to provide the same results even with skewed data (Norman, 2010) and that Spearman's correlation is not the best means for determining the level of variance an independent variable explains in a dependent variable (Hauke & Kossowski, 2011).

The Kendall rank correlation coefficient only provides probabilities that data are in a particular order and not correlations between variables (Hauke & Kossowski, 2011). Bivariate correlations would reveal the strength of correlations in one-on-one relationships between variables, but would not provide information on the variance that might be shared between predictor variables (Warner, 2013). Researchers have used partial least squares structural equation modeling in many studies reviewed in this proposal but it is more appropriate for complex models with a large number of latent constructs that have inner-model relationships (Bauer & Bernroider, 2017).

Threats to Validity

A study can be said to have internal validity when the design of the study is such that one has high confidence that all rival hypotheses have been eliminated and that the variation of the dependent variable is explained by the independent variable and not other sources of influence (Onwuegbuzie, 2000). External validity describes the level to which the results of the study can be generalized across multiple populations, settings, and times (Onwuegbuzie, 2000). Donald Campbell and Julian Stanley are known for their seminal work on external and internal validity (Onwuegbuzie, 2000). Onwuegbuzie (2000) noted that Campbell and Stanley (1963) focused on experimental research and that there were many more threats to validity to consider for non-experimental quantitative research. The threats to validity defined by Onwuegbuzie, how they relate to this study, and what will be done to mitigate these threats are described in the following sections.

External Validity

The sample population was adults in the United States that are not part of a vulnerable population and that work in higher education institutions with an ISP. Consequently, the results of the study are generalizable to any organization in the United States that has an ISP increasing the external validity of the study. This limits the application of the findings to western cultures that are similar to the United States.

The study measured the *intention* to comply with ISP and did not observe compliance behavior. While the goal of the study was to improve compliance with ISP and not improve the *intention* to comply with ISP, measuring behavior is expensive (Bélanger et al., 2017) and beyond the fiscal limitations of this study. There has been debate on the strength of the correlation between intention and behavior (Crossler et al., 2014), yet studies have found a strong correlation between the intention to act and the performance of an act (Clapper & Richmond, 2016; Moody & Siponen, 2013). Measuring intention instead of behavior may limit the generalizability of the study.

When participants know they are being observed or measured, there is a potential for participant reactivity (Onwuegbuzie, 2000), especially as it relates to being asked questions about complying with policies. An anonymous online survey mitigated some of this threat to external validity. Social desirability bias occurs when a person tends to provide socially desirable responses when describing oneself (Johnson, Fendrich, & Mackesy-Amiti, 2012). Internet-based surveys can provide a high level of anonymity, which can increase self-esteem, decrease social anxiety, and mitigate issues with social desirability (Fox et al., 2003). The fact that the survey was anonymous and did not gather personally identifiable data may have mitigated the risk associated with self-reported behavior and encouraged participants to respond honestly (Bélanger et al., 2017). Adding questions from the Marlowe-Crowne Social Desirability scale to the survey to assess the tendency of each participant to answer in a socially desirable way may have increased quality. It is questionable if this would have improved the dataset. Some research indicates that the Marlowe-Crowne Social Desirability scale is not a robust predictor of the tendency to provide socially desirable answers on a survey (Johnson et al., 2012)

Temporal validity may threaten the external validity of the study (Onwuegbuzie, 2000). The data were gathered and analyzed at a specific point in time. The information gathered in the study was associated with technology used to enforce ISP at a specific time, meaning that the study findings are only be generalizable for a period before technology changes to the point that the information is no longer useful.

Researcher bias can threaten the external validity of a study because the values of the researcher could affect the collection of data (Onwuegbuzie, 2000). The goal of the study was to compare the effects of sanctions and awareness. As an executive at a health care institution, I am aware of the possible punitive actions that can be taken when employees do not follow ISP and have participated in discussions about these policies, which could have influenced the design of the study to favor *sanctions* over *awareness*. Personal bias should not affect the external validity of the study because the instrument was designed and validated by other researchers, and the analysis method was determined by the committee chair.

The specificity of variables or the unique way in which specific variables are measured by a specific instrument at a specific time with a specific group of participants can threaten the external validity of a study (Onwuegbuzie, 2000). The more specific and unique each of the conditions is defined, the less generalizable the results will be (Onwuegbuzie, 2000). The participants were a randomly chosen sample from across the United States, decreasing the specificity of the participant selection. The time of the study was February 12, 2020, to February 14, 2020. There was no control over the specific time of the survey. Previous research defined and validated the variables and the survey instrument. The validations for the sanction and intention variables included reviews by academic experts, pilot tests, and statistical analysis, including tests for construct reliability, convergent validity, discriminant validity, and Cronbach’s alpha test (Herath & Rao, 2009). Yazdanmehr and Wang (2016) pretested the variable awareness in a pilot study and used statistical analysis techniques including item reliability, composite reliability, convergent validity, and factor and cross loadings to validate the construct and how it was measured.

Internal Validity

The use of multiple regression with survey data statistically limited the study to finding correlations and precludes determining causal relationships. While it could be argued that any one employee’s *intention* to comply with ISP is unlikely to cause *sanctions* or *awareness* to change and therefore the relationships between the variables could be causal, one could also argue that a large group of individuals refusing to follow ISP could be the cause for changes in policy that influence the use of sanctions and changes in the organization's SETA programs that could affect *awareness*. The use of multiple regression to analyze survey data limited the internal validity of the study since causal relationships cannot be determined.

Onwuegbuzie (2000) defined many possible threats to internal validity and grouped them based on the type of threats. Some threats are temporal due to the way an experiment or treatment is administered (Onwuegbuzie, 2000). Some threats are associated with the way the sample was collected or the way the instrument is deployed (Onwuegbuzie, 2000). There are other threats related to the nature of interventions. I have described each threat briefly in the following sections.

Some threats such as history, and history X treatment interaction, were not relevant to the study because there was one interaction with each participant, and there was no prior contact or events (Onwuegbuzie, 2000) for the participant to reference. Maturation, which describes changes in a participant during the study, mortality, which describes the loss of a participant, and sample augmentation bias, which is the addition of a participant (Onwuegbuzie, 2000) did not affect the study because there was one interaction with the participant when the survey is administered. Time X treatment interaction, which occurs when one set of participants are exposed to a treatment longer than others (Onwuegbuzie, 2000), was not a factor in this study because there was no treatment, and only there was only one interaction with the participant. Statistical Regression, the tendency for extreme scores to regress toward the mean on subsequent measures and pretest sensitization, which is an effect that occurs when an individual is tested a second time (Onwuegbuzie, 2000) was not a factor in the study because there was only one measurement.

Differential selection of participants, which occurs when non-random or pre-existing groups are used in a study (Onwuegbuzie, 2000), did not affect this study because the selection of participants was random. Selection interaction effects such as selection by history, selection by maturation, or selection by mortality occur when the researcher selects participants based on a characteristic (Onwuegbuzie, 2000). Differential selection did not affect the study because there was one randomly selected group of participants. Matching bias occurs when a researcher matches participants to a group or treatment (Onwuegbuzie, 2000) but was not applicable because the sample selection was random, and there was no intervention, so the researcher could not match participants to a group or treatment. Observational bias can occur when there is an insufficient sample or a lack of observation or engagement (Onwuegbuzie, 2000). Observational bias could have been a threat to this study if the sample had been too small. The survey company that conducted the survey continued to solicit participants until the sample size reached 100. Sample augmentation bias is a temporal and sample threat and has already been discussed in the temporal section.

Evaluation anxiety is the stressful reaction a person has to being tested or questioned. There was a possibility that the stress of answering questions about compliance with ISP may have caused a participant to answer questions in a way that is not entirely accurate. Online surveys can increase self-esteem and decrease social anxiety (Fox et al., 2003), thus mitigating the effects of evaluation anxiety.

Construct Validity

Construct validity indicates how accurately an element of an assessment instrument measures and represents the given construct (Haynes & Richard, 1995). Constructs are measured to ensure convergent validity, which is an indication that the elements of a construct are more correlated with each other than they are with the elements of a different construct, and to ensure discriminant validity, which is an indication that distinct constructs are not correlated (Petter et al., 2007). Cronbach’s alpha is a technique used to ensure construct validity (Cronbach & Meehl, 1955).

Two previous studies provided the constructs used in this study. An instrument developed by Herath and Rao (2009) provided the constructs *severity*, *vulnerability*, and *intention* and the way these variables are operationalized and measured. The researchers field-tested the instrument with a group of subject matter experts from various relevant fields. Construct reliability, discriminant validity, convergent validity, and composite reliability were all evaluated and found adequate. There is a risk that the validations performed by Herath and Rao were flawed, but this is unlikely given how long the paper has been published and the number of times the work has been cited. Details about how Herath and Rao validated the constructs in their instrument is in the Instrumentation and Operationalization of Constructs section of this proposal.

Yazdanmehr and Wang (2016) provided the construct *awareness*. A group of MBA students evaluated the questions, and the researchers validated the item reliability, convergent validity, composite reliability, and factor and cross loadings. The constructs were distinct. The article is more recent than most, and this definition of *awareness* was novel. Yazdanmehr and Wang validated the measurement of the construct. Details about the validation of the *awareness* construct and instrument are in the Instrumentation and Operationalization of Constructs section of this proposal.

Ethical Procedures

The research design included these steps to protect study participants. IRB approval was obtained before any interaction with participants occurred. The approval date and IRB approval number were included in the final dissertation. The IRB approval number was included on all forms and communications used in the study. The first page of the survey contained a consent form. Participants acknowledged the consent form before proceeding with the survey. No incentives were provided to participants.

Data were anonymous so there was no means of identifying participants. Three of the survey questions asked the participant if they intend to comply with ISP. The intent not to comply with ISP might have damaging consequences for the participant if the information was made available to the participant's employer. Consequently, anonymity was essential in this study. An online survey that gathered the data acted as a barrier between me and the participants and increased the assurance of anonymity.

No educational, financial, medical, mental, sexual, or demographic data were gathered. No data about family history, substance use, or illegal activities were gathered. The survey contained questions about environmental elements and the participant's *intention* to comply with information security policies and should not have induced any psychological stress greater than one would experience in daily life. All data were encrypted and password-protected and will be destroyed five years after the completion of the dissertation. The only individuals with access to the data were the survey company, researcher, and dissertation committee.

Participants were not minors, residents of a facility, economically disadvantaged, mentally disabled, emotionally disabled, in crisis, pregnant, or part of any vulnerable population. Participants may have been elderly because the IRB determined that participants over the age of 64 should be included in the sample population. Participants lived in the United States and were not subordinates or clients of the researcher. Participants were not coerced in any way.

Summary

This quantitative, non-experimental, correlational, cross-sectional study measured and compared the strengths of the relationships between the independent variables *severity*, *vulnerability*, and *awareness* and the dependent variable *intention*. The data collection was through an online survey. Multiple regression provided the statistical data to determine and rank the strengths of the relationships between the independent variables and the dependent variable.

This chapter included information about the research design and rationale of the study, the methodology of the study, and a description of the sample population and sampling procedures. The chapter contained the definition of the survey instrument, a justification for the plan for screening and analyzing data, and the research questions and hypotheses. Finally, it contained a description of the issues that threaten the validity of the study, procedures for mitigating threats to validity, and the procedures that will ensure ethical practices and protect patients.

In Chapter 4, I provide the research questions and hypotheses, present, and discuss the results from prescreening the data. Chapter 4 also contains an analysis of the data and the tests of the four hypotheses. The chapter concludes with a summary of the analysis.

Chapter 4: Results

The purpose of this quantitative study was to measure the relationships between the independent variables *severity*, *vulnerability*, and *awareness* and the independent variable, *intention*. Employees in the United States working in an institution of higher education with an ISP completed a survey. The strength of the relationships between the variables was measured and ranked using multiple linear regression. Finding relationships between the variables may contribute to the knowledge of the factors that affect ISP compliance and enable information security officials to develop policies, education, tools, and enforcement programs that are more effective at increasing compliance with ISP and reducing the number of data breaches.

The following chapter contains the research questions and hypotheses. The chapter also contains the results from the data prescreening. The chapter concludes with a presentation of the results from the multiple regression analysis used to test the hypotheses.

Research Questions and Hypotheses

RQ1: What is the relationship between *severity* and *intention*?

$H_0$1: There is no relationship between *severity* and *intention*.

H_a1: There is a relationship between *severity* and *intention*.

RQ2: What is the relationship between *vulnerability* and *intention*?

$H_0$2: There is no relationship between *vulnerability* and *intention*.

H_a2: There is a relationship between *vulnerability* and *intention*.

RQ3: What is the relationship between *awareness* and *intention*?

$H_0$3: There is no relationship between *awareness* and *intention*.

H_a3: There is a relationship between *awareness* and *intention*.

RQ4: What is the relationship between *severity*, *vulnerability*, and *awareness*, taken collectively, and *intention*?

$H_0$4: There is no relationship between severity, vulnerability, and awareness, taken collectively, and intention.

H_a4: There is a relationship between *severity*, *vulnerability*, and *awareness*, taken collectively, and *intention*.

Data Collection

The data collection plan in the approved proposal involved contacting security officers at institutions of higher learning and asking them to forward an email solicitation to participate in the study to employees at those institutions. However, the Walden IRB rejected this approach because of the possibility that officers would not forward to all employees and would instead forward to a select group causing the sample not to be random. The IRB also questioned excluding persons over 64 years of age. After negotiation, the IRB determined that a survey company could solicit participants randomly and that adults over the age of 64 should be included.

The Qualtrics survey company hosted the survey and sent solicitations to potential participants. Data collection began on February 12, 2020 and completed February 14, 2020. Qualtrics sent solicitations to 1288 individuals that matched several demographic data points. The potential participants were over the age of 17, lived in the United States, worked in the education industry, and worked as a university professor, administrator, or staff member. Of the 1288 individuals solicited, 306 attempted the survey, 50 provided invalid responses (such as answering all the questions with the same answers), and 100 completed the survey for a completion rate of 7.76%. There were no demographic or personally identifying data collected.

