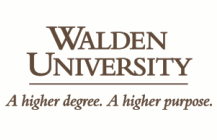

2017

Examining the Behavioral Intention of Individuals' Compliance with Information Security Policies

David A. Brown
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

David Brown

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. Anthony Lolas, Committee Chairperson,
Applied Management and Decision Sciences Faculty

Dr. Raghu Korrapati, Committee Member,
Applied Management and Decision Sciences Faculty

Dr. Jean Gordon, University Reviewer
Applied Management and Decision Sciences Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2017

Abstract

Examining the Behavioral Intention of Individuals' Compliance with Information Security Policies

by

David A. Brown

MEng, Stevens Institute of Technology, 2007

MS, New Jersey Institute of Technology, 2002

MS, Drexel University, 1988

MBA, Monmouth University, 1984

BS, Stockton University, 1980

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Applied Management and Decision Sciences

Walden University

May 2017

Abstract

Target Corporation experienced an information security breach resulting in compromising customers' financial information. Management is responsible for implementing adequate information security policies that protect corporate data and minimize financial losses. The purpose of this experimental study was to examine the effect of a fear appeal communication on an individual's information security policy behavioral intention. The sample population involved information technology professionals randomly selected from the SurveyMonkey audience. A research model, developed using constructs from deterrence theory and protection motivation theory, became the structural model used for partial least squares-structural equation modeling (PLS-SEM) analysis of the survey response data, which indicated that self-efficacy was statistically significant. The remaining model variables, perceived threat vulnerability, perceived threat severity, response efficacy, informal sanction certainty, informal sanction severity, formal sanction certainty, and formal sanction severity, were not statistically significant. A statistically significant self-efficacy result could indicate confidence among the population to comply with information security policies. The nonsignificant results could indicate the fear appeal treatment did not motivate a change in behavior or information security policy awareness bias was introduced by selecting information technology professionals. Social change in information security could be achieved by developing an effective information security policy compliance fear appeal communication, which could change information security compliance behavior and contribute to securing the nation's critical cyber infrastructure and protecting data.

Examining the Behavioral Intention of Individuals' Compliance with Information Security Policies

by

David A. Brown

MEng, Stevens Institute of Technology, 2007

MS, New Jersey Institute of Technology, 2002

MS, Drexel University, 1988

MBA, Monmouth University, 1984

BS, Stockton University, 1980

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Applied Management and Decision Sciences

Walden University

May 2017

Dedication

In loving memory of my mother. My mother understood the value of an education. When I was young, my mother always told me I was going to college, but she never got to see me graduate.

Acknowledgments

I would like to take this opportunity to thank my dissertation chair, Dr. Anthony Lolas, for his motivation to keep us moving forward toward the goal. Also for his assistance and advice guiding me through the dissertation process. I would also like to thank my dissertation team members, Dr. James Froh and Dr. Jean Gordon, for their contribution to helping me complete my dissertation. I would also like to thank Dr. Richard Bush who helped me as I began my Ph.D. education journey.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Deploying information security has become a necessity for organizations implementing information technology. Ensuring employees follow information security policies is a challenge for management. The purpose of this study was to examine the effect of an individual's perspectives on information security policy compliance behavioral intention. Individuals received a survey, and responses to their perspectives and behaviors were statistically analyzed. The results of the study could be useful to management responsible for implementing information security. Reliance on information technology to support public infrastructure is increasing. An improvement in information security compliance could be achieved by examining information technology professionals' perceptions regarding information security policies. Improved information security compliance could encourage positive social change in information security and contribute to securing the public's information technology infrastructure.

In Chapter 1, I present background information regarding the development of a study designed to examine information security compliance behavioral intention. This chapter also includes a statement of the problem, the purpose of the study, research questions, hypotheses, and theoretical foundation. The chapter concludes with a discussion on the nature of the study definition, assumptions, scope, delimitation, limitations, and the significance of the research study.

Background of the Study

Information security has become an increasing concern for management (Padayachee, 2012). Researchers who have examined information security have focused

on the technical aspects of information security (Crossler et al., 2013). Technical aspects of information security are the hardware and software measures integrated into an organization's information system infrastructure. Standard information security measures include firewalls, antivirus software, data backup, access controls, encryption, and continuous monitoring (Ifinedo, 2012). Ifinedo (2012) found that organizations incorporating both technical and nontechnical information security measures are more successful at protecting their information assets. Management should implement a multifaceted approach to information asset protection to achieve an improved level of information security (Ifinedo, 2012). Management should incorporate individual and organizational issues in addition to information security technology implementation (Ifinedo, 2014). Because of the need to address nontechnical information security measures, researchers have incorporated sociology, psychology, and organizational behavior approaches into their information security studies (Chu & Chau, 2014). Improving information security policy compliance is one method that could improve information asset protection. When users do not comply with information security policies, implemented information security measures lose their effectiveness (Puhakainen & Siponen, 2010). Information security policies are those guidelines, requirements, and rules established by management to direct the behaviors of their employees (Ifinedo, 2014). Crossler et al. (2013) identified areas of information security behavioral research to be examined in future research. Future research topics should consider

- deviant behavior versus misbehavior of insiders;
- revealing the world of the hacker;

- information security compliance improvement; and
- information security across cultures.

Because of the importance of information security compliance behaviors, researchers have examined behavioral intention by adapting theories from sociology and psychology as theoretical foundations.

Protection motivation theory originated in the field of psychology, and researchers have adapted this theory to information security compliance behavioral research (Kim, Yang, & Park, 2014). The basis of protection motivation theory is when an individual confronts a threat in which the result is a response (Anderson & Argawal, 2010). This threat is a fear appeal and contains information communicating the severity and possibility of a threat along with a recommended response. Once a fear appeal is received, a cognitive mediating process begins, and an individual appraises the threat and the recommended response. At the conclusion of the appraisal process, the individual takes action because the level of fear has motivated him or her or he or she takes no action because there is no perception of a threat (Johnston & Warkentin, 2010). Because a fear appeal could motivate an individual to take action, researchers in information technology behavior frequently use protection motivation theory as a theoretical foundation for their studies.

Vance, Siponen, and Pahnila (2012) used protection motivation theory to examine information security compliance among Finnish municipal employees. Ifinedo (2012) integrated the constructs of protection motivation theory and the theory of planned behavior to examine information security policy compliance behavioral intention in

Canadian noninformation system managers. Siponen, Mahmood, and Pahnila (2014) also used protection motivation theory in a study of information security policy behavioral intention. Siponen et al. expanded protection motivation theory by including constructs from the theory of reasoned action and cognitive evaluation theory. Protection motivation theory served as the basis for all of these studies, but each developed a unique research model. There were other opinions on the application of protection motivation theory was inadequate for the study of information security compliance behavioral intention.