The survey started with the informed consent form that the participant had to acknowledge. It then proceeded to screening questions to validate that the participant was appropriate for the study. The first screening question asked if the participant worked in a higher education institution in the United States with an ISP. If the participant answered *No,* the survey ended. The second screening question asked if they were 18 or older to ensure there were no minors in the population. If the participant answered *No,* the survey ended. The third screening question asked the participant if they worked at The University of Oklahoma. Because I am an assistant vice-president at the University of Oklahoma, asking employees of the institution where I work to take the survey would have been a form of coercion. If the participant answered *Yes,* the survey ended. The survey contained three questions to measure the independent variables *severity*, and *awareness,* and the dependent variable *intention.* I indexed the data by taking the mean score of each set of questions for each variable. The result was a potential 19-point scale for the variables *severity,* and *awareness* with values from one to seven in increments of .0, .33, and .67. The survey contained two questions to measure the independent variable *vulnerability*, resulting in a potential 13-point scale from one to seven in increments of .0 and .5.

The survey used for data collection functioned differently than was stated in the proposal. The proposal for this study specified that each question would have an option to choose not to answer the question. The Qualtrics company representative explained that the cost for the services was based on the number of completed surveys and that a complete survey with unanswered questions may not be usable but would still cost $30.00. The representative went on to explain that a participant could leave the survey at any time if they did not want to answer a question and that a participant could complete the survey but choose not to submit it, and that these surveys would not have a cost. This process enabled participants to end the survey at any time and not answer a question if they chose not to, without causing unusable surveys to be included in the data set or increasing the cost of the survey unnecessarily. The representative stated that many Walden students had used this process for enabling participants to leave a survey and that it would be acceptable to the Walden IRB. I updated the design of the survey by removing the option to choose not to answer a question, resubmitted my application, and received approval from the Walden IRB on February 6, 2020. The IRB number is 02-06-20-0597454.

Study Results

Data Prescreening

An examination of the data indicated no missing values and no values outside the range of the Likert scale. The data were gathered using a Likert scale where *strongly agree* was scored as a 1 and *strongly disagree* was scored as a 7, which caused the data to appear inverted with a low score indicating a high level of *intention*. The data were transformed by inverting the Likert scale such that *strongly agree* was changed to a 7, and *strongly disagree* was changed to 1. The scale used to gather the data is in the first column of Table 2, and the scale used to analyze the data is in the second column of Table 2.

Table 2

Likert Scale Used to Gather Data and Likert Scale Used for Analysis

Scale used to gather data	Scale used for analysis
1 – *Strongly agree*	7 – *Strongly agree*
2 – *Agree*	6 – *Agree*
3 – *Somewhat agree*	5 – *Somewhat agree*
4 – *Neither agree or disagree*	4 – *Neither agree or disagree*
5 – *Somewhat disagree*	3 – *Somewhat disagree*
6 – *Disagree*	2 – *Disagree*
7 – *Strongly disagree*	1 – *Strongly disagree*

Skewed distributions were visible in the variables, as was expected (Barlow et al., 2013). Distributions with a skew value between -0.5 and 0.5 are considered to be approximately symmetrical, skew values between -1.0 and -.05 and 0.5 and 1.0 are moderately skewed, and values below -1.0 or above 1.0 are highly skewed (Bulmer, 1979). Figures 3 through 6 are histograms of the four variables. *Vulnerability* had a skew of -0.47, which is approximately symmetric. *Severity* had a skew of -0.53, and *vulnerability* had a skew of -0.81, which are moderate levels of skewness. *Intention* was highly skewed at -1.22. While the data in three of the variables are skewed, multiple regression can still provide an accurate analysis of the data (Norman, 2010).

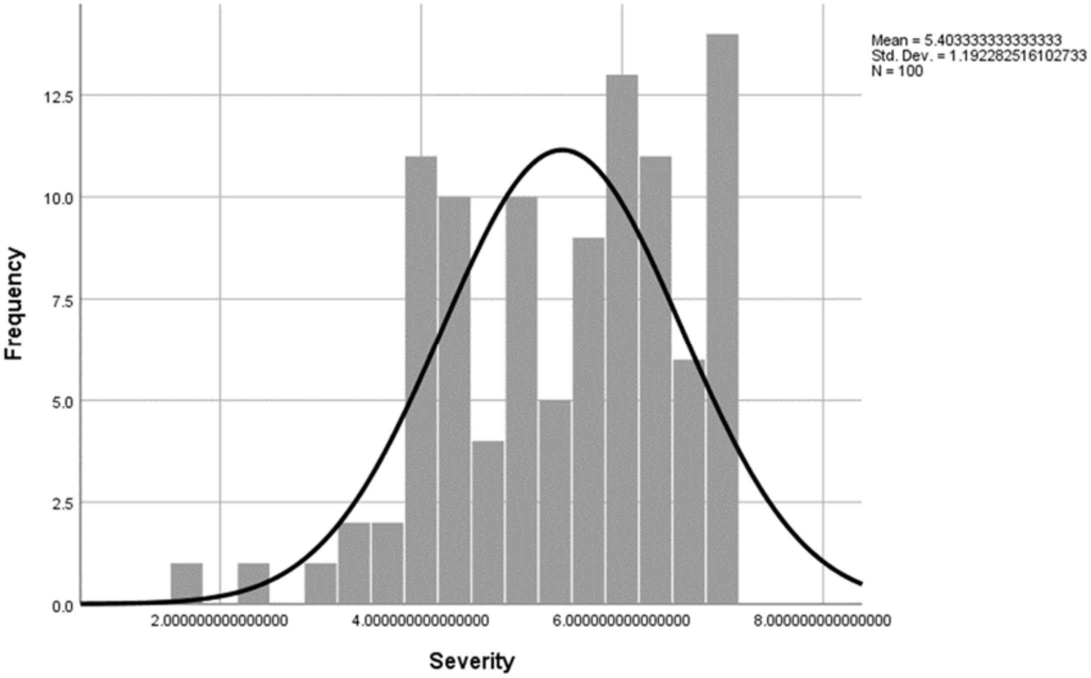


Figure 3. Histogram of the Values for the Independent Variable *Severity*

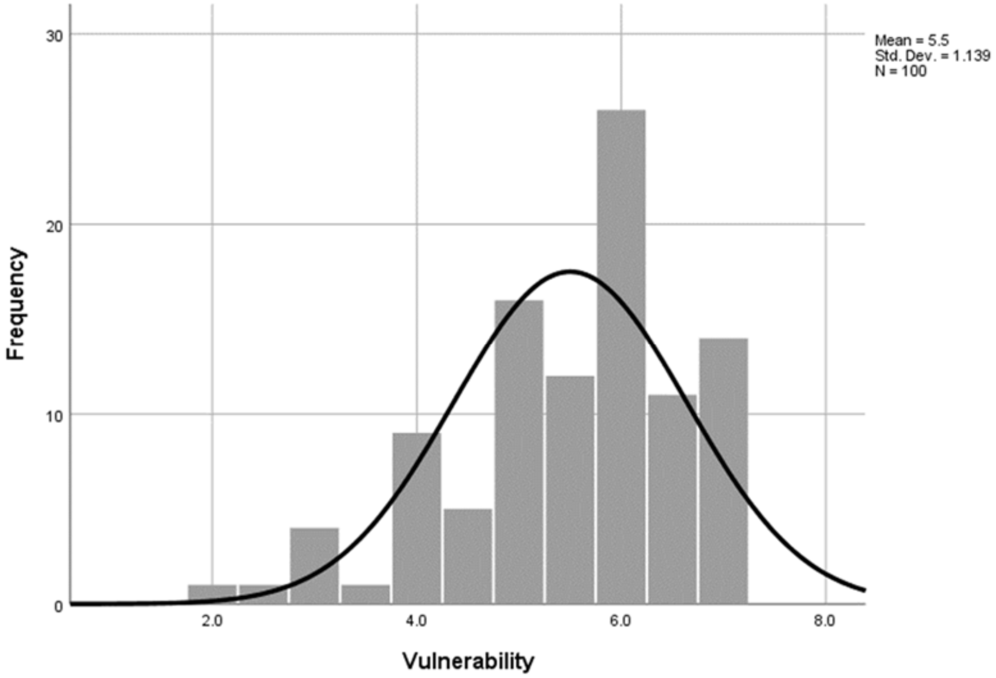


Figure 4. Histogram of the Values for the Independent Variable *Vulnerability*

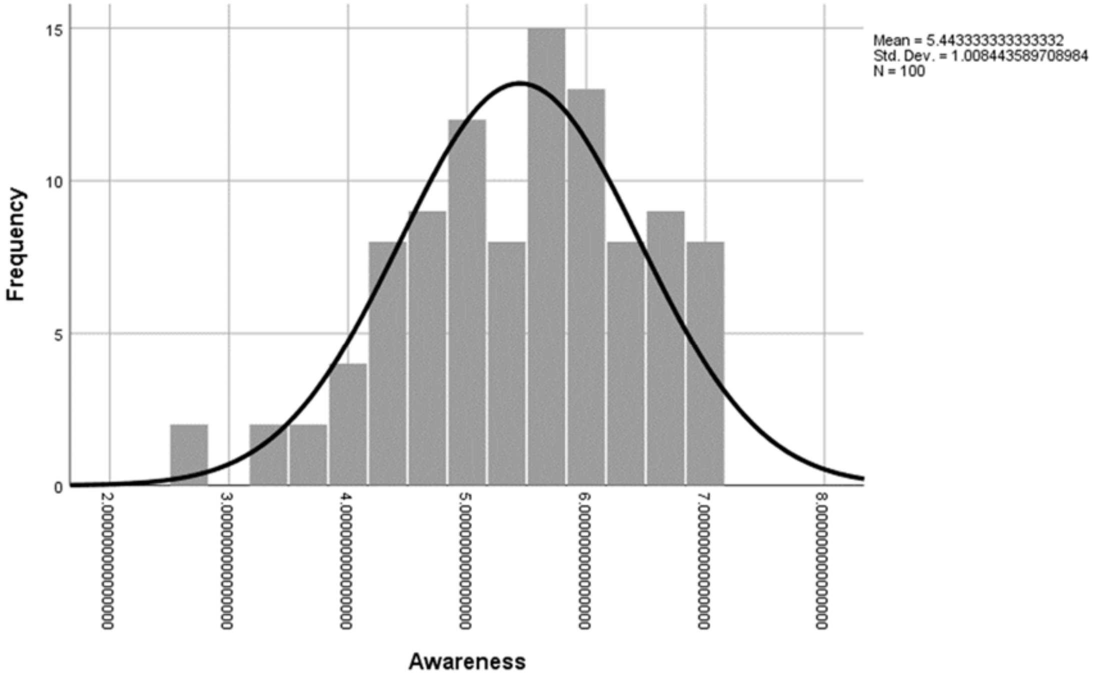


Figure 5. Histogram of the Values for the Independent Variable *Awareness*

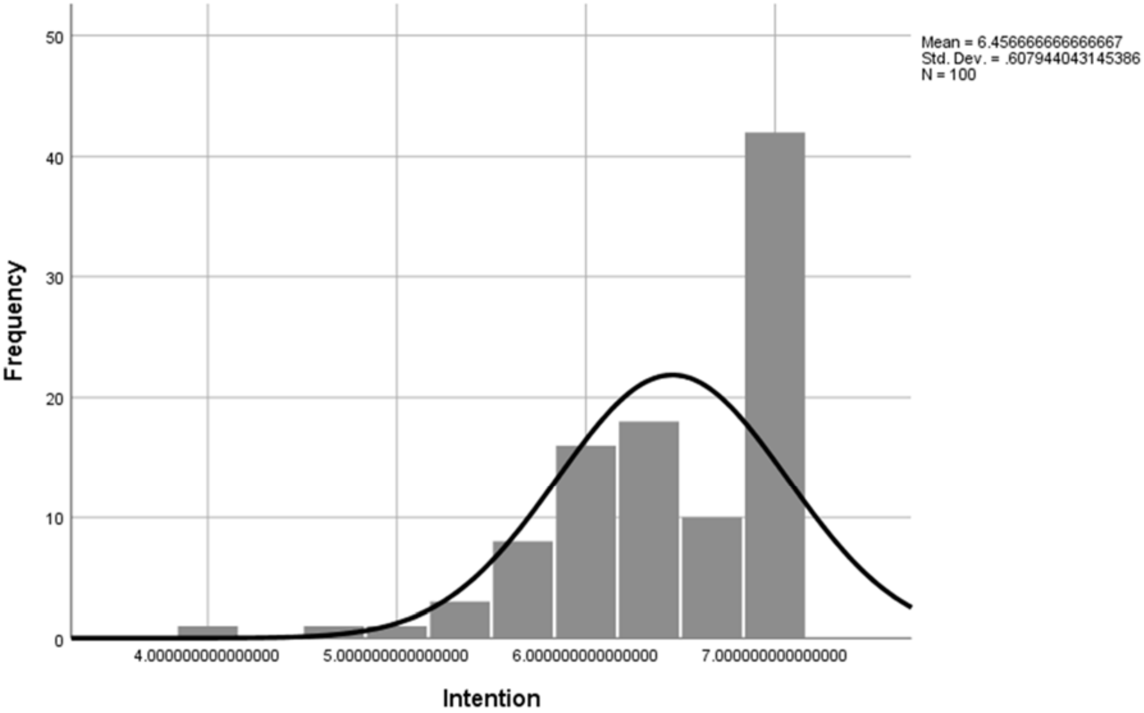


Figure 6. Histogram of the Values for the Dependent Variable *Intention*

A standardized plot of the residuals helped to determine if there was a normal distribution of the errors and that the mean of the errors was zero, which is referred to as homoscedasticity (Williams et al., 2013). The plot shown in Figure 7 for the full model shows a somewhat even spread of residuals above and below the fit line with few outliers and no curvilinear shape indicating the errors were normally distributed with a mean of zero (Allison, 1999). The histogram of the standardized residuals for the full model shown in Figure 8 appears normally distributed with one outlier, causing some skew that is not negatively affecting the analysis. Scatterplots and histograms for the models used for each RQ appear in Appendix B and are similar to scatterplots and histograms for the full model.

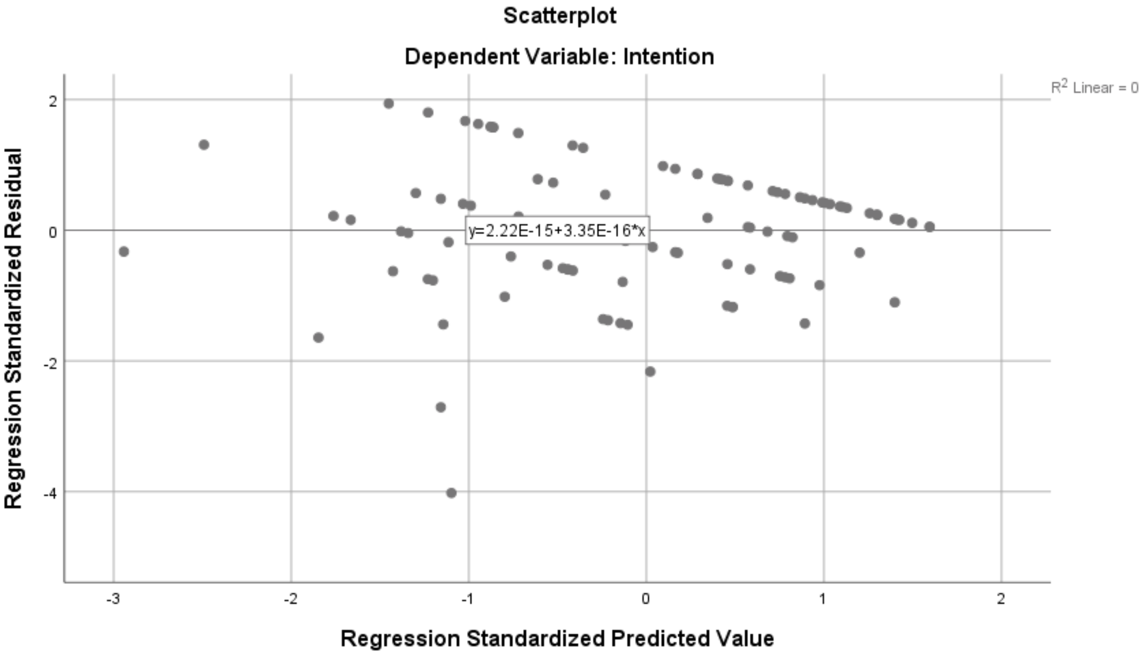


Figure 7. Plot of Standardized Residuals for the Full Model

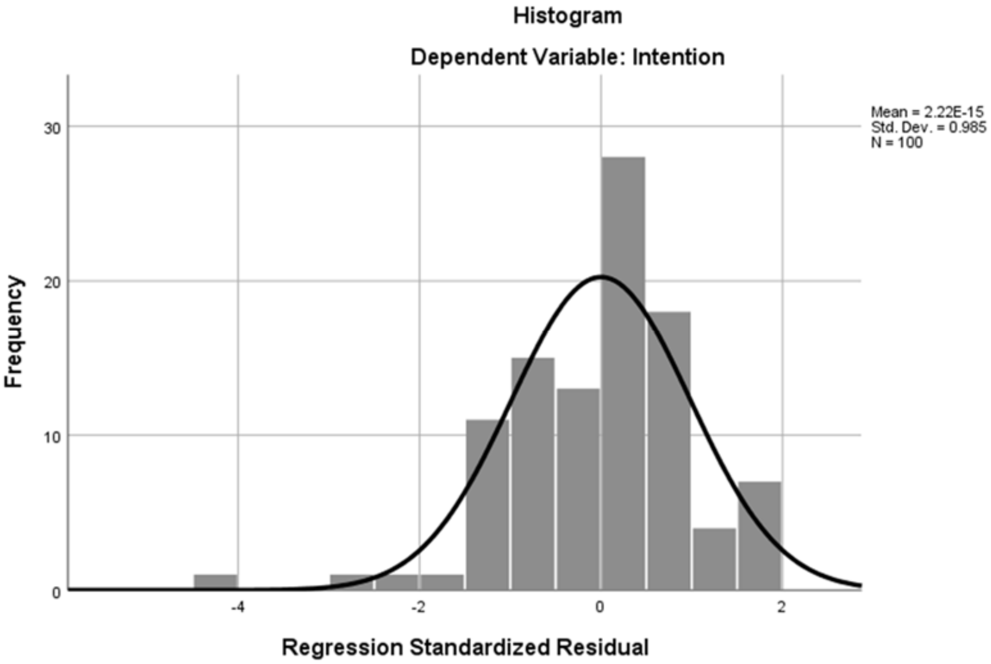


Figure 8. Histogram of the Values for the Standardized Residuals for the Full Model

The next step in data prescreening was determining if there was a linear relationship between the independent variables and the dependent variable. Linear regression requires that all levels of the independent variables are homogenous, with the variance of the dependent variable from its mean (Warner, 2013). In Figures 9-11, scatterplots for each of the three relationships show data evenly spread around the fit line, indicating a linear relationship between the independent variables and the dependent variable.

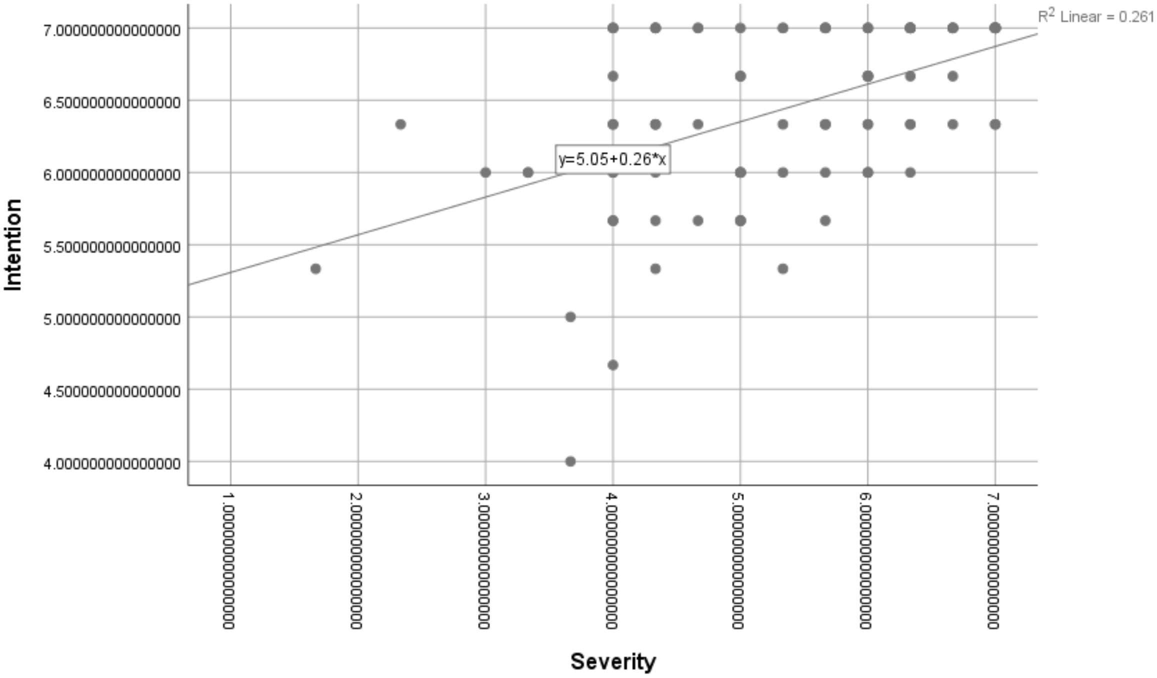


Figure 9. Scatterplot of the Values for *Severity* and *Intention*

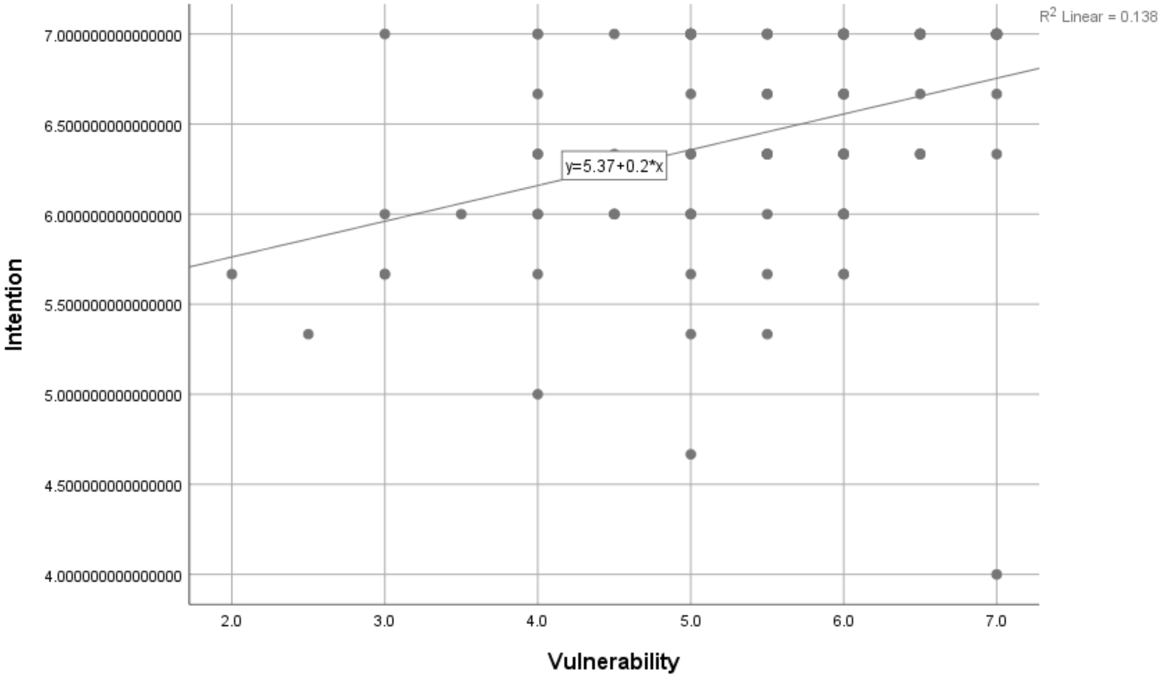


Figure 10. Scatterplot of the Values for *Vulnerability* and *Intention*

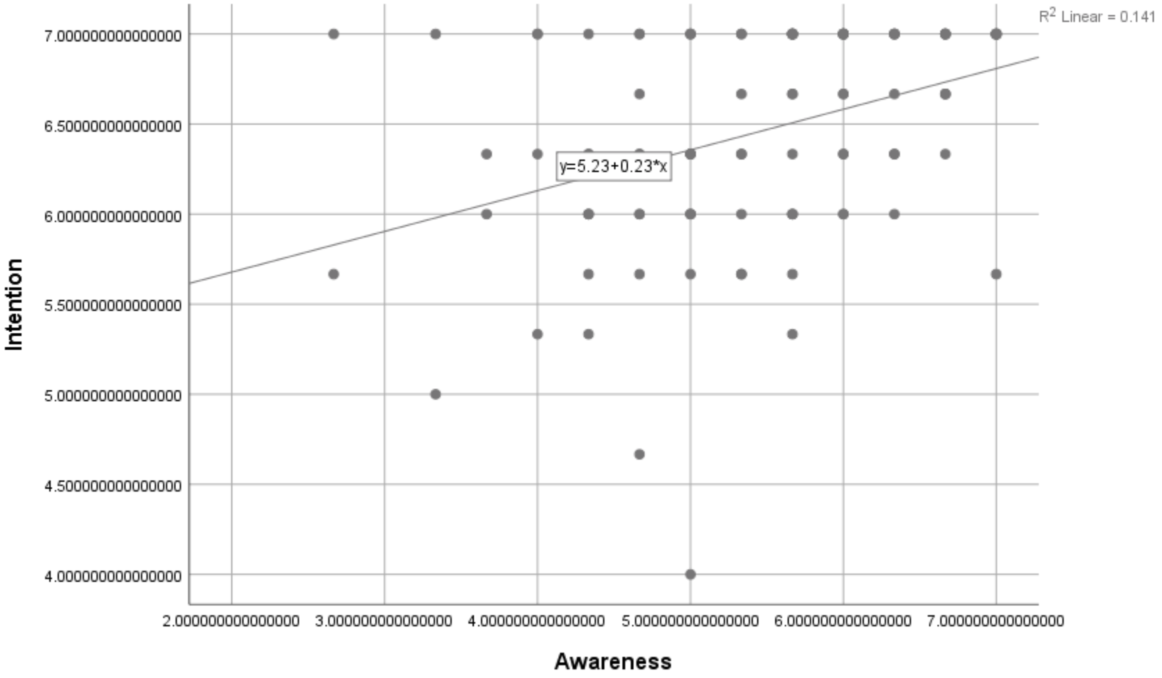


Figure 11. Scatterplot of the Values for *Awareness* and *Intention*

Cook's distance is a measurement of outlier data that may influence the slope of the analysis (Fox, 1991). The Cook's distance for the data set had a minimum value of .00 and the maximum value of .61, indicating a difference of .61, which is below the commonly accepted threshold of 1.0, indicating that outliers should not affect the analysis. I examined the individual data point with the Cook's distance of .61 and determined that the data point is a valid sample that does not contain an unlikely set of answers such as all ones or all sevens. Since the data point appeared to be valid, and the Cook's distance was less than 1, the data point was left in the data set used for the analysis.

Multicollinearity, which is a correlation between the independent variables, can increase the standard errors of the coefficients and reduce the accuracy of the analysis (Allison, 1999). Table 3 contains the Pearson values for the relationships between the independent variables, and all of them are significant. The correlation between *vulnerability* and *severity* is strong at 0.64.

Table 3

Pearson Correlations

	Severity	Vulnerability	Awareness
Severity		.64	.49
Vulnerability	.64		.40
Awareness	.49	.40	

N = 100

While Table 3 indicates there is some multicollinearity, it should not have affected the analysis. Variance inflation factors provide information to determine if there is a level of multicollinearity that will affect the analysis (Williams et al., 2013). The variance inflation factor for *severity* was 1.90, for *vulnerability* was 1.72, and for *awareness* was 1.34. Each of the variance inflation factors were below the threshold of 3.3 that would indicate the level of multicollinearity is negatively affecting the robustness of the analysis (Petter et al., 2007).