Johnston, Warkentin, and Siponen (2015) contended that the results of studies using protection motivation theory as a theoretical foundation were inconsistent. Johnston et al. developed a new research model merging deterrence theory with protection motivation theory to examine information security compliance behavioral intention. The merged theories were intended to address the inadequacies regarding protection motivation theory. Deterrence theory is a theoretical view based in criminology, and according to the theory, people make reasoned decisions (D'Arcy & Herath, 2011). Before committing a crime, an individual performs a cost-benefit analysis. If the risk of getting caught is high and the punishment is severe, an individual will not commit the crime (Siponen & Vance, 2010). Because an individual is less likely to commit an unwanted behavior when the probability of getting caught is high and the punishment is severe, researchers examining information security policy compliance have used deterrence theory as a theoretical foundation (Son, 2011).

Siponen and Vance (2010) combined the constructs of neutralization theory and deterrence theory to create a research model to examine information security policy

violations. Son (2011) focused on the constructs of deterrence theory for a research model examining information security policy compliance behavioral intention. Cheng, Li, Li, Holm, and Zhai (2013) conducted a study examining information security policy violation behavioral intention using deterrence theory and social bond theory.

Although there have been some studies on information security compliance behavioral intention using protection motivation theory and deterrence theory individually or combined with other behavioral theory constructs, there is a gap in the knowledge regarding the merging of protection motivation theory and deterrence theory to examine information security policy compliance behavioral intention. Johnston et al. (2015) merged protection motivation theory and deterrence theory in the literature, but examined password, USB, and data theft. The population for the Johnston et al. study was Finnish government employees. To address this gap in knowledge, I conducted a study examining information security policy compliance behavioral intention of individuals located in the United States using protection motivation theory and deterrence theory. This study is needed to increase information asset security through the improvement of information security policy compliance behavioral intention.

Problem Statement

An information security breach at Target resulted in compromised customer information and is expected to cost in excess of $1 billion (Stanwick & Stanwick, 2014). Information security policy compliance is crucial to information security success (Furnell & Rajendran, 2012). Management's general problem is the inability to implement

adequate information security, which results in compromised data and financial losses (Posey, Roberts, Lowry, & Hightower, 2014).

Implementing information security using only a technical approach is insufficient (Ifinedo, 2012). Information security policy compliance is a nontechnical security method (Vance et al., 2012). Chu and Chau (2014) examined behavioral intentions to understand how perceptions affect information security compliance. There is a gap in the literature related to studies of information security policy compliance behavioral intention merging protection motivation theory and deterrence theory. The behavior of information technology professionals that results in noncompliance with information security policy resulting in inadequate information security leads to data compromise

Energy, transportation, communication, and civil protection infrastructure supporting society is increasingly dependent on information technology (Piggin, 2014). Inadequate information security puts this infrastructure at risk. An examination of behavioral intention to comply with information security policies by information technology professionals could result in information security compliance and could encourage positive social change in information security and contribute to securing society's information technology infrastructure.

Purpose of the Study

The purpose of the quantitative, experimental study was to examine the relationship between information security policy compliance behavioral intention and the merged constructs from protection motivation theory and deterrence theory. The constructs from protection motivation theory and deterrence theory (perceived threat

vulnerability, perceived threat severity, response efficacy, self-efficacy, informal sanction certainty, informal sanction severity, formal sanction certainty, and formal sanction severity) were the independent variables. Information security policy compliance behavioral intention was the dependent variable. Information technology professionals in intermediate and entry level positions were randomly selected from the SurveyMonkey audience. Control and intervening variables were not applicable to the study because the focus was on the relationship between the independent and dependent variables.

Research Questions and Hypotheses

Siponen et al. (2014) identified protection motivation theory as "the leading theory in the area of health behavior motivation" (p. 218). Constructs from protection motivation theory were included in the research model to examine information security compliance behavioral intention. Siponen et al. hypothesized that perceived threat vulnerability, perceived threat severity, response efficacy, and self-efficacy would influence information security policy compliance behavioral intention. Johnston et al. (2015) recognized that protection motivation theory served as the theoretical foundation in information security compliance research, but the results were mixed. Constructs from protection motivation theory were merged with constructs from deterrence theory to address the inconsistent results. The research model included the protection motivation theory constructs perceived threat vulnerability, perceived threat severity, response efficacy, and self-efficacy. Deterrence theory constructs, informal sanction certainty, informal sanction severity, formal sanction certainty, formal sanction severity, and sanction celerity were also included in the research model examining information

security policy compliance behavioral intention. The research model developed by Johnston et al. served as the basis for the development of the research model for this dissertation. One of the deterrence theory constructs, sanction celerity, was excluded from the dissertation research model. Johnston et al. argued that sanction celerity was more relevant to animal behavior and voiced concerns about its relevance. Johnston et al. indicated that sanction celerity was not a significant influence on information security compliance behavioral intention. Due to the Johnston et al.'s concern about the relevance of sanction celerity and the nonsignificant results, the construct sanction celerity was omitted from the dissertation research model. These factors led to the development of the following research questions:

RQ1–What is the effect of informal sanction certainty on an individual's information security policy compliance behavioral?

$H_0$1: Informal sanction certainty will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a1: Informal sanction certainty will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ2–What is the effect of informal sanction severity on an individual's behavioral intention to comply with information security policies?

$H_0$2: Informal sanction severity will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a 2: Informal sanction severity will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ3–What is the effect of formal sanction certainty on an individual's behavioral intention to comply with information security policies?

$H_0$3: Formal sanction certainty will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a3: Formal sanction certainty will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ4–What is the effect of formal sanction severity on an individual's behavioral intention to comply with information security policies?

$H_0$4: Formal sanction severity will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a4: Formal sanction severity will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ5–What is the effect of perceived threat vulnerability on an individual's behavioral intention to comply with information security policies?

$H_0$5: Perceived threat vulnerability will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a5: Perceived threat vulnerability will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ6–What is the effect of perceived threat severity on an individual's behavioral intention to comply with information security policies?

$H_0$6: Perceived threat severity will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a6: Perceived threat severity will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ7–What is the effect of response efficacy on an individual's behavioral intention to comply with information security policies?

$H_0 7$: Response efficacy will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

$H_a 7$: Response efficacy will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ8–What is the effect of self-efficacy on an individual's behavioral intention to comply with information security policies?

$H_0 8$: Self-efficacy will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

$H_a 8$: Self-efficacy will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

Theoretical Foundation

Scholars who have examined information security behavior have incorporated theories from criminology and psychology (Vance et al., 2012). Neutralization theory and deterrence theory from the study of criminology have been used to examine information security policy compliance (Siponen & Vance, 2010). Researchers used theories from the field of psychology to study information security behaviors. Meso, Ding, and Zu (2013) developed a research model based on protection motivation theory to examine how course lecture knowledge and hands-on project experience affect student information

security behavioral intention. Bulgurcu, Cavusoglu, and Benbast (2010) examined information security compliance behavior using a research model based on the theory of planned behavior.