The last data prescreening step was assuring that the error terms in the full model are not correlated and are independent (Durbin & Watson, 1950). The Durbin-Watson test will indicate if there is some level of correlation of the error terms (Chan, 2004; Garson, 2012) that could have caused the analysis to be inefficient (Williams et al., 2013). The Durbin-Watson value for the full data set was 2.02, which is in the acceptable range between 1.5 and 2.5, indicating there was no significant correlation between the error terms (Garson, 2012). The Durbin Watson test values for the data in the models used for RQ1, RQ2, and RQ3 ranged from 1.91 to 2.15. The Durbin Watson values for the data in the partial models used for RQ4 four ranged from 1.94 to 2.04. All of the values were in the acceptable range (Garson, 2012).

Data Analysis

I conducted the analysis with IBM SPSS 25 and used multiple regression to analyze the strength of the relationships between independent variables and the dependent variable. Table 4 shows the values of the means, standard deviation, median, and range of the variables. One can discern that the data tends toward the high end of the

Likert scale and that the range indicates that no participant selected *strongly disagree* as the answer to any of the questions in the survey.

Table 4

Means, Standard Deviations, Median, and Range of Indexed Data

	Mean	Standard Deviation	Median	Range
Severity	5.40	1.19	5.67	5.33, 1.67 – 7.00
Vulnerability	5.50	1.14	6.00	5.00, 2.00 – 7.00
Awareness	5.44	1.00	5.67	4.33, 2.67 – 7.00
Intention	6.46	0.60	6.67	3.00, 4.00 – 7.00

N = 100

The answers to RQ1, RQ2, and RQ3 were determined by running a regression for each independent variable and the dependent variable. SPSS 25 was used to perform individual F-tests to determine if the relationship between each independent variable and the dependent variable was significant. Table 5 shows the linear regression summary from the three analyses.

Alternative hypothesis one was that there is a relationship between the independent variable *severity,* which represented the harshness of the punishment for not complying with ISP, and the dependent variable *intention,* which represented the participant’s intention to comply with ISP. The Pearson r for the relationship between *severity* and *intention* was .51, indicating a moderately positive relationship, and the R^2 is .26, indicating that *severity* explains 26% of the variance in the dependent variable *intention* about its mean. The results of the F-test indicated the relationship was significant, F(1, 98) = 34.69, p < .001. The null hypothesis for RQ1 was rejected in favor of the alternative hypothesis that *severity* explains a significant amount of the variation in *intention*. The answer to RQ1 was that there is a significant, albeit moderate, relationship between *severity* and *intention.*

Table 5

Summary of Three Simple Linear Regressions

	R	R2	Std. Error	β	F	df1	df2	Sig
Severity	.51	.26	.53	.51	34.69	1	98	.000
Vulnerability	.37	.14	.57	.37	15.73	1	98	.000
Awareness	.38	.14	.57	.38	16.03	1	98	.000

Dependent Variable: Intention

Alternative hypothesis two was that there is a relationship between *vulnerability,* which represents the likeliness that a person will be caught not complying with ISP and *intention.* The Pearson r for the relationship between *vulnerability* and *intention* was moderately positive, with a value of .37. The R^2 value was.14, indicating that 14% of the variance of the dependent variable about its mean is explained by the independent variable *vulnerability*. The F-test results were significant, F(1, 98) = 15.73, p < .001. The null hypothesis for RQ2 was rejected in favor of the alternative hypothesis that *vulnerability* explains a significant amount of the variation in *intention*. The answer to RQ2 was that there is a significant, albeit small, relationship between *vulnerability* and *intention.*

Alternative hypothesis three was that there is a relationship between *awareness,* which represents the knowledge that one's behavior affects others, and *intention.* The value of the Pearson r for *awareness* and *intention* was .38, which is moderately positive.

The R^2 for *awareness* was .14. The F-test indicated the relationship between *awareness* and *intention* is significant, F(1, 98) = 16.03, p < .001. The null hypothesis for RQ3 was rejected in favor of the alternative hypothesis that *awareness* explains a significant amount of the variation in *intention*. The answer to RQ3 was that there is a significant, albeit small, relationship between *awareness* and *intention.*

Alternative hypothesis four was that there is a relationship between the three independent variables collectively and the dependent variable. I ran a multiple regression analysis of the full research model with three the independent variables and the dependent variable to test the hypothesis. The R^2 for the model was .28. The results of the F-test were significant, F(3, 96) = 12.67, p < .001.

While the F-test of the full model indicated a significant relationship between the independent variables taken collectively and the dependent variable, the results of the t-tests shown in Table 6 indicated that *severity* was the only variable in the full model that had a significant relationship with the dependent variable *intention.*

Table 6

Regression Coefficients for Full Model

	B	Std. Error	β	t	Sig
Constant	4.68	.37		14.27	.000
Severity	.20	.06	.40	3.37	.001
Vulnerability	.03	.06	.05	0.46	.647
Awareness	.10	.06	.16	1.59	.116

Dependent Variable: Intention

The null hypothesis that there was no relationship between the independent variables, taken collectively, and intention was rejected in favor of the alternative hypothesis that there was a relationship between at least one of the independent variables and the dependent variable.

Figure 12 depicts the research model and shows a solid line for the significant but moderate relationship between *severity* and *intention,* a dashed line for the significant but small relationship between *awareness* and *intention,* and a dotted line for the significant but small relationship between *vulnerability* and *intention* based on the findings of the three simple linear regression analyses.

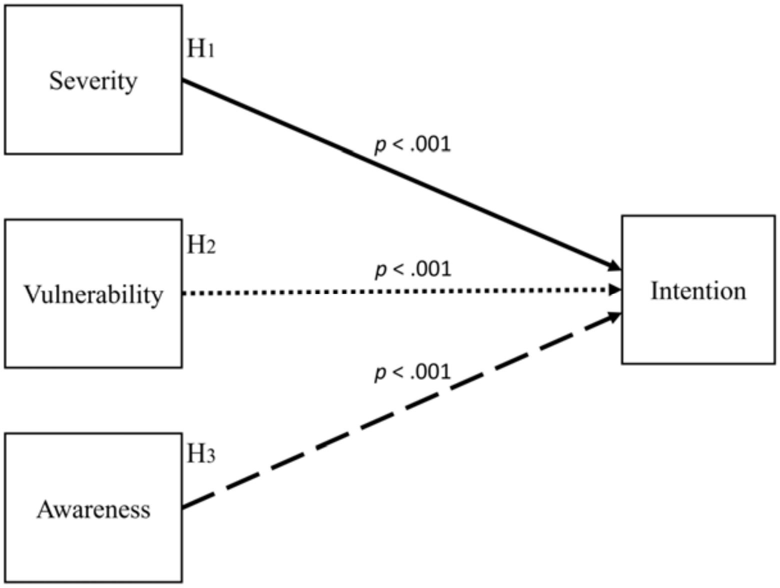


Figure 12. Research Model Depicting the Significance of the Relationships

Summary

The results of the study indicated that there was a significant relationship between each of the independent variables and the dependent variable. The full model used to answer RQ4 had the highest R^2 value of .28 and was the best model for predicting the dependent variable *intention*. The null hypothesis was rejected for hypotheses one, two, and three in favor of the respective alternative hypothesis. The answer to RQ1, RQ2, and RQ3 was that there is a significant relationship between *severity* and *intention,* a significant relationship between *vulnerability* and *intention,* and a significant relationship between *awareness* and *intention,* with *severity* having the strongest relationship with the dependent variable *intention* as measured by R^2*,* and *awareness* and *vulnerability* a less strong relationship with the dependent variable *intention.* The answer to RQ4 was that, taken collectively, there was a significant relationship between one or more of the independent variables and the dependent variable.

This chapter contained the research questions and hypotheses, an explanation of the data collection processes, and any differences between what the procedures stated in the proposal and the procedures I conducted. The chapter also contained explanations of how data were prescreened and how they were prepared for analysis. The chapter concluded with an interpretation of the data.

Chapter 5 contains the interpretation of the analysis of the study. I discuss the limitations of the study and recommendations for further research. The chapter concluded with the implications and conclusions of this research.

Chapter 5: Discussion, Conclusions, and Recommendation

The purpose of this study was to improve understanding of the relationships between the variables *severity*, *vulnerability*, and *intention to comply* with ISP, and the relationship between *awareness of the consequences of data breaches* and the *intention to comply* with ISP. The independent variables were *severity, vulnerability,* and *awareness,* and the dependent variable was *intention.* Multiple regression revealed the strengths of the relationships between these variables. Measuring and ranking the relationships between these variables could enable information security officers to develop more effective training programs and policies that reduce the incidence and damage of data breaches.

The results of this study indicated significant relationships between each of the independent variables and the dependent variable *intention* with *severity* having the strongest relationship, *awareness* having the next strongest relationship, and *vulnerability* having the least strong relationship with the dependent variable. The first three null hypotheses were rejected in favor of the alternative hypotheses that each of the three independent variables would have a significant relationship with the dependent variable. The null hypothesis for RQ4 was rejected in favor of the alternative hypothesis that there is a relationship between at least one of the independent variables and the dependent variable. This study reduced a gap in the literature where researchers have found inconsistent results when observing the relationships between sanction constructs and compliance.

In this chapter, I present interpretations of the findings as they relate to previous work, explain how the findings relate to the theoretical framework, and discuss the limitations of the study. This chapter also contains recommendations, implications for practice, and a conclusion.

Interpretation of Findings

In this study, I surveyed 100 participants living in the United States who worked in an institution of higher education. The survey measured the participants' perceptions of *sanction severity* and *sanction vulnerability* for not complying with ISP, *awareness of the consequences of a data breach*, and the *intention to comply* with ISP. *Severity* had the strongest relationship with *intention,* followed by *awareness,* and then *vulnerability.*

Comparisons to Studies with the Same Instrument Variables

I measured the variables *severity, vulnerability,* and *intention* with an instrument developed by Herath and Rao (2009) and measured the variable *awareness* using an instrument developed by Yazdanmehr and Wang (2016). The results of the study conducted for this dissertation contradict the work done by Herath and Rao where the researchers hypothesized that there would be a significant positive relationship between sanction severity and intention to comply. However, they found a significant negative relationship between punishment severity and security policy compliance intention and a stronger significant positive relationship between detection certainty and security policy compliance intention. Herath and Rao also found significant positive relationships between security policy compliance intention and subjective norms, description norms, organizational commitment, and self-efficacy.

Yazdanmehr and Wang (2016) found a significant relationship between ISP-related awareness of consequences and ISP-related personal norms, and a significant relationship between ISP-related personal norms and ISP compliance behavior. The researchers did not measure the relationship between ISP-related awareness of the consequences and ISP compliance behavior but did test to determine if ISP-related awareness of consequences moderated the relationship between ISP-related personal norms and ISP compliance behavior. They found no significant moderating relationship. Consequently, this study neither confirmed nor contradicted the findings of Yazdanmehr and Wang, but did support the finding that this form of awareness affects the intention to comply with ISP.

Comparisons to Studies Measuring Severity and Vulnerability

The results of this study indicated significant relationships between both independent variables *severity* and *vulnerability* and the dependent variable *intention.* This supported work done by Chen et al. (2012), who found significant relationships between the independent variables sanction severity, sanction certainty, and rewards for compliance, and the independent variable intention. The researchers also found that sanction certainty positively moderated the relationships between sanction severity and intention, and reward for compliance and intention, indicating that individuals consider punishment and reward more seriously when the risk of detection is high (Chen et al., 2012).

In contrast, the results of this study contradicted work done by D’Arcy et al. (2014), who measured sanctions in terms of certainty and severity. They found no direct relationship between perceived sanctions and intention to comply with ISP but did find a relationship between perceived sanctions and moral disengagement. The researchers argued that sanctions increased moral disengagement, which in turn increased cognitive rationalizations that lead to volitional but non-malicious ISP violations (D’Arcy et al., 2014). The authors suggested that SETA programs should emphasize avoiding cognitive rationalizations provided by NT.

The results of several studies conducted in 2016 supported a relationship between GDT severity and intent, but not vulnerability and intent. In a study with Canadian IT professionals, Ifinedo (2016) found a strong relationship between severity and intent. The researcher also found relationships between management support and intent, and cost benefit analysis and intent, but found no connection between vulnerability and intent. Ifinedo suggested that when individuals use neutralization techniques to justify violating ISP, they become less concerned with vulnerability. Yang and Lee (2016) found similar results with a sample of information security users in a university hospital in South Korea. The researchers found an inverse relationship between severity and the intent to illegally use health information systems but found no relationship between vulnerability and illegal intent. Cheng et al. (2013) used a scenario-based survey with employees in

China to measure relationships between sanction variables, social bonds variables, social pressure variables, and the dependent variable IS security policy violation intention. They found a negative relationship between severity and violation intention, but no relationship between vulnerability and violation intention.

The results of some of the studies reviewed in Chapter 2 supported a relationship between GDT vulnerability and intent, but not severity and intent. Foth (2016) measured relationships between the independent variables attitude, subjective norms, perceived behavioral control, severity, and certainty, and the dependent variable intention to comply with data protection regulations and found significant relationships between all of the independent variables and the dependent variable except for severity. Cheng et al. (2014) measured relationships between neutralization techniques and the dependent variable intention to use the internet for personal reasons at work. They measured the relationships between sanction severity, detection certainty, and perceived benefits and the dependent variables.

The researchers found support for all hypotheses except the relationship between sanction severity and use the internet for personal reasons at work. Li et al. (2014) found significant relationships between sanction certainty and the intention to comply with internet use policy, but no support for a relationship with sanction severity in a study with American employees. In an interesting contrast, Hovav and D’Arcy (2012) found a relationship between severity and intention in the United States, but found no such relationship in Korea, and conversely, found a relationship between vulnerability and intention in Korea, but did not find the same relationship in the United States.

Comparisons to Studies Measuring Awareness

Researchers have defined awareness in different ways in different studies. Han et al. (2017) operationalized awareness as knowing the policy and the actions an organization will take to enforce compliance. Han et al. conducted a survey with employees and managers in manufacturing, education, financial services and banking industries to test hypotheses based on rational choice theory and psychological contract theory. The researchers measured the relationships between independent variables such as perceived cost, perceived benefits, and psychological contract fulfillment, and the dependent variable intention to comply. Han et al. also measured the relationships between the independent variable ISP awareness, and the dependent variables perceived cost and perceived benefits. They found that ISP awareness had a significant relationship with perceived benefits for both managers and employees, but found the relationship between ISP awareness and perceived costs to be significant for managers, but not employees.

Like Han et al. (2017), Al-Mukahal and Alshare (2015) defined awareness as knowledge of ISP. The researchers' model indicated significant relationships between the intrinsic, independent variables awareness of ISP and trust, the extrinsic independent variables clarity of policy and effects on work environment, and the dependent variable number of ISP violations. Unlike the work done by Moquin and Wakefield (2016) and

Han et al., awareness of ISP was the only variable without a significant relationship with the dependent variable.

Moquin and Wakefield (2016) defined awareness as knowledge of how to be compliant with software license agreements and the costs, risks, and consequences of not complying with agreements, which is similar to Han et al. (2017) and Al-Mukahal and Alshare (2015). Moquin and Wakefield found significant relationships between the independent variable awareness and the mediating variables legal sanctions, organizational sanctions, and software ethics. These all had a significant relationship with the moderating variable compliance attitude, which had a significant relationship with the dependent variable compliance behavior (Moquin & Wakefield, 2016).

Bélanger et al. (2017) added a temporal element to awareness by specifying that a user must be aware that policy has changed and of what they must do to comply with the new policy. The study was distinctive because it involved direct observation with an experiment where the researchers sent a message to participants in a university telling them to change their password, and then used a computer system to determine if and when the participants changed the passwords (Bélanger et al., 2017). The results supported relationships between organizational triggers and ISP awareness, and between the independent variables ISP awareness, threat severity, and vulnerability, and the dependent variable attitude (Bélanger et al., 2017).

The previously mentioned studies have measured awareness primarily as knowledge of ISP. Other researchers have begun to expand the definition of awareness from knowing how to comply with ISP to knowing why to comply with ISP by incorporating understanding risk into the definition. Bauer and Bernroider (2017) defined information security awareness as an employee’s ability to recognize information security threats and the risk they pose to the organization. Bauer and Bernroider found that information security awareness positively correlated with attitude and social norms, and negatively correlated with neutralization techniques. The researchers further found that neutralization techniques negatively correlated with intention for compliant information security behavior.

Yang and Lee (2016) defined awareness as knowing the policy, which includes understanding roles and responsibilities, knowing there are sanctions for not complying with ISP, and recognizing the consequences of security threats. The addition of recognition of consequences to the definition of awareness was novel. Yang and Lee hypothesized that there would be correlations between security awareness and threat severity, threat vulnerability, response efficacy, and self-efficacy. The results of a survey conducted with employees in a South Korean hospital did not support a relationship between security awareness and vulnerability but did support the relationships between security awareness and threat severity, response efficacy, and self-efficacy. Yang and Lee defined awareness in a way more similar to the work of Yazdanmehr and Wang (2016) by including the concept of consequences from security threats. I utilized Yazdanmehr and Wang’s definition of awareness in this study but could not confirm the results of their work because I measured different relationships.

Theoretical Framework

GDT and NT were the behavioral theories that supported this study. GDT supported the constructs *severity* and *vulnerability,* and NT explained how *awareness* of the consequences relates to *intention* to comply with ISP. The significant relationships between *severity* and *vulnerability,* and *intention,* suggested that GDT is an effective behavioral theory for informing policy enforcement. The support for *awareness* in the context of being aware of the damage caused by data breaches indicated that a form of awareness beyond knowing how to comply with ISP may diminish the use of neutralization techniques and reduce non-compliance with ISP.

General Deterrence Theory

The use of GDT in policy enforcement may be effective, but it is difficult to support this idea with research literature. The results of the studies reviewed in this dissertation that measured the constructs *severity* and *vulnerability* from GDT against the dependent variable *intention* or a similar variable were nearly evenly dispersed, with one early study having support for both sanction variables, three studies supporting *severity* but not *vulnerability,* three studies providing support for *vulnerability* but not *severity,* and one study resulting in no support for the sanction variables. Adding the results of this study to the list would further balance the disparate results by bringing the total number of studies finding support for both variables to two.

It is interesting to note the relative strengths of the relationships found in this study. The simple linear regressions revealed that severity explains 26% of the variance of the dependent variable intention about its mean, while both awareness and vulnerability explain 14% of the variance in the dependent variable about its mean.

Some researchers such as Cheng et al. (2013), Ifinedo (2016), Yang and Lee (2016), and in United States, Hovav and D'Arcy (2012), have found vulnerability to have little or no influence on intention and the results in this study are the same. The reason may be that while people fear the severity of the punishment for violating ISP, they think the chances the organization will catch them are low. In contrast, some researchers such as Cheng et al. (2014), Foth (2016), Li et al. (2014), and in Korea, Hovav and D'Arcy, have found support for the relationship between vulnerability and intention, but not severity and intention. The support for vulnerability may have been due to environments or cultures with strong bonds among employees with high organizational commitment, who fear humiliation and public identification as a violator of ISP more than they fear the punishment for violating ISP. Johnston et al. (2015) found a significant relationship between informal severity and intent, and informal vulnerability and intent, but did not find the same relationships between formal severity, formal vulnerability, and intent implying that they perceive peers noticing a violation as more severe than the organization noticing a violation.

Neutralization Theory

I used *awareness* in this study as a counterpart to deterrence and measured the relationships between sanction factors and *intention,* and *awareness* and *intention* and compared the strengths of the relationships to determine which terms had the most influence on *intention.* The results indicated that *severity* had the strongest relationship with *intention,* and *awareness* and *vulnerability* had the next strongest relationship. *Awareness,* in the context of knowledge of the damage done by data breaches, has a role to play in ISP enforcement because of how it nullifies the use of neutralization techniques to justify ISP violation.

Barlow et al. (2013) found that employees use neutralization techniques such as defense of necessity and denial of injury to justify ISP violations and that SETA programs decrease policy violations. Barlow et al. and Siponen and Vance (2010) both found that neutralization techniques were more strongly correlated with ISP violations than sanctions. Yazdanmehr and Wang (2015) found that when an individual perceives that the cost of compliance exceeds the benefit, they will use neutralization techniques such as denial of injury to nullify moral obligation. The use of neutralization techniques is common and has a strong negative effect on ISP compliance.

Al-Mukahal and Alshare (2015) suggested that awareness and education programs should teach how employees use neutralization to justify volitional non-malicious ISP violation and how to avoid such rationalization. Bauer and Bernroider (2017) suggested that increasing employee awareness would decrease the use of neutralization techniques and increase other positive predictors of compliance. Teh et al. (2015) found that individuals in high power distance cultures that typically respond well to authoritarian leadership use neutralization techniques and that SETA programs should include training on how to avoid using neutralization techniques. Willison et al. (2018)

suggested that organizations use transparent communications designed to deter the use of neutralization techniques to justify ISP non-compliance. Various forms of awareness including knowledge of how to comply, and just as importantly, why one must comply, can be effective tools in decreasing neutralization techniques used to justify ISP violations.

Limitations of the Study

As referenced in Chapter 1, the nature of the data collection and analysis limited this study. Common method variance can affect survey data collected about behaviors (Warkentin et al., 2016) and may contain false responses about the participant's compliance (Lebek et al., 2014). An anonymous survey may mitigate common method variance by encouraging participants to provide truthful answers (Fox et al., 2003). Data collected with a Likert scale can reduce the robustness of the analysis because the perceived distance between each point on the scale is not necessarily the same (Warner, 2013).

The participants for the study were all employees in the United States who worked in higher education institutions and who responded to a single request to complete a survey at a single point time. Consequently, it is not possible to generalize the results to the overall population of the United States and are not representative of non-western cultures. The demographics of the sample population limited the external validity of the study to those similar to the sample population. Additionally, the study measured the *intention* to comply and not behavior. Studies in which researchers directly observe participants are rare (Bélanger et al., 2017) because organizations are reluctant to release information about violations of security policies (Lebek et al., 2014) and because designs that include observation are difficult (Bélanger et al., 2017; Lebek et al., 2014). Measuring *intention* instead of behavior limits the generalizability of the findings.

This design of this study and interpretation of the findings rested on an assumption of causality. While some forms of statistical analysis can determine the direction of influence between variables, multiple regression can only detect correlation and cannot assess causality. While this may have limited the internal validity of the study, it is reasonable to assume that an individual's *intention* to comply with policy would not have a causal effect on the level of sanctions used by an institution to enforce compliance with the policy and would not affect the individual's *awareness* of the damages caused by a data breach. Consequently, it is reasonable to assume that sanctions and *awareness* have a causal relationship with the *intention* to comply.

Recommendations

Future research should examine sanctions with other attributes of individuals such as organizational commitment. Teh et al. (2015) found that the use of neutralization correlated with the volitional but non-malicious intention to violate ISP and that employees with low organizational commitment were more likely to use neutralization than employees with high organizational commitment. Researchers should examine organizational commitment as a moderating variable affecting the relationship between constructs from GDT and the *intention* to comply with ISP.

Many researchers that have measured the construct awareness have defined it as knowledge of ISP (Tsohou, Karyda, & Kokolakis et al. 2015) or knowledge of behaviors and best practices (Safa et al., 2015, 2016). The construct *awareness* in this study came from work done in the last five years by Yazdanmehr and Wang (2016), who defined the construct as being aware of how one's conduct affects others. In a similar study, Yang and Lee (2016) defined awareness as the knowledge that a data breach would do damage to information systems. In another similar study, Dang-Pham and Pittayachawan (2015) defined awareness as understanding how data breaches and other violations threaten organizational assets. Researchers should expand the definition of awareness beyond the knowledge of policy and how to comply to include awareness of the consequences of a data breach and awareness that one's behavior affects others. Operationalizing awareness in ways similar to Yazdanmehr and Wang, Yang and Lee, and Dang-Pham and Pittayachawan in future studies could enable researchers and practitioners to gain more understanding of how a more holistic view of awareness affects the *intention* to comply with ISP.

Various studies have found conflicting results for severity and vulnerability of sanctions. Some researchers have suggested that vulnerability may have more effect in some organizations because of strong team bonds and work done by Cheng et al. (2013) and Johnston et al. (2015) found that informal sanctions have more impact than formal sanctions. Researchers should examine the effects of formal and informal sanctions, and vulnerability in different cultures to determine if there are environmental factors that moderate the effect of vulnerability.

All three factors of GDT, *severity*, *vulnerability*, and celerity must have significance for deterrence to be effective (Beccaria, 1963). Why should a person fear a punishment they do not believe they will receive because *vulnerability* is very low or because celerity is very high? Perhaps humans do not respond to changes in the GDT variables linearly. A person may react to a continuum of sanctions from benign to severe in an exponential way by having little to no reaction to low-level sanctions such as emails with admonishing language, a lecture from a supervisor, or even the implied threat of termination, but have very high reactions to sanctions that go much beyond this such as demotions, pay cuts, termination, or incarceration.

Human may perceive *vulnerability* in a similar way where there is no response until the variable reaches some threshold. Additionally, *vulnerability* may be moderating the relationship between *severity* and *intention.* Chen et al. (2018) noted that the different results for GDT studies might be due to missing moderating variables and inconsistent analysis procedures for measuring moderating variables. The possible moderating relationship between *vulnerability* and *severity* might be a sigmoid curve where *severity* does not influence *intention* until *vulnerability* reaches a mid-value. *Severity's* influence on *intention* may increase until *vulnerability* reaches a certain point where increases in *vulnerability* cease have an impact on *severity*. Researchers could conduct experiments where several groups of participants receive SETA threat appeals that all have the same levels of *severity,* but that have different levels of *vulnerability* to determine if there is are thresholds for *vulnerability* below and above which *severity* has no effect.

Researchers have found PMT to be an excellent model for predicting how individuals make decisions about complying with ISP (Crossler & Bélanger, 2014; Posey et al., 2015; Torten et al., 2018; Yang & Lee, 2016). I suggest that an organization communicate ISP and the associated GDT factors to a person with a threat appeal via SETA. The person cognitively processes the information in the threat appeal using protection motivation theory, and if the person chooses not to comply, they will use neutralization techniques to justify the response. Researchers should examine how individuals make decisions using protection motivation theory and NT, and how creating SETA programs that address neutralization could be more effective than programs that only rely on GDT.

Implications

Data breaches can cause financial and reputation damage to organizations (Clapper & Richmond, 2016) because unauthorized individuals use illegally obtained data to commit crimes (Teh et al., 2015). Compromised medicals can cause serious harm to individuals by exposing social security numbers and medical diagnoses such as mental illness (Li & Slee, 2014). Reducing the number of data breaches will reduce the incidence of bankruptcies and identify theft. The findings from this study may help information security officers create effective policies and education programs that prevent data breaches because it contributes to reducing a gap in the literature by confirming previous work where researchers found relationships between sanction variables and the *intention* to comply with ISP, and between *awareness* and *intention.*

The relationships between *severity* and *intention,* and *vulnerability* and *intention* indicated that the threat of sanctions is an effective enforcement tool. The cognitive processes that occur when an organization threatens an individual with sanctions for not complying with policy may be different from the cognitive processes that occur when a government threatens an individual with sanctions for committing a crime, but there is no conclusive evidence that using sanctions to enforce policy is not effective. Practitioners should continue to include punitive actions in programs for enforcing compliance with ISP. However, practitioners could make enforcement programs more effective by including training that emphasizes multiple forms of awareness.

The significant relationship between *awareness* operationalized as knowledge that data breaches cause damage and *intention* indicated that individuals are aware of the potential damage from data breaches and understand that complying with ISP can mitigate the risk of a data breach occurring. Information security professionals should improve SETA programs by emphasizing awareness of the consequences of a data breach and how non-malicious volitional violations lead to adverse outcomes for the organization and individuals associated with the organization. Training programs should focus on training people to understand how data breaches affect the organization, how they affect employees, and how they affect customers.