Researchers have also expanded the theoretical foundations used in information security behavior studies by combining theories. Ifinedo (2012) combined protection motivation theory and the theory of planned behavior to examine information security compliance behavior. Yoon and Kim (2013) combined protection motivation theory and the theory of planned behavior to examine information security behavioral intention. Siponen and Vance (2010) researched information security policy violations using a theoretical foundation combining neutralization theory and deterrence theory. Johnston et al. (2015) identified deficiencies and inconsistent results in prior research using protection motivation theory. To address these issues, Johnston et al. extended protection motivation theory by integrating the constructs of deterrence theory to examine information security policy compliance behavioral intention. The Johnston et al. theoretical foundation served as the basis for the research model developed for this dissertation. As the Johnston et al. study was the only one identified during a search of the literature combining protection motivation theory and deterrence theory, each theory will be introduced separately.

Protection Motivation Theory

Rogers (1975) proposed protection motivation theory in the seminal research on how a fear appeal can change attitudes. A fear appeal is a persuasive communication intended to modify a behavior (Johnston & Warkentin, 2010). Witte (1992) identified two

components in a fear appeal. The first part contains information regarding the severity of a threat and the chance of the threat occurring. A recommendation is included in the second part and provides an action to avoid the threat and the value of performing the recommended action. Rogers (1983) expanded on protection motivation theory to define the perceptions associated with the cognitive mediating processes initiated by the fear appeal. Once the information regarding a threat is received, a cognitive mediating process begins an appraisal process that will produce positive or negative responses. There is a threat appraisal process and a coping appraisal process. Within the threat appraisal process are the constructs perceived threat vulnerability, perceived threat severity, and rewards. Constructs in the coping appraisal process include response efficacy, self-efficacy, and response cost. Each construct is hypothesized to either positively or negatively affect an individual's behavioral intention. Perceived threat vulnerability, perceived threat severity, response efficacy, and self-efficacy were hypothesized to have a positive effect. Reward and response cost were hypothesized to have a negative effect (Vance et al., 2012).

Deterrence Theory

According to deterrence theory, before committing a crime, a person will perform a cost-benefit analysis. If the individual believes the risk of getting caught is high and the associated punishment if caught is equally high, there is less motivation to commit the violation (Johnston et al., 2015). Onwudiwe, Odo, and Onyeozili (2004) found the constructs of deterrence theory in the works of Hobbes, Beccaria, and Bentham. There are three constructs included in deterrence theory: perceived severity, perceived certainty,

and perceived celerity. When an individual perceives the punishment for an activity to be severe, committing an undesirable act is a less likely possibility. If a person perceives a punishment for an undesirable act is certain, an individual is less likely to commit an undesirable action. A swift punishment will also reduce the possibility of committing an undesirable action. Siponen and Vance (2010) hypothesized that within an organization there could be external and internal punishments and personal shame associated with an information security policy violation. Each of these could have a negative effect on information security policy violations.

Researchers examining information security behaviors used protection motivation theory and deterrence theory as theoretical foundations. Anderson and Agarwal (2010) found several information security behavior studies that included protection motivation theory as a theoretical foundation. D'Arcy and Devaraj (2012) identified that the deterrence theory constructs, perceived sanction severity and perceived sanction certainty, were frequently used in information security behavior research. Because the focus of this dissertation was on an examination of information security compliance behavioral intention, using a quantitative research methodology combining protection motivation theory and deterrence theory assisted in answering the research questions. Chapter 2 includes a more detailed examination of protection motivation theory and deterrence theory.

Nature of the Study

Much of the literature on investigating information security behaviors used a nonexperimental, correlational research design. Posey et al. (2014) identified a need to

examine the difference between groups as opposed to additional protection motivation theory relationship validation. Johnston et al. (2015) conducted a study of information security compliance behaviors using the mixed-methods research. The quantitative portion of the research included a posttest-only control group experimental design. Study participants were assigned randomly to either the experimental or control groups. Participants in the experimental group received an experimental treatment and a posttest survey. The control group only received a posttest survey and did not receive the treatment. A two group research design allowed for an additional level of statistical analysis. Any change between groups can be attributed to the information provided in the treatment.

Key study variables for the dissertation study were those constructs from protection motivation theory and deterrence theory. These theoretical constructs were the research model independent variables. Independent variables from protection motivation theory were perceived threat vulnerability, perceived threat severity, response efficacy, and self-efficacy. Deterrence theory independent variables were formal sanction certainty, formal sanction severity, informal sanction certainty, and informal sanction severity. Information security compliance behavioral intention was the dependent variable. Because the focus of the dissertation research was on the independent and dependent variables, no mediating or covariate variables are included.

Each variable was examined individually. An examination of the interaction of variables was beyond the scope of this study. Each variable was measured using a 5-point Likert scale. Questions related to protection motivation theory used a Likert-type level of

agreement scale and included the following responses 1=*strongly disagree*, 2=*disagree*, 3=*neither agree or disagree*, 4=*agree*, and 5=*strongly agree* (Vagias, 2006). For questions related to deterrence theory, a level of probability scale was used and included the responses 1=*not probable*, 2=*somewhat improbable*, 3=*neutral*, 4=*somewhat probable*, and 5=*very probable* (Vagias, 2006).

Johnston et al. (2015) used the mixed-methods research to examine information security behaviors, and the quantitative portion of the study included a posttest-only control group research design. Singleton and Straits (2010) identified the posttest-only control group design as "the simplest of the true experimental designs" (p. 239). All of the necessary elements for an experimental design, random assignment of participants to the experimental and control groups, the introduction of an experimental treatment, and a posttreatment survey, are included in the research design. Because additional information regarding the experimental treatment can be obtained, I only used a posttest-only control group experimental design. Using a true experimental design requires the random selection of participants. Individuals self-reporting their job function as information technology and their job level as intermediate or entry level professionals, over the age of 18, and located in the United States were selected from the SurveyMonkey audience. Individuals participating in the study were asked if they had received information security policy training. Participants for this dissertation were randomly selected from the SurveyMonkey audience population and randomly assigned to either the experimental group or control group. SurveyMonkey performed the random selection process and forwarded an e-mail to each participant with a link to the survey. After the survey had

been completed, response and demographic data were downloaded from the SurveyMonkey website. Descriptive statistical analysis was performed on the data. A partial least squares-structural equation model analysis was conducted to validate the research model and perform hypotheses analysis.

Definition of Terms

Appeal to higher loyalties: The belief the only method of protection is by complying with information security policies (Kim et al., 2014).

Behavioral intention: "[A] judgment call about how an individual will behave toward complying with information security policies" (Siponen et al., 2015, p. 219).

Condemnation of the condemners: The amount an individual places the blame for an information security policy violation on those judging the action (Kim et al., 2014).

Defense of the necessity: The belief that there is no guilt associated with an information security policy violation because it was unavoidable (Kim et al., 2014).

Defense of ubiquity: The belief an information security policy violation is acceptable because everyone violates the policy (Kim et al., 2014).

Denial of injury: The amount an individual denies an information security policy violation causes any harm (Kim et al., 2014).

Denial of responsibility: The amount an individual denies responsibility for an information security policy compliance violation (Kim et al., 2014).

Denial of the victim: The belief that the victim deserves the outcome of an information security policy violation (Siponen & Vance, 2010).

Formal sanction certainty: A perception that organizational punishment will be imposed (Johnston et al., 2015).