Barlow et al. (2013) found that the use of neutralization techniques outweighed the threat of sanctions when individuals considered violating ISP for non-malicious reasons such as doing work efficiently. There is evidence that individuals use neutralization techniques to justify non-compliance with ISP and that one of the techniques that people use is the metaphor of the ledger (Teh et al., 2015). The relationship between *awareness* and *intention* indicated that individuals consider the potential damage done by a data breach when considering ISP compliance. Directly addressing neutralization and attempting to adjust the values on an individual's personal ledger by increasing the individuals *awareness* of the damage done by data breaches may be a successful strategy for increasing compliance. Additionally, Teh et al. (2015) found that employees with low levels of organizational commitment are more prone to use neutralization techniques than employees with high levels of organizational commitment. Programs designed to increase organizational commitment should decrease the use of neutralization and, in turn, increase compliance with ISP and decrease the risk of a data breach.

Hovav and D'Arcy (2012), Cheng et al. (2014), Li et al. (2014), and Foth (2016) all found support for the relationship between vulnerability and some form of intention to follow policy, but no relationship between severity and intention. These findings are interesting because they challenge the idea that severity and vulnerability must both exist for sanctions to have an impact. Herath and Rao (2009) found a positive relationship between detection certainty and intention to comply, and this led the researchers to conclude that individuals perceive peers knowing they violated ISP more severely than they perceive the associated punishment. This finding may be because humans perceive and react to social rejection in the same way they perceive and react to pain (Eisenberger, 2003). Information security officers may be able to enhance enforcement strategies by deploying mechanisms that publicly identify ISP violators.

Conclusions

Over 50% of data breaches are caused by employees and other internal actors violating ISP (D'Arcy & Greene, 2014), who are often acting with volition but in a non-malicious way (Teh et al., 2015) and these data breaches cause harm to organizations (Clapper & Richmond, 2016) and individuals (Li & Slee, 2014). The results of this study indicated that sanctions are a useful tool for enforcing ISP, but there is still little consensus in the literature. Researchers have linked ISP awareness to ISP compliance (Chen et al., 2012) and awareness of the consequences of a data breach to ISP compliance (Yang & Lee, 2016), but researchers have done little work with a holistic view of awareness that includes knowledge of consequences.

As our daily lives become more intertwined with electronic systems such as social media, online banking, and online shopping, and as more of the overall population of the world gains access to these systems, the potential damage from data breaches increases. Data security can no longer be a function that a department in an organization performs and instead must become part of our societal hygiene. Safe practices in the workplace, at home, and in every aspect of life will become more important, and communicating and enforcing these practices must become a part of our culture. Effective policies and policy enforcement will serve as a vehicle to transition society from the current state of risk to one where good security practices are implicit.

References

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. *Action Control*, 11–39. https://doi.org/10.1007/978-3-642-69746-3_2

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Al-diabat, M. (2018). Investigating the determinants of college students information security behavior using a validated multiple regression models. *International Journal of Computer Science & Information Technology*, *10*(6), 81–96. https://doi.org/10.5121/ijcsit.2018.10608

Al-Mukahal, H. M., & Alshare, K. (2015). An examination of factors that influence the number of information security policy violations in Qatari organizations. *Information and Computer Security*, *23*(1), 102–118. https://doi.org/10.1108/ICS-03-2014-0018

Allison, P. D. (1999). *Multiple regression: A primer.* Thousand Oaks, CA: Sage.

Alshare, K. A., Lane, P. L., & Lane, M. R. (2018). Information security policy compliance: a higher education case study. *Information and Computer Security*, *26*(1), 91–108. https://doi.org/10.1108/ICS-09-2016-0073

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312. https://doi.org/10.1016/j.chb.2014.05.046

Aurigemma, S., & Mattson, T. (2017). Deterrence and punishment experience impacts on ISP compliance attitudes. *Information and Computer Security*, *25*(4), 421–436. https://doi.org/10.1108/ICS-11-2016-0089

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. (2018). Don’t even think about it! The effects of anti-neutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems*, *19*(8), 689–715. https://doi.org/10.17705/1jais.00506

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don’t make excuses! Discouraging neutralization to reduce IT policy violation. *Computers and Security*, *39*(B), 145–159. https://doi.org/10.1016/j.cose.2013.05.006

Bauer, S., & Bernroider, E. W. N. (2017). From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database: The Database for Advances in Information Systems*, *48*(3), 44–68. https://doi.org/10.1145/3130515.3130519

Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users’ non-compliance with information security policies in banks. *Computers & Security*, *68*, 145–159. https://doi.org/10.1016/j.cose.2017.04.009

Beccaria, C. (1963). *On crime and punishments*. New York, NY: MacMillan.

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management*, *54*(7), 887–901. https://doi.org/10.1016/J.IM.2017.01.003

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Bulgurcu, Cavusoglu, & Benbasat. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523. https://doi.org/10.2307/25750690

Bulmer, M. G. (1979). *Principles of statistics*. Mineola, NY: Dover Publications.

Burkholder, G. J., Cox, K. A., & Crawford, L. M. (2016). *The scholar-practitioner's guide to research design*. Baltimore, MD: Laureate Publishing.

Chan, Y. (2004). Biostatistic 201: Linear regression analysis. *Singapore Medical Journal*, *45*(2), 55–61. Retrieved from http://www.smj.org.sg/

Chen, X., Wu, D., Chen, L., & Teng, J. K. L. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management*, *55*(8), 1049–1060. https://doi.org/10.1016/J.IM.2018.05.011

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information*

Systems, *29*(3), 157–188. https://doi.org/10.2753/MIS0742-1222290305

Cheng, L., Li, W., Zhai, Q., & Smyth, R. (2014). Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. *Computers in Human Behavior*, *38*, 220–228. https://doi.org/10.1016/j.chb.2014.05.043

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*(Part B), 447–459. https://doi.org/10.1016/j.cose.2013.09.009

Choi, M., & Song, J. (2018). Social control through deterrence on the compliance with information security policy. *Soft Computing*, *22*(20), 6765–6772. https://doi.org/10.1007/s00500-018-3354-z

Chu, A. M. Y., & Chau, P. Y. K. (2014). Development and validation of instruments of information security deviant behavior. *Decision Support Systems*, *66*, 93–101. https://doi.org/10.1016/J.DSS.2014.06.008

Clapper, D., & Richmond, W. (2016). Small business compliance with PCI DSS. *Journal of Management Information and Decision Sciences*, *19*(1), 54–67. Retrieved from http://www.abacademies.org/journals/journal-of-management-information-and-decision-sciences-home.html

Coe, R. (2002). It’s the effect size, stupid: What effect size is and why it is important. In *Annual Conference of the British Educational Research Association*. Education-line.

Retrieved from https://www.leeds.ac.uk

Cohen, J. (1992). A power primer. *Psychological Bulletin*, *112*(1), 155–159. https://doi.org/10.1037/0033-2909.112.1.155

Coleman, J. W. (1987). Toward an integrated theory of white-collar crime. *American Journal of Sociology*, *93*(2), 406–439. https://doi.org/10.1086/228750

Connolly, L. Y., Lang, M., Gathegi, J., & Tygar, D. J. (2017). Organisational culture, procedural countermeasures, and employee security behaviour. *Information and Computer Security*, *25*(2), 118–136. https://doi.org/10.1108/ICS-03-2017-0013

Cronbach, L. J., & Meehl, P. E. (1955). Construct validity in psychological tests. *Psychological Bulletin*, *52*(4), 281–302. https://doi.org/10.1037/h0040957

Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviors. *ACM SIGMIS Database*, *45*(4), 51–71. https://doi.org/10.1145/2691517.2691521

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. https://doi.org/10.1016/j.cose.2012.09.010

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems*, *28*(1), 209–226. https://doi.org/10.2308/isys-50704

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, *22*(5), 474–489. https://doi.org/10.1108/IMCS-08-2013-0057

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. https://doi.org/10.1057/ejis.2011.23

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, *31*(2), 285–318. https://doi.org/10.2753/MIS0742-1222310210

D'Arcy, J., & Teh, P.-L. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management*. https://doi.org/10.1016/J.IM.2019.02.006

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach. *Computers & Security*, *48*, 281–297. https://doi.org/10.1016/J.COSE.2014.11.002

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319. https://doi.org/10.2307/249008

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations, 293–314. https://doi.org/10.1111/j.1365-

2575.2006.00219.x

Durbin, J., & Watson, G. S. (1950). Testing for serial correlation in least squares regression: I. *Biometrika*, *37*(3/4), 409. https://doi.org/10.2307/2332391

Eisenberger, N. I. (2003). Does rejection hurt? An fMRI study of social exclusion. *Science*, *302*(5643), 290–292. https://doi.org/10.1126/science.1089134

Foth, M. (2016). Factors influencing the intention to comply with data protection regulations in hospitals: Based on gender differences in behaviour and deterrence. *European Journal of Information Systems*, *25*(2), 91–109. https://doi.org/10.1057/ejis.2015.9

Fox, J. (1991). *Regression diagnostics*. Thousand Oaks, CA: Sage.

Fox, Murray, C., & Warm, A. (2003). Conducting research using web-based questionnaires: Practical, methodological, and ethical considerations. *International Journal of Social Research Methodology*, *6*(2), 167–180. https://doi.org/10.1080/13645570210142883

Garson, G. D. (2012). *Testing statistical assumptions* (2012th ed.). Asheboro, NC: Statistical Associates Publishing. Retrieved from https://www.researchgate.net

Goo, J., Yim, M.-S., & Kim, D. J. (2014). A path to successful management of employee security compliance: An empirical study of information security climate. *IEEE Transactions on Professional Communication*, *57*(4), 286–308. https://doi.org/10.1109/TPC.2014.2374011

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. https://doi.org/10.2753/MIS0742-1222280208

Han, J., Kim, Y. Y., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, *66*, 52–65. https://doi.org/10.1016/j.cose.2016.12.016

Hauke, J., & Kossowski, T. (2011). Comparison of values of Pearson's and Spearman's correlation coefficients on the same sets of data. *Quaestiones Geographicae*, *30*(2), 87–93. https://doi.org/10.2478/v10117-011-0021-1

Haynes, S. N., & Richard, D. C. S. (1995). Content validity in psychological assessment: A functional approach to concepts and methods introduction to content validity. *Psychological Assessment*, *7*(3), 238–247. https://doi.org/10.1037/1040-3590.7.3.238

Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals. *Information Management & Computer Security*, *21*(4), 266–287. https://doi.org/10.1108/IMCS-08-2012-0043

Hepler, J. (2015). A good thing isn't always a good thing: Dispositional attitudes predict non-normative judgments. *Personality and Individual Differences*, *75*, 59–63. https://doi.org/10.1016/j.paid.2014.11.016

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the United States. *Journal of Financial Crime*, *22*(2), 242–260. https://doi.org/10.1108/JFC-09-2013-0055

Hovav, A., & D’Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management*, *49*(2), 99–110. https://doi.org/10.1016/J.IM.2011.12.005

Humaidi, N., & Balakrishnan, V. (2015). Leadership styles and information security compliance behavior: The mediator effect of information security awareness. *International Journal of Information and Education Technology*, *5*(4), 311–318. https://doi.org/10.7763/IJIET.2015.V5.522

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*, *41*(1), 2–18. https://doi.org/10.1108/OIR-11-2015-0358

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, *51*(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001

Ifinedo, P. (2016). Critical times for organizations: What should be done to curb workers’ noncompliance with IS security policy guidelines? *Information Systems*

Management, *33*(1), 30–41. https://doi.org/10.1080/10580530.2015.1117868

Johnson, T. P., Fendrich, M., & Mackesy-Amiti, M. E. (2012). An evaluation of the validity of the Crowne–Marlowe need for approval scale. *Qual Quant*, *46*(6), 1883–1896. https://doi.org/10.1007/s11135-011-9563-5

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. https://doi.org/10.1057/ejis.2015.15

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning Rhetoric. *MIS Quarterly*, *39*(1), 113–134. https://doi.org/10.1.1.677.1125

Kajzer, M., D’Arcy, J., Crowell, C. R., & Striegel, A. (2014). An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers & Security*, *43*, 64–76. https://doi.org/10.1016/j.cose.2014.03.003

Kam, H.-J., & Katerattanakul, P. (2014). Information security in higher education: A neo-institutional perspective. In *Journal of Information Privacy and Security* (Vol. 10, pp. 28–43). https://doi.org/10.1080/15536548.2014.912482

Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of information security policy compliance. *The Scientific World Journal*, *2014*, 1–12. https://doi.org/10.1155/2014/463870

Klein, R. H., & Luciano, E. M. (2016). What influences information security behavior? A study with Brazilian users. *Journal of Information Systems and Technology Management*, *13*(3), 479–496. https://doi.org/10.4301/S1807-17752016000300007

Klockars, C. B. (1974). *The professional fence*. New York, NY: Free Press.