Formal sanction severity: A perception that organizational punishment will be harsh (Johnston et al., 2015).

Informal sanction certainty: A perception that punishment from friends and peers will be imposed (Johnston et al., 2015).

Informal sanction severity: A perception that punishment from friends and peers will be harsh (Johnston et al., 2015).

Metaphor of the ledger: The belief an information security policy violation would be excused because of previous good behavior (Kim et al., 2014).

Perceived threat severity: "[T]he severity of the consequences of the event" (Meso et al., 2013, p. 53).

Perceived threat vulnerability: "[A]n individual's assessment of the probability of threatening events" (Meso et al., 2013, p. 53).

Response costs: "[T]he costs associated with the recommended behavior" (Meso et al., 2013, p. 53).

Response efficacy: "[T]he effectiveness of the recommended behavior in removing or preventing possible harm" (Meso et al., 2013, p. 53).

Reward: A method used to encourage information security policy compliance (Padayachee, 2012, p. 677).

Self-efficacy: "[T]he belief that one can successfully enact the recommended behavior" (Meso et al., 2013, p. 53).

Sanction celerity: A perception that punishment will be quick (Johnston et al., 2015).

Assumptions

For this study, certain assumptions about the cognitive mediating process associated with a fear appeal communication were made. I assumed that the fear appeal communication was sufficient to motivate a change in the participant. It was also assumed that the responses provided by the participant reflected his or her actual perceptions to the survey questions and statements. The accuracy of the participants' demographic information used to select the sample and their willingness to complete the survey was also assumed.

Scope and Delimitations

For this study, the population was information technology professionals in intermediate or entry-level position professionals who are over the age of 18 located in the United States and who were members of the SurveyMonkey audience. Study participants were asked if they had received information security policy training. These demographics served as the parameters provided to SurveyMonkey to select study participants. SurveyMonkey recruits individuals to become SurveyMonkey audience members willing to participate in responding to surveys. With more than 45 million members, the SurveyMonkey audience offers a diverse population to academic researchers (SurveyMonkey Audience for Academics, 2016). Individuals who were not SurveyMonkey members were excluded from the study. SurveyMonkey performs the participant sample selection based on the provided demographics. Because participant

selection was from the SurveyMonkey audience and not the general population, generalization is limited. A random sample was selected from the population to increase the ability to generalize the results.

Various other behavioral theories have been used in whole or in part for information security compliance studies. The theory of reasoned action, the theory of planned behavior, neutralization theory, social bond theory, and cognitive evaluation theory were not considered and were excluded from the study.

A delimitation of the study is related to the availability of literature supporting the theoretical foundation. After a review of the literature, only a single study was found that included a combination of protection motivation theory and deterrence theory as a theoretical foundation. Because of a lack of similar literature, the formulation of the research model relied on multiple information security studies using protection motivation theory as the theoretical foundation. These studies were combined with information security compliance studies using deterrence theory to develop a research model used to examine information security policy compliance behavioral intention.

Limitations

A limitation of the study was the reliance on respondents' self-reported responses to the survey. Although obtaining actual measures of behavioral intention could be an improvement, obtaining these actual measures could not be possible. The study sample was selected based on the demographic information provided by the SurveyMonkey audience member. Because the demographic information provided to SurveyMonkey by the member was not verifiable, determining the accuracy of the demographic data was

not possible. The introduction of bias was possible by using the SurveyMonkey audience. Because SurveyMonkey audience members were familiar with the use of information technology required for online survey participation, this increased information technology awareness may introduce bias. Individuals regularly using information technology may have additional information security policy awareness that the general population does not possess.

Significance of the Study

This research may fill a gap in the literature regarding management's understanding of information security policy behavioral intention by integrating deterrence theory and protection motivation theory to examine behavioral intention to comply with information security policy. The results of this study could provide contributions to the theories on behavioral intention and practical applications that can be used by an organization's management to address the problem of information security policy noncompliance. There is a growing threat to the United States's critical cyber infrastructure from cybercriminals (Shackelford, Proia, Martell, & Craig, 2015). The results of the study could add to the body of knowledge on the problem of information security noncompliance. Examining the behavioral intention to comply with information security policies by information technology professionals could result in improved information security compliance and could foster positive social change in information security and contribute to securing the nation's cyber infrastructure.

Significance to Theory

Rogers's (1975) seminal work on fear appeals and proposing protection motivation theory identified a limitation to the theory. Because the proposed theory did not include all possible elements affecting attitude change, there may be other variables that affect attitude change. Rogers acknowledged that protection motivation theory possesses a limited number of elements used to explain model variance and other variables may determine attitude change. Rogers suggested the development of a comprehensive theoretical foundation through "theory building and empirical research" (p. 110).

Rogers's (1975) suggestion of elaborating on protection motivation theory by conducting research and developing a new theoretical foundation has served as motivation for subsequent research. Studies on information security compliance using protection motivation theory have expanded the theoretical foundation by integrating additional constructs. Lee (2011) included the constructs of moral obligation and social influence with protection motivation theory to examine antiplagiarism software adoption. Ifinedo (2012) combined the constructs from the theory of planned behavior with protection motivation theory to examine information security policy compliance behavioral intention. Johnston et al. (2015) combined deterrence theory and protection motivation theory to develop an enhanced fear appeal theoretical framework. The theoretical foundation developed by Johnston et al. served as the theoretical foundation for this dissertation.

This study will advance theory by refining the Johnston et al.'s (2015) theoretical model, selecting a different population, and selecting information security policy compliance behavioral intention as the dependent variable. Research on the effect of a fear appeal on information security compliance behavioral intention was limited to the research conducted by Johnston et al. Contributions to advancing the theory are possible through validating the theoretical foundation, determining the ability of the theoretical foundation to be generalized, and building on prior research through refinement of the research model.

Significance to Practice

Information security management confronts daily threats to information assets, information system infrastructure, and personal computers (Johnston & Warkentin, 2010). Because organizations have become reliant on information technology, management must deploy both technical and nontechnical information security measures (Ifinedo, 2012). Over half of the information security breaches are the result of employees not complying with information security policy. Management has become concerned about the criticality of information security policy compliance by employees (Vance et al., 2012).

Implications for practice contribution made by this dissertation include improving information security policy compliance, understanding how perceptions influence information security policy compliance, and development of effective communications to enhance the information security environment. Ifinedo (2012) noted the importance of self-efficacy and response efficacy to information security policy compliance.

Management can use the information in this dissertation to determine employee self-efficacy and response efficacy and develop the knowledge and skills necessary to protect the information assets. Management can also use the dissertation survey technique of surveying two groups and providing an information security communication to only one group. Comparing two groups could give management the ability to determine the effectiveness of an information security communication before distributing the communication through the entire organization.

Significance to Social Change

Society has become reliant on information technology for providing critical services. Transportation, civil infrastructure, power delivery, and medical treatment all rely on information technology. Organizations responsible for operating these technology infrastructures are also responsible for their protection. These organizations are responsible to society for the safe and reliable delivery of the services provided by these infrastructures. The public has become more aware of the information security risks associated with an industrial control system with the release of information regarding the Stuxnet malware (Piggin, 2014). Positive social change can be achieved through increasing the information security policy compliance of employees responsible for operating the information technology controlling society's critical infrastructure. A majority of the information security breaches occur as the result of information security policy noncompliance (Vance et al., 2012). Compliance with information security policy will improve organizational information asset protection. Improved information security policy compliance could promote positive social change in information technology

security and contribute to securing society's critical information technology infrastructure.

Summary and Transition

Because of noncompliance with information security policy, the problem of inadequate information security is an issue for management. I conducted a study to examine individuals' perceptions and their influence on behavioral intention to fill a gap in the knowledge regarding information security policy compliance behavioral intention. I used a theoretical foundation combining the constructs of protection motivation and deterrence theory to examine information security policy behavioral intention. In much of the literature reviewed, researchers conducted nonexperimental studies to examine information security compliance. A posttest-only control group research design was used to expand on the research design used in prior studies. Many of the security breaches organizations experience are the result of insufficient information security policy compliance. An organization can achieve information asset protection improvement through information security compliance.

Chapter 2 is a review of the literature regarding the topic of information security compliance and associated theories. Because the theories used to study information security compliance come from the fields of criminology and psychology, seminal work on the development of protection motivation theory and deterrence theory is discussed. A discussion of studies using various theoretical foundations to examine information security policy behavioral intention follows an introduction to the theories. The review

concludes with an examination of literature regarding using a survey service provider to conduct web-based surveys.

Chapter 2: Literature Review

A single information security breach at Target resulted in 40 million customers having their credit and debit card information compromised and is expected to cost more than $1 billion (Stanwick & Stanwick, 2014). Information security risks carry severe consequences that include corporate liability, loss of reputation, and monetary loss (Bulgurcu et al., 2010). Acceptance and compliance with an organization's information security policies by employees are crucial to a successful information security implementation (Furnell & Rajendran, 2012). The problem of information security policy noncompliance was analyzed through an approach combining protection motivation theory and deterrence theory to investigate behavioral intention. The purpose of this study was to examine behavioral intention to comply with information security policy. To better understand how behaviors affect information security compliance, research was conducted examining behavioral effects (Chu & Chau, 2014; Humaidi & Balakrishnan, 2015; Kim et al., 2014; Safa, Von Solms, & Furnell, 2016; Shropshire, Warkentin, & Sharma, 2015).

Because protection motivation theory and deterrence theory served as the theoretical foundation, current literature on both theories are discussed. Literature on the genesis of protection motivation theory and deterrence theory will start the literature review. Following the seminal study discussion are summaries of research studies on information security compliance using protection motivation theory as the theoretical foundation. Protection motivation theory study summaries are followed by additional studies using deterrence theory to examine information security policy behavioral

intention. I will demonstrate how researchers have used constructs from these theories to develop research models used to examine information security compliance behavior. Neutralization theory and the theory of planned behavior have also been used in studies to examine information security compliance and are discussed to provide a complete view of the current literature. Concluding the literature review is a review of the literature related to survey service providers. Because I used a survey process provider, a review of research studies using a survey service provider is presented.

Literature Search Strategy

I obtained literature for this review from databases in the Walden University Library and Google Scholar. Stockton University library was also used to obtain books and copies of printed articles. The search did not include individual databases in the Walden University Library. Searches were performed using Thoreau to search multiple databases. All searches were limited to peer-reviewed scholarly journals. The scope of the initial literature search included the years 2006 to 2016 to gain a broader perspective. As the search continued, the search was limited to include the years 2010 to 2016. Initial search terms included *information security compliance, information security behavior,* and *information security policy compliance.* After reviewing the initial set of literature, the search was expanded to include search terms related to theories used in these studies and included *protection motivation theory, deterrence theory, the theory of planned behavior, the theory of reasoned action,* and *neutralization theory*. To further narrow the search criteria, the theory terms *protection motivation theory, deterrence theory, the theory of planned behavior, the theory of reasoned action,* and *neutralization theory* were

combined with topic terms *information security compliance, information security behavior,* and *information security policy compliance* in pairs. Searches were performed using one theory and one topic term. As the research study review progressed, the search scope was expanded to gather seminal research on protection motivation theory. Because deterrence theory was also used in criminology studies, the terms *deterrence theory* and *criminology* were included in the search to identify seminal work. Peer-reviewed articles were used to obtain literature on information security behavior studies and their associated theoretical foundations. A final search was performed using the term *SurveyMonkey* to identify research studies using the SurveyMonkey survey service. A combination of peer-reviewed articles and websites were used to gather literature related to SurveyMonkey.

Theoretical Foundation

Organizations relying on information systems to store valuable information implement information security measures to protect their information assets. Frequently these measures include technical information security measures that may include firewalls and antivirus software. Although technical information security measures provide a certain level of protection, management should include nontechnical security measures in their information security portfolio. One example of a nontechnical information security measure is an information security policy. Information security policy can influence an individual's behavior (Ifinedo, 2012). Scholars examining these behaviors have used theories from social psychology and criminology. Vance et al. (2012) suggested the use of the sociocognitive protection motivation theory as a

theoretical foundation for examining information security policy compliance behavior. Johnston et al. (2015) disagreed and found protection motivation theory as inadequate and suggested an enhanced research model incorporating constructs from deterrence theory into a protection motivation theory research model. The theoretical foundation for the quantitative dissertation study incorporated constructs from protection motivation theory and deterrence theory.

Seminal Work

Rogers (1975) examined the effect of fear appeals ability to change attitudes and proposed protection motivation theory. A fear appeal is a persuasive communication that invokes a fear arousal response to eliminate actions that could produce an adverse result or take an action that would prevent a harmful event. The contents of the communication describe an unfavorable event that will occur if the receiver fails to implement the recommendation included in the communication. Communications with a high level of fear arousal are more persuasive than those with a low level of fear arousal. The level of fear arousal is dependent on the value the recipient attaches to the communication, the seriousness of the event, the perceived vulnerability, avoidance importance, and event apprehension.

Protection motivation theorists established a set of variables related to a fear appeal and those actions taken to implement the provided recommendation. Variables associated with a fear appeal include the degree of harm, occurrence probability, and value of the recommendation. Each of the fear appeal variables will produce an associated thoughtful response. The degree of harm will cause the individual to determine

the severity of the fear appeal. An analysis of the occurrence probability will result in determining the expected exposure to harm. A determination of the value of the recommendation will produce a perception regarding the efficacy of the coping response. After developing the thoughtful response to the fear appeal, an attitude change may occur. This attitude change is the protection motivation that affects the individual's intention to implement the recommended response (Rogers, 1975).