Kuo, K.-M., Ma, C.-C., & Alexander, J. W. (2014). How do patients respond to violation of their information privacy? *Health Information Management Journal*, *43*(2), 23–33. https://doi.org/10.1177/183335831404300204

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, *37*(12), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security*, *59*, 60–70. https://doi.org/10.1016/j.cose.2016.02.004

Li, H., Sarathy, R., Zhang, J., & Luo, X. (2014). Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Information Systems Journal*, *24*(6), 479–502. https://doi.org/10.1111/isj.12037

Li, T., & Slee, T. (2014). The effects of information privacy concerns on digitizing personal health records. *Journal of the Association for Information Science and Technology*, *65*(8), 1541–1554. https://doi.org/10.1002/asi.23068

Lowry, P. B., Posey, C., Bennett, R. B. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: an empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal*, *25*(3), 193–273. https://doi.org/10.1111/isj.12063

Ma, C.-C., Kuo, K.-M., & Alexander, J. W. (2016). A survey-based study of factors that motivate nurses to protect the privacy of electronic medical records. BMC Medical Informatics and Decision Making, 16(1), 13. https://doi.org/10.1186/s12911-016-0254-y

Merhi, M. I., & Ahluwalia, P. (2019). Examining the impact of deterrence factors and norms on resistance to Information Systems Security. *Computers in Human Behavior*, *92*, 37–46. https://doi.org/10.1016/J.CHB.2018.10.031

Minor, W. W. (1981). Techniques of neutralization: A reconceptualization and empirical examination. *Journal of Research in Crime and Delinquency*, *18*(2), 295–318. https://doi.org/10.1177/002242788101800206

Moody, G. D., & Siponen, M. (2013). Using the theory of interpersonal behavior to explain non-work-related personal use of the Internet at work. *Information & Management*, *50*(6), 322–335. https://doi.org/10.1016/J.IM.2013.04.005

Moquin, R., & Wakefield, R. L. (2016). The roles of awareness, sanctions, and ethics in software compliance. *Journal of Computer Information Systems*, *56*(3), 261–270. https://doi.org/10.1080/08874417.2016.1153922

Nathans, L. L., Oswald, F. L., & Nimon, K. (2012). Interpreting multiple linear regression: A guidebook of variable importance. *Practical Assessment, Research &*

Evaluation, *17*(9), 1–19. Retrieved from http://pareonline.net/

Norman, G. (2010). Likert scales, levels of measurement and the “laws” of statistics. *Advances in Health Sciences Education*, *15*(5), 625–632. https://doi.org/10.1007/s10459-010-9222-y

Onwuegbuzie, A. J. (2000). Expanding the framework of internal and external validity in quantitative research. *Research in Schools*, *10*, 71–89. Retrieved from http://www.msera.org/publications-rits.html

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, *66*, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly*, *31*(4), 623. https://doi.org/10.2307/25148814

Piquero, N. L., Tibbetts, S. G., & Blankenship, M. B. (2005). Examining the role of differential association and techniques of neutralization in explaining corporate crime. *Deviant Behavior*, *26*(2), 159–188. https://doi.org/10.1080/01639620590881930

Posey, C., Roberts, T. L., Benjamin, P., & Hightower, R. T. (2014). Bridging the divide : A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management*, *51*(5), 551–567. https://doi.org/10.1016/j.im.2014.03.009

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179–214. https://doi.org/10.1080/07421222.2015.1138374

Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security*, *80*, 211–223. https://doi.org/10.1016/J.COSE.2018.09.016

Ritzman, M. E., & Kahle-Piasecki, L. (2016). What works: A systems approach to employee performance in strengthening information security. *Performance Improvement*, *55*(8), 17–22. https://doi.org/10.1002/pfi.21614

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

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. https://doi.org/10.1016/j.cose.2015.05.012

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach : An empirical approach. *Journal of Management Information Systems*, *32*(2), 314–341. https://doi.org/10.1080/07421222.2015.1063315

Sher, M.-L., Talley, P. C., Yang, C.-W., & Kuo, K.-M. (2017). Compliance with electronic medical records privacy policy: an empirical investigation of hospital information technology staff. INQUIRY: The Journal of Health Care Organization, Provision, and Financing, 54, 004695801771175. https://doi.org/10.1177/0046958017711759

Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. *Information and Management*, *54*(8), 1023–1037. https://doi.org/10.1016/j.im.2017.02.007

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487–502. https://doi.org/10.2307/25750688

Siponen, M., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *European Journal of Information Systems*, *23*(3), 289–305. https://doi.org/10.1057/ejis.2012.59

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*, *22*(1), 42–75. https://doi.org/10.1108/IMCS-08-2012-0045

Stahl, B. C., Doherty, N. F., Shaw, M., & Janicke, H. (2014). Critical theory as an approach to the ethics of information security. *Science and Engineering Ethics*, *20*(3), 675–699. https://doi.org/10.1007/s11948-013-9496-6

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, *22*(6), 664–670. https://doi.org/10.2307/2089195

Tarafdar, M., D’Arcy, J., Turel, O., & Gupta, A. (2015). The dark side of information technology. *Sloan Management Review*, *56*(2), 59–70. https://doi.org/10.1111/isj.12015

Teh, P., Ahmed, P. K., & D’Arcy, J. (2015). What drives information security policy violations among banking employees? *Journal of Global Information Management*, *23*(1), 44–64. https://doi.org/10.4018/jgim.2015010103

Tonidandel, S., LeBreton, J. M., & Johnson, J. W. (2009). Determining the statistical significance of relative weights. *Psychological Methods*, *14*(4), 387–399. https://doi.org/10.1037/a0017735

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awarness on information technology professionals’ behavior. *Computers & Security*, *79*, 68–79. https://doi.org/10.1016/J.COSE.2018.08.007

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138–150. https://doi.org/10.1016/J.COSE.2016.02.009

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies : Recommendations for information security awareness programs. *Computers & Security*, *52*, 128–141. https://doi.org/10.1016/j.cose.2015.04.006

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. https://doi.org/10.1057/ejis.2013.27

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, *92*, 25–35. https://doi.org/10.1016/j.dss.2016.09.013

Warner, R. M. (2013). *Applied statistics from bivariate through multivariate techniques* (2nd ed.). Thousand Oaks, CA: Sage.

Weidman, J., & Grossklags, J. (2018). What's in your policy? An analysis of the current state of information security policies in academic institutions (pp. 1–16). Retrieved from https://aisel.aisnet.org/ecis2018_rp/23

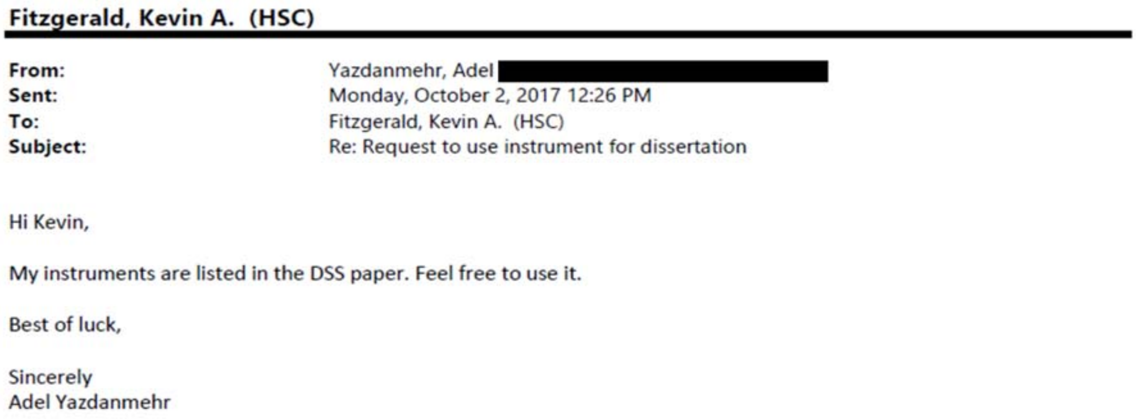
Williams, M. N., Gómez Grajales, C. A., & Kurkiewicz, D. (2013). Assumptions of multiple regression: Correcting two misconceptions. *Practical Assessment, Research & Evaluation*, *18*(11), 1–14. Retrieved from http://pareonline.net/

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*, *28*(2), 266–293. https://doi.org/10.1111/isj.12129

Yang, C., & Lee, H. (2016). A study on the antecedents of healthcare information protection intention. *Information Systems Frontiers*, *18*(2), 253–263. https://doi.org/10.1007/s10796-015-9594-x

Yazdanmehr, A., & Wang, J. (2016). Employees’ information security policy compliance: A norm activation perspective. *Decision Support Systems*, *92*, 36–46. https://doi.org/10.1016/j.dss.2016.09.009

Appendix A: Written Authorization to Use Survey Instruments



Fitzgerald, Kevin A. (HSC)

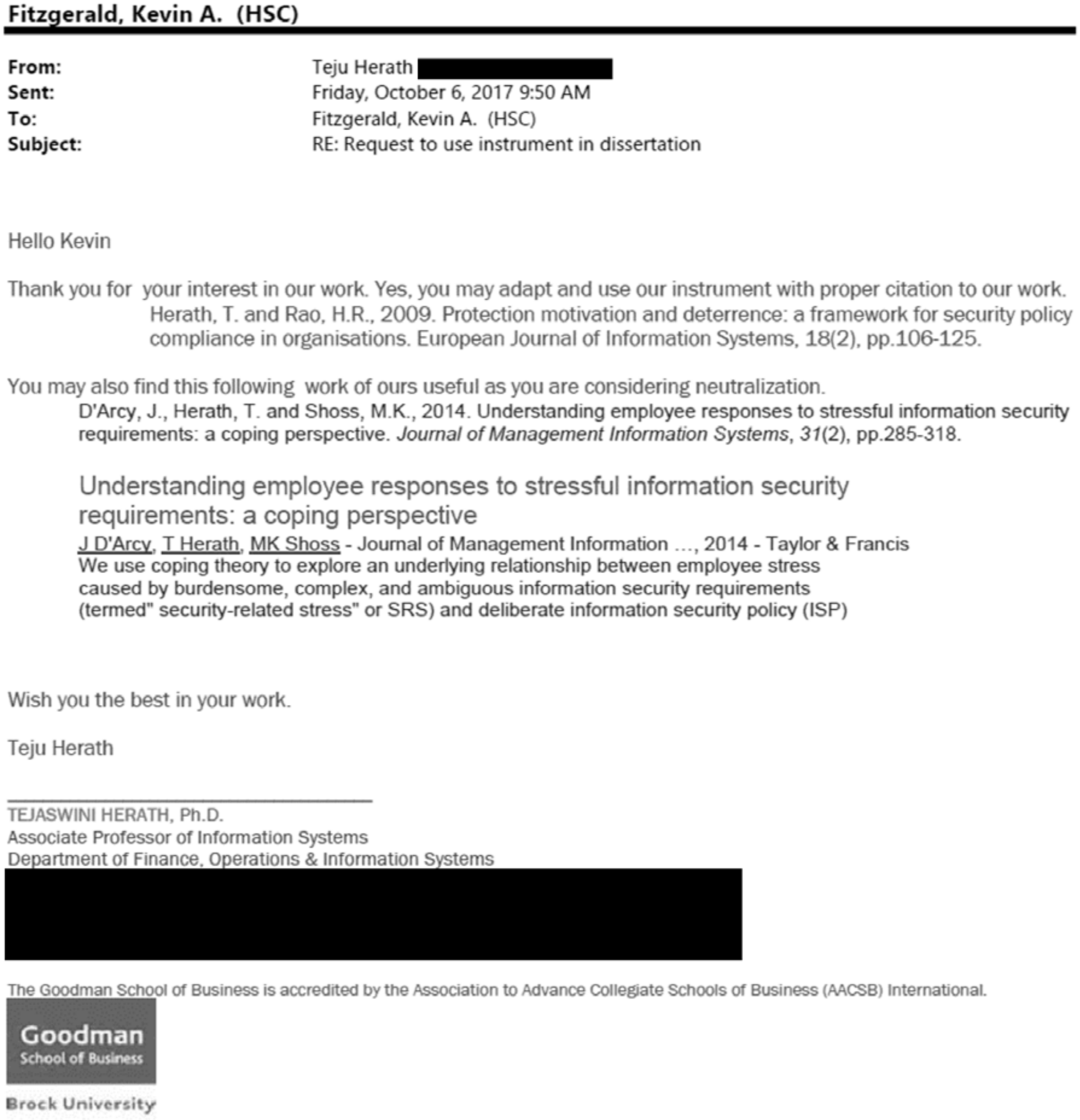
From:	Yazdanmehr, Adel [redacted]
Sent:	Monday, October 2, 2017 12:26 PM
To:	Fitzgerald, Kevin A. (HSC)
Subject:	Re: Request to use instrument for dissertation

Hi Kevin,

My instruments are listed in the DSS paper. Feel free to use it.

Best of luck,

Sincerely
Adel Yazdanmehr



Fitzgerald, Kevin A. (HSC)

From: Teju Herath [redacted]
Sent: Friday, October 6, 2017 9:50 AM
To: Fitzgerald, Kevin A. (HSC)
Subject: RE: Request to use instrument in dissertation

Hello Kevin

Thank you for your interest in our work. Yes, you may adapt and use our instrument with proper citation to our work.
Herath, T. and Rao, H.R., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), pp.106-125.

You may also find this following work of ours useful as you are considering neutralization.
D'Arcy, J., Herath, T. and Shoss, M.K., 2014. Understanding employee responses to stressful information security requirements: a coping perspective. *Journal of Management Information Systems*, *31*(2), pp.285-318.

Understanding employee responses to stressful information security requirements: a coping perspective
J D'Arcy, T Herath, MK Shoss - Journal of Management Information ..., 2014 - Taylor & Francis
We use coping theory to explore an underlying relationship between employee stress caused by burdensome, complex, and ambiguous information security requirements (termed" security-related stress" or SRS) and deliberate information security policy (ISP)

Wish you the best in your work.

Teju Herath

TEJASWINI HERATH, Ph.D.
Associate Professor of Information Systems
Department of Finance, Operations & Information Systems
[redacted]

The Goodman School of Business is accredited by the Association to Advance Collegiate Schools of Business (AACSB) International.