The origins of deterrence theory can be found in "the works of classical philosophers such as Thomas Hobbes (1588-1678), Ceasare Beccaria (1738-1794), and Jeremy Bentham (1748-1832)" (Onwudiwe et al., 2004, p. 2). Hobbes (1651/1904) did not define men as either good or bad. Instead, they were viewed as individuals with their feelings who will want things and will fight to obtain them. People are interested in their self-interest that will result in conflict without a governing authority. Because people are rational, the pursuit of self-interest would result in crime and conflict (Onwudiwe et al., 2004). This realization would result in the development of a social contract with the government to avoid crime and conflict (Onwudiwe et al., 2004). It becomes the responsibility of the government to enforce the social contract, but crime will still occur. When crimes do occur, the punishment must exceed the benefits associated with committing a crime. Punishment acts as a deterrent for violations of the social contract to maintain the social contract (Onwudiwe et al., 2004).

Beccaria (1764/1819) elaborated on the concept of the social contract and challenged the right of the government to punish crimes. Because people are rational, committing crimes would not occur if the cost of the punishment exceeds the benefits.

Also if the level of punishment exceeded what was necessary to deter crime, crime would not be reduced (Onwudiwe et al., 2004). The best method of preventing crime was with swift and certain punishment. Beccaria also asserted that laws should be published to inform the people of the purpose and intent of the law.

Bentham (1780/1907) was concerned about the arbitrary administration of punishment and the brutality found in the criminal laws. It is the responsibility of the state to encourage happiness through the use of rewards and punishment. The objective of laws is to increase happiness through increased pleasure and decreased pain in the community. Bentham felt that punishment more than what was necessary to maintain deterrence was unjustified.

The work of Hobbes, Beccaria, and Bentham resulted in the three components of deterrence theory. Any punishment for a crime should have the elements of severity, certainty, and celerity (Onwudiwe et al., 2004). Punishment should be severe enough to keep a rational person from committing a crime. Punishment should be certain because if a person believes punishment will occur, they would be less likely to commit a crime. Swift punishment is also necessary to deter crime. When the punishment is administered close to the time of a criminal act, there is an increased realization that crime does not pay (Onwudiwe et al., 2004).

Straub (1990) used deterrence theory as a theoretical foundation for a study examining the effect of deterrents on computer misuse. Straub and Nance (1990) contended that information technology misuse could be minimized if these activities are detected and punished. A reduction in activities regarding information technology abuse

is related to the use of information system security deterrents (Straub, 1990). In an examination of the prevention of cheating among programming students, Straub, Carlson, and Jones (1993) used deterrence theory as a theoretical foundation. These studies led to the application of deterrence theory constructs to the study of information systems. Siponen et al. (2007) applied the deterrence theory constructs informal sanctions and formal sanctions to a study on information system security policy compliance.

Compliance

Organizations both public and private increasingly rely on information technology. Protection of these information assets has become a concern and a priority for management (Ifinedo, 2014). Information security software methods include virus, malware, spam, phishing, and spyware prevention systems. Hardware security technology measures include firewalls and intrusion protection systems. Implementing all of these measures will not ensure a secure information system (Safa et al., 2016). Information system users are frequently identified as a weak link in information security (Bulgurcu et al., 2010). These users become an internal threat to information security (Ifinedo, 2014). A serious threat to the organization is leaving removable storage unattended and the use of unauthorized applications (Chu & Chau, 2014). Prevention of breaches in information security caused by users is not probable using only technical measures (Wall, Palvia, & Lowry, 2013). Because organizations cannot rely solely on technology to provide adequate security, compliance with information security policies has increased in importance (Kim et al., 2014). Information security policies typically contain management defined principles, requirements, and guidelines. The information

contained in these policies include the acceptable use of information assets, violation consequences, information security responsibilities, and training opportunities (Sommestad, Hallberg, Lundholm, & Bengtsson, 2014). Organizations influence their employees' behaviors through the use of requirements, rules, and guidelines incorporated into information security policies. Although an organization may have put information security policies into practice, employee adherence is not guaranteed (Ifinedo, 2014).

Management has implemented both positive and negative measures to gain compliance to improve information security policy compliance among users. Negative measures are based in criminology where a system of sanctions and penalties are used to prevent information system misuse (Ifinedo, 2014). Positive measures include information security policy training and education to persuade an individual to comply with information security policies through knowledge and awareness. Continuous communication of information security policy reinforces training and improves policy compliance (Puhakainen & Siponen, 2010). Information security policy compliant behavior refers to those activities a user performs to ensure information security is maintained. These information security activities are defined in the organization's information security policies (Padayachee, 2012). Because user behaviors play a role in information security, various behavioral models are used to examine security behaviors.

Scholars who have conducted studies on information security policy compliance behavior have incorporated various social psychological theories. Bulgurcu et al. (2010) suggested that the attitude of the employee is influenced by the benefit and cost of compliance, the cost of noncompliance, and information security awareness. The theory

of planned behavior and rational choice theory are combined to serve as the theoretical foundation for the Bulgurcu et al. study. Attitude, subjective norms, and perceived behavioral control are constructs taken from the theory of planned behavior and were included in the Bulgurcu et al. study. The rational choice theory was previously applied to studies on economic and social behaviors. Based on neo-classical economics, the rational choice theory provides insight into the decision-making process when choices are offered. Puhakainen and Siponen (2010) created a research model incorporating the elaboration likelihood model and universal constructive instructional model to examine the effect of training on information security policy compliance. The universal constructive instructional model includes a framework for developing information security policy compliance training. Complementing the universal constructive instructional model, the elaboration likelihood model assists practitioners with how and why the training is expected to perform. Wall et al. (2013) suggested control-related motivations can explain information security policy compliance behavior. Self-determination theory was used to study intrinsic motivations influencing behavior intention to comply with information security policies. Kim et al. (2014) developed a research model merging planned action theory, rational choice theory, neutralization theory, and protection motivation theory. Constructs from each of the theories were examined to determine both the combined and individual effect on behavioral intention. Ifinedo (2014) combined constructs from the theory of planned behavior, social cognitive theory, and social bond theory. Elements of the social bond theory were hypothesized to influence constructs from the theory of planned behavior in the Ifinedo (2014) study.

Both the constructs from the theory of planned behavior and social cognitive theory would affect information security policy compliance behavioral intention. Crossler, Long, Loraas, and Trinkle (2014) focused on a single theory for their research model. Self-efficacy, response efficacy, and threat severity are constructs from protection motivation theory and were incorporated into a research model examining information security compliance behavioral intention.

Protection Motivation Theory Studies

Rogers (1983) expanded and revised the original protection motivation theory to

- identify additional sources of information that begin the coping process;
- include additional cognitive mediating processes; and
- provide clarification on coping modes.

Original elements of protection motivation theory remain intact and the fear appeal persuasive communication was included as a verbal persuasion source of information.

In addition to the original fear appeal identified as a verbal persuasion, Rogers (1983) included observational learning as an environmental source of information. Observational learning occurs when an individual “sees what happens to others” (Roger, 1983, p. 167). Interpersonal sources of information include personality variables and any previous experience with a similar situation. This previous experience would include a learned response from a prior coping activity. Upon receiving any of the sources of information, an individual would start the cognitive mediating process. Cognitive mediating processes are the central concept of protection motivation theory.

Protection motivation theory cognitive mediating processes include two appraisal methods: threat appraisal and coping appraisal. A threat appraisal includes factors related to a maladaptive response. These factors either increase or decrease the probability of initiating a response. Maladaptive responses are a continuation of the current behavior. Intrinsic and extrinsic rewards increase the probability of a maladaptive response, and the perceived severity and perceived vulnerability to the source of information decreases the probability of a maladaptive response (Rogers, 1983). Contrary to the maladaptive response, the adaptive response is the perception the recommended response is effective. During the coping appraisal process, an individual evaluates his or her ability to respond to the identified threat (Rogers, 1983). Both response efficacy and self-efficacy increase the probability of affecting the adaptive response and the cost associated with the adaptive response decrease the probability of affecting the adaptive response (Rogers, 1983). The result of the threat appraisal and coping appraisal process determines the level of protection motivation. Although there are different methods to measure protection motivation, the best measurement is behavioral intention. When an individual generates a sufficient level of motivation, the behavioral intention is to perform the activities associated with the coping mode (Rogers, 1983).

Rogers (1983) stated that the behavioral intention generated by protection motivation would result in an individual taking some action, or no action. If the decision is to perform an activity to cope with the threat, the activity could involve a single action, repeated single actions, multiple actions, or repeated multiple actions. The purpose of the

source of information is to identify the threat and a persuasion to perform an activity. The persuasion could also be a form of prevention to prevent an activity.

Rogers' (1983) protection motivation theory model of examining the factors affecting the threat appraisal and coping appraisal cognitive processes resulting in a protection motivation behavioral intention serve as the basis of the theoretical foundation for studies examining information security behavior. These information security behavior studies can be categorized into one of three different protection motivation theory model use types. The first type of protection motivation theory model uses all of the constructs of the Rogers' model. The second type of theoretical foundation based on protection motivation theory is a combination of theory constructs. In this theoretical foundation model type, including constructs from other behavioral theories enhance protection motivation theory. Finally, the last theoretical foundation type is a reverse of the second model type. Here a behavioral theory is enhanced by integrating constructs from protection motivation theory.

Six Theory Constructs

Studies conducted by Boss, Galletta, Lowry, Moody, and Polak (2015); Dang-Pham and Pittayachawan (2015); Posey et al (2014); and Vance et al. (2012) developed research models using all six of the protection motivation theory constructs. Although all four studies used all of the protection motivation theory constructs, there were no other similarities among the studies. There were differences in sources of information, research design, and population.

Vance et al. (2012) investigated compliance with information security procedures through the integration of two socio-cognitive theories. Habit theory was integrated with protection motivation theory to explain compliance behavior. In Habit theory, a habit is a type of routine behavior. Vance et al. hypothesized the protection motivation theory constructs perceived threat vulnerability, perceived threat severity, response efficacy, and self-efficacy would positively affect an employee's behavioral intention to comply with information security policy. Protection motivation theory constructs rewards and response cost were hypothesized to negatively affect an employee's behavioral intention to comply with information security policy. Vance et al. further hypothesized habit would positively affect all of the protection motivation theory constructs.

To test the research model, Vance et al. (2012) invited clerical and administrative staff of a Finnish municipal organization to complete a web-based survey. A total of 210 responses to the survey were received and used for data analysis. All survey responses were recorded using an 11-point Likert scale. A one-way ANOVA test was used to evaluate the hypothesized information security policy behavioral intention.

Theoretical model analysis indicated results that differed from the hypotheses. Habit's effect on the protection motivation theory constructs was positive as hypothesized and statistically significant at the $p < 0.01$ level. Perceived threat vulnerability did not have a significant effect on information security policy behavioral intention. Perceived threat severity, rewards, self-efficacy, and response cost affected information security policy behavioral intention as hypothesized. Response efficacy also

had a significant effect on information security policy behavioral intention, but the result was negative instead of positive as hypothesized (Vance et al., 2012).

Posey et al. (2014) examined the perception of information security between information security professionals and organizational insiders. Because information security is important for most organizations and technical information security methods cannot solve behavior problems, understanding user behavior is essential. Posey et al. selected protection motivation theory as the theoretical foundation because of its focus on understanding behavioral intention. Prior research has examined information security adoption behaviors and validated constructs. Posey et al. identified a lack of research conducting a thorough comparison of information security understanding between information security professionals and organizational insiders.

Posey et al. (2014) used a qualitative research method to gather data from study participants. Posey et al. recruited participants from different industries and organizational positions. Interview questions were derived from protection motivation theory and other possible motivators. Posey et al. conducted a total of 33 interviews with 22 organizational insiders and 11 information security professionals as study participants. Each interview lasted approximately 30 minutes. If necessary, follow-up questions were asked to gather more information from the participant. All of the interviews were recorded and professionally transcribed. Qualitative data analysis was performed using the NVivo 8 software program. Common themes within each of the protection motivation theory constructs were identified, coded, and counted for each participant group.

Thematic frequencies for each unique response were calculated for group comparison (Posey et al., 2014).

Posey et al. (2014) found both inconsistencies and consistencies between the two participant groups. Posey et al. identified a major difference between the groups regarding information security protection behavior. This difference could result in organizational information security deficiencies. These deficiencies direct management to include both technical and behavioral elements into their information security environment.

Dang-Pham and Pittayachawan (2015) identified the increased use of mobile devices in a bring your own device (BYOD) environment and the information risk associated with these devices. Insecure BYODs pose a risk to the individual user, wireless service provider, and other wireless service users. A specific risk identified by Dang-Pham and Pittayachawan (2015) was the threat posed by malware. Malware infections can originate on social media, e-mail, and videos. Because of the rise in malware targeting mobile devices, there is a possibility a nonwork related Internet activity can affect work-related activities in a BYOD work environment. Implementation of BYOD policies and antimalware software implementation could mitigate malware infections.

Complying with BYOD security policies and the implementation of antimalware software rely on the behaviors of the user. Dang-Pham and Pittayachawan (2015) conducted a research study focusing on the behavioral intention to implement antimalware software. Dang-Pham and Pittayachawan constructed a research model

based on protection motivation theory to examine the behavioral intention of university students to avoid malware.

Dang-Pham and Pittayachawan (2015) hypothesized the constructs of protection motivation theory would affect behavioral intention to avoid malware on mobile devices. A survey of 56 questions was developed to gather data on malware avoidance behavioral intention to test these hypotheses. A 6-point Likert scale was used to record responses to each question. Dang-Pham and Pittayachawan noted the 6-point Likert scale was used to disallow neutral responses. Students from an Australian university were recruited to participate in the survey. Surveys were distributed both online and in person. A total of 252 responses obtained from both survey distribution methods were used for data analysis. The data analysis method included four steps beginning with exploratory factor analysis, followed by model measurement, structural equation modeling, and ending with hypotheses testing. All of the protection motivation theory hypotheses tested significantly supported the behavioral intention to avoid malware. The effect of perceived rewards was very small, and self-efficacy had a large effect on malware avoidance behavioral intention.