Goodman
School of Business
Brock University

Appendix B: Plots and Histograms of the Standardized Residuals for Each Model

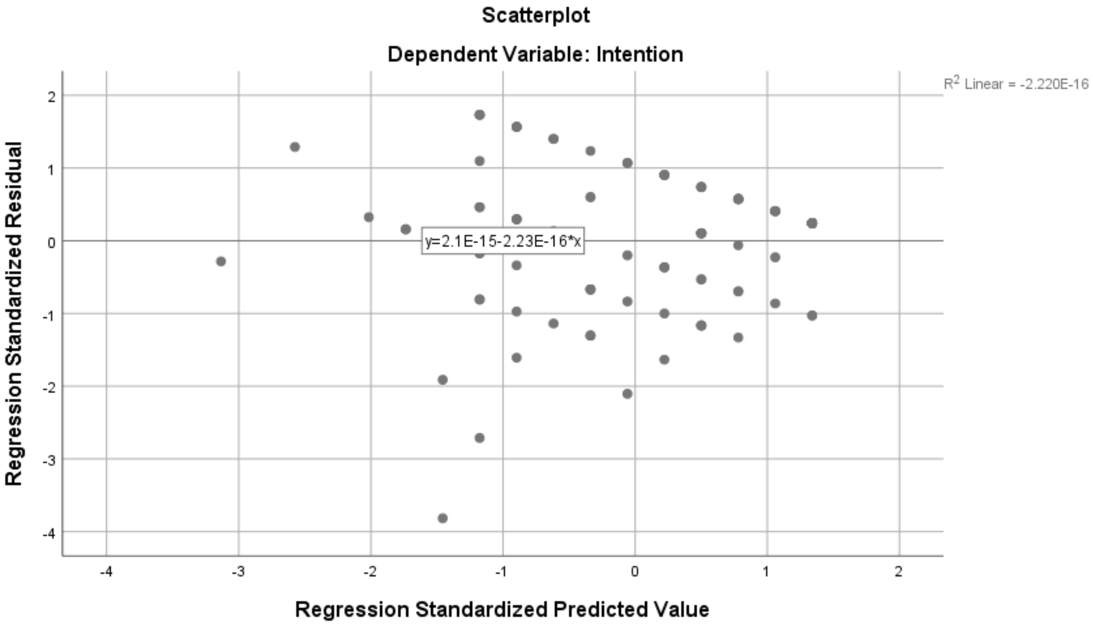


Figure 13. Residuals plot for RQ1, *Severity* and *Intention*.

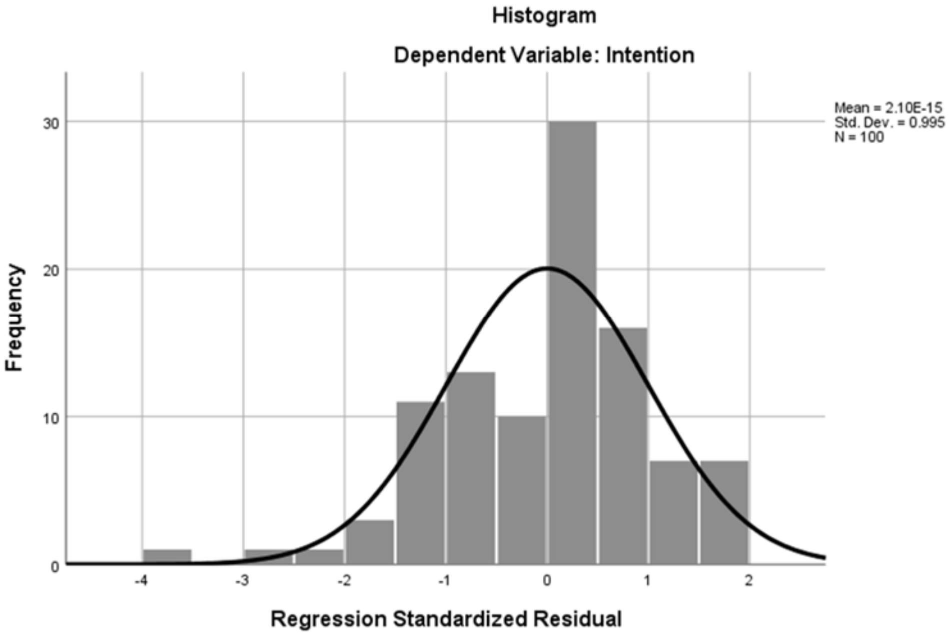


Figure 14. Residuals histogram for RQ1, *Severity* and *Intention*.

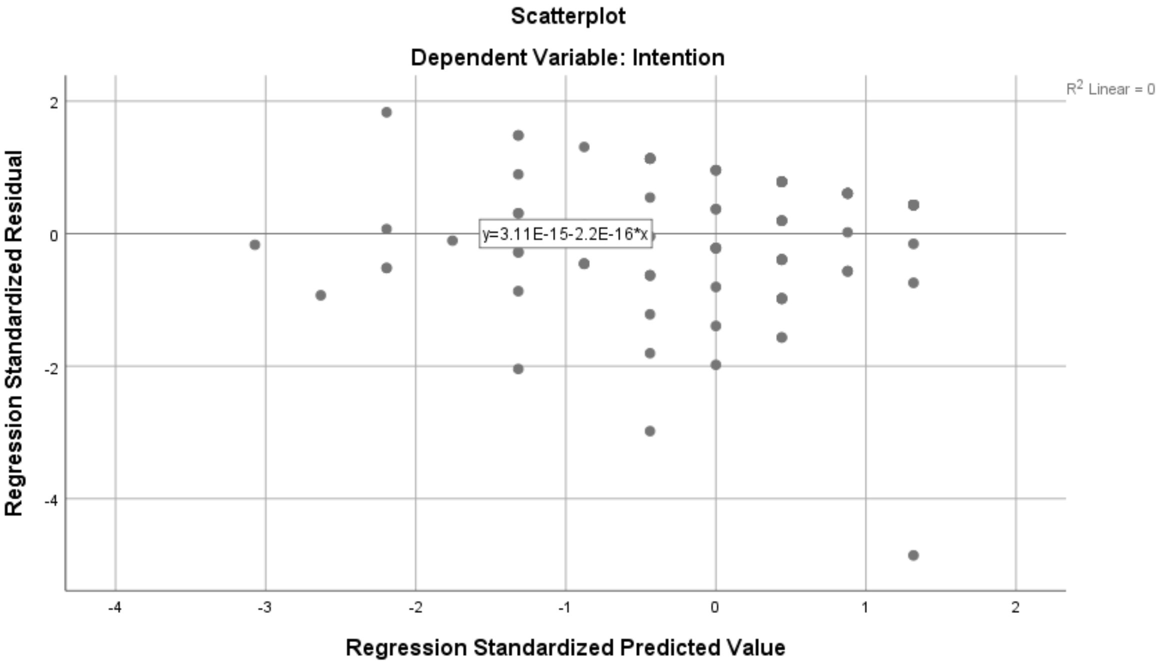


Figure 15. Residuals plot for RQ2, *Vulnerability* and *Intention*.

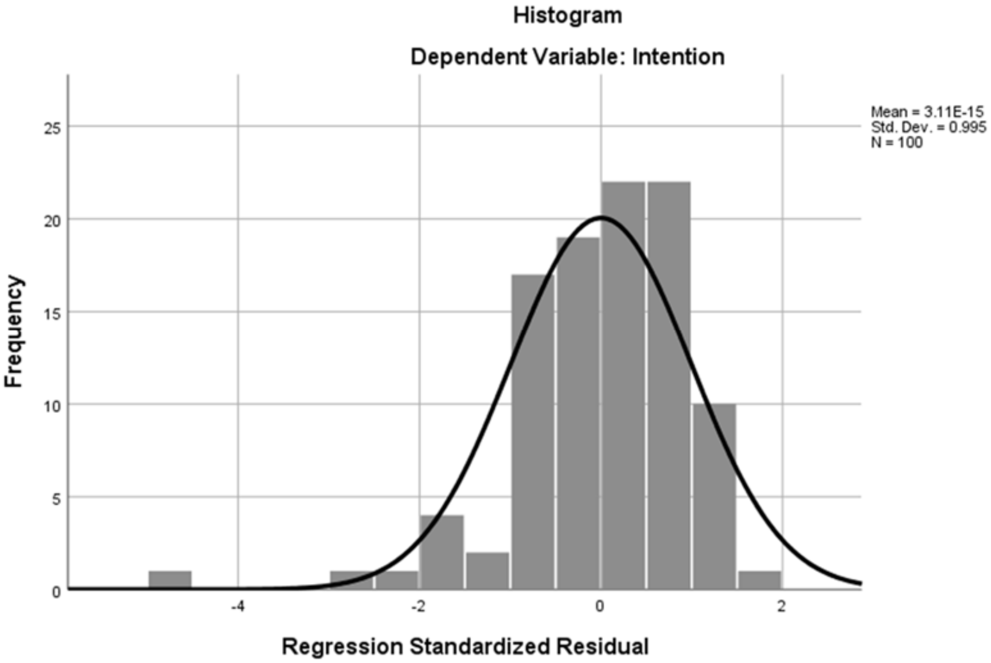


Figure 16. Residuals histogram for RQ2, *Vulnerability* and *Intention*.

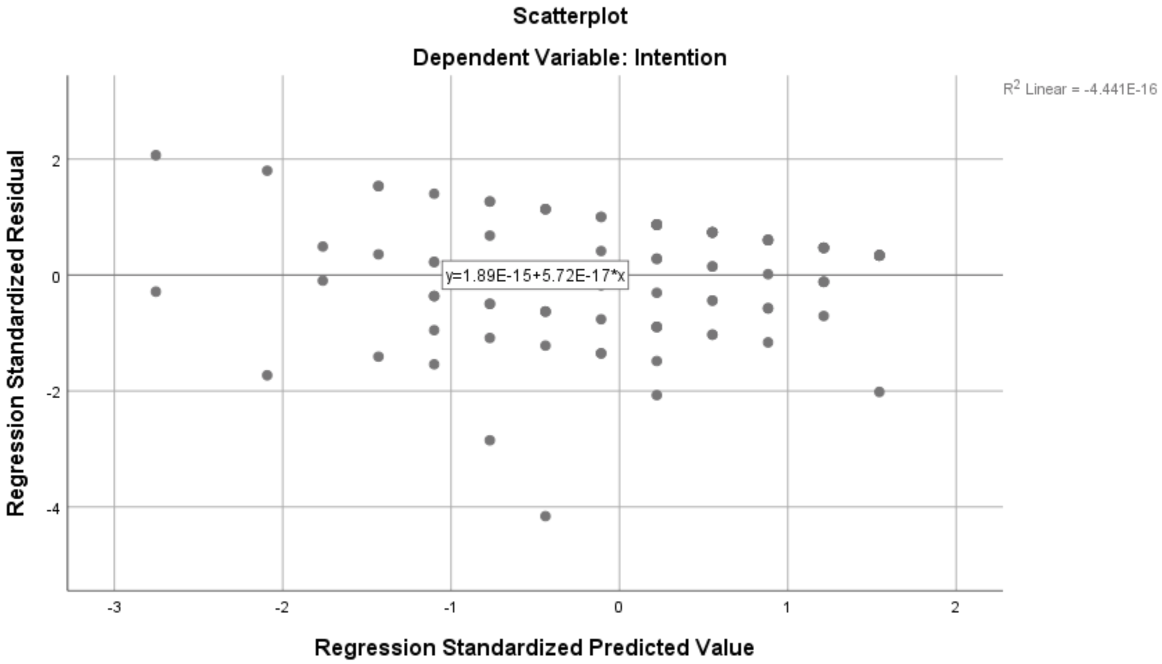


Figure 17. Residuals plot for RQ3, *Awareness* and *Intention*.

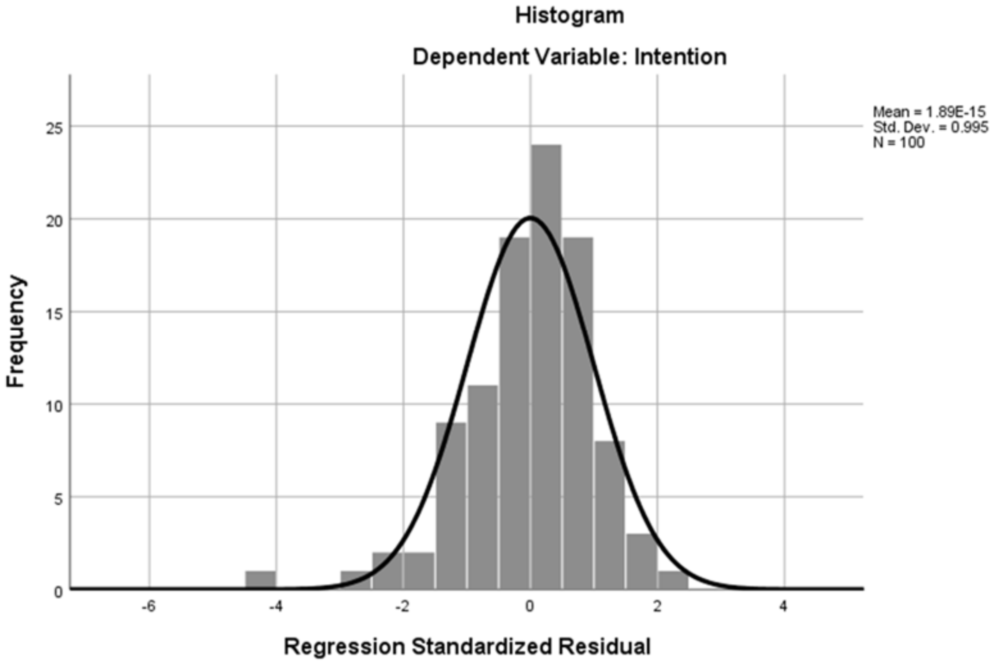


Figure 18. Residuals histogram for RQ3, *Awareness* and *Intention*.

Appendix C: Instrument

Screening Questions

1. Do you work in a higher education organization in the United States with an information security policy?

    (Users that answer “No” will exit the survey.)

2. Are you 18 years old or older?

    (Users that answer “No” will exit the survey.)

3. Do you work at the University of Oklahoma?

    (Users that answer “Yes” will exit the survey.)

Survey Questions

Severity

- The organization disciplines employees who break information security rules.
- My organization terminates employees who repeatedly break security rules.
- If I were caught violating organization information security policies, I would be severely punished.

Vulnerability

- Employee computer practices are properly monitored for policy violations.
- If I violate organization security policies, I would probably be caught.

Awareness

- I believe violation of the organization's information security policy will cause serious troubles to other employees.
- I believe violation of the organization's information security policy will cause serious damages to the organization.
- I worry about problems caused by violation of the organization's information security policy.

Intention

- I am likely to follow organizational security policies.
- It is possible that I will comply with organizational IS security policies to protect the organization's information security.
- I am certain that I will follow organizational security policies.

Survey question Likert scale

1 – *Strongly agree*

2 – *Agree*

3 – *Somewhat agree*

4 – *Neither agree or disagree*

5 – *Somewhat disagree*

6 – *Disagree*

7 – *Strongly disagree*