Boss et al. (2015) identified information security violations as a common problem in personal and work surroundings. Information security research has previously conducted studies to find methods to motivate protection of information assets. Protection motivation theory is frequently used in information security research. Boss et al. identified the use of all protection motivation theory constructs in information security research as a gap in the literature. To address this gap, Boss et al. developed a research

model including the central protection motivation theory constructs and the constructs perceived fear and maladaptive rewards. Boss et al. hypothesized the constructs perceived threat severity and perceived threat vulnerability would positively affect perceived fear. Boss et al. also hypothesized that all of the model constructs would affect protection motivation. Maladaptive rewards and response costs would have a negative effect while the remaining constructs would have a positive effect.

Two fear appeal scenarios were developed to test the research model and hypotheses. Each of the fear appeals had a different level of threat severity. Boss et al. (2015) used data loss and mitigation with backups for the low severity fear appeal, and a virus infection message was used for the high severity fear appeal. To validate the effectiveness of the fear appeal, Boss et al. included a control group in the research design. Each threat severity research design produced a research design resulting in two independent studies. Students enrolled in the MBA program were selected for the low severity study. Participants for the high severity study were taken from undergraduate psychology students. Questionnaires were provided to the participants and responses to the statements were recorded on a 7-point Likert scale. The low severity study used 104 participant responses, and the high severity study used 327 participant responses for data analysis (Boss et al., 2015). Confirmatory factor analysis was used for model validity and was supported at the $p < .001$ level. Composite factor reliability scores exceeded the suggested 0.70 level. A comparison of the two severity studies indicated a high fear appeal had twice the influence on motivation intention over the low fear appeal. Construct influence on behavioral intention was mixed. For the high fear appeal model,

all of the constructs had a significant influence on behavioral intention. Some of the constructs in the low fear appeal model had a nonsignificant influence on behavioral intention. These constructs included perceived threat severity, response efficacy, and self-efficacy (Boss et al., 2015).

To better understand how researchers are using protection motivation theory to examine information security compliance behaviors, a brief review of prior studies is discussed. The discussion begins with studies using research models with five protection motivation theory constructs. These studies also had a combination of protection motivation theory constructs and constructs from other theories.

Five Theory Constructs

Research studies using less than the full complement of protection motivation theory constructs as a theoretical foundation comprised a majority of the literature reviewed. The number of protection motivation theory constructs used in the theoretical foundation varied from a high of five to a low of two. Ifinedo (2012); Lee (2011); Meso et al. (2013); Yoon, Hwang, and Kim (2012); and others included five protection motivation theory constructs. Researchers used protection motivation theory constructs either in conjunction with other constructs or no additional constructs.

Crossler and Bélanger (2014) develop a unified measure of security to empirically test the behavioral intention to implement a collection of information security measures using protection motivation theory. The unified measure of security includes multiple information security behaviors to identify a complete view of an individual's security posture. Using a unified measure differs from previous research where only the

behavioral intention to implement a single information security method was measured. Examining an individual information security behavior does not align with the measures people must implement to secure their computer and network infrastructure. This information security behavior necessitated the development of a unified security practices measure that included technical security measures implemented to protect information assets and operational security measures involving the daily information security activities. Examining behavioral intention is a strength of protection motivation theory.

Researchers used protection motivation theory for their theoretical foundation because of its usefulness in understanding the information security decision process. The outcome of this decision-making process is guided by the threat and coping appraisal processes. Within the threat appraisal process is an individual's perceived threat severity and perceived threat vulnerability to the threat. Response efficacy, self-efficacy, and response cost are elements of the coping appraisal process and are the remaining research model constructs. Crossler and Bélanger (2014) hypothesized that perceived threat severity perceived threat vulnerability, response efficacy, and self-efficacy would positively influence the unified security practice. Crossler and Bélanger also hypothesized response cost would negatively influence unified security practices.

Testing of these hypotheses began with the development of a unified security practices instrument. Before deployment of the instrument, it was subject to both a pre-test and pilot test. Once validated, the instrument was placed online, and professionals, students, and small business employees received invitations to participate in the study. Data from a total of 279 responses were used for data analysis. Data analysis was

performed using partial least squares, and the results were used in hypotheses testing. Perceived threat severity, perceived threat vulnerability, response efficacy, and self-efficacy all significantly influenced the unified security practices. Although perceived threat vulnerability significantly influenced unified security practices, the result was in the opposite direction of the hypothesis. Additionally, response cost did not significantly influence unified security practices (Crossler & Bélanger, 2014).

Although Crossler and Bélanger (2014) contended the unified security practices measure would benefit information security practitioners, it is unclear if a broad measure of information security behavior would be beneficial in a normal organization operational environment. Because the unified security practice measure is a broad brush, it may not measure those items associated with an individual's activities. Some security measures may be completely transparent to the user. Two of the items included in the unified security practice were antivirus software and back-ups. In many organizations these activities are transparent to the individual user and including these activities in the measure would not provide an accurate measure of the user's security practice. A multi-activity measure may be beneficial to information security practitioners, but the measure would have to be tailored to the information security environment of the organization.

Crossler et al. (2014) conducted a seminal study investigating the compliance behaviors related to bring your own device (BYOD) policies. Management permitting BYODs should understand the risks to information security and privacy associated with these devices. Crossler et al. used protection motivation theory as a theoretical foundation because of its use in social psychology and information security research. The constructs

perceived threat vulnerability, perceived threat severity, response efficacy, self-efficacy, and response costs were hypothesized to influence both the intention to comply with policies and the actual policy compliance. Including actual policy compliance differs from the established use of protection motivation theory that only includes behavioral intention. Prior studies conducted by Lee (2011) and Ifinedo (2012) augmented protection motivation theory with the inclusion of different behavioral constructs. A nonenhanced protection motivation theory served as the theoretical foundation for the Crossler et al. (2014) study, and no additional behavioral constructs were incorporated into the research model.

Testing of the research model and hypotheses began with submitting invitations to complete online surveys to two different samples. One sample was used to test policy compliance behavioral intention and the other actual policy compliance. Students were used for the policy compliance behavioral intention, and white collar workers were used for the actual policy compliance group. Survey responses included 250 students and 194 white collar workers and were analyzed using descriptive statistics and partial least squares analysis (Crossler et al., 2014).

Demographic descriptive statistics included age, gender, BYOD use experience, and work experience. Construct variable means for each of the group's responses were also provided. Policy behavioral intention hypotheses were analyzed using partial least squares. Results indicated both self-efficacy and response efficacy were positively related to behavioral intention. In contrast, the data did not support a relationship between perceived threat severity, perceived threat vulnerability, and response cost with

behavioral intention. Analysis for actual policy compliance showed support for perceived threat severity, self-efficacy, response efficacy, and response cost. Perceived threat vulnerability did not have a significant contribution to actual policy compliance (Crossler et al., 2014).

Several studies used five protection motivation theory constructs expanded by incorporating additional behavioral constructs. In some research studies, researchers incorporated a single or multiple construct design into the research model. Ifinedo (2012) went a step further by combining constructs from protection motivation theory and the theory of planned behavior into a single research model. Several of these research studies are discussed to understand how researchers incorporated additional constructs into their protection motivation theory research models.

Lee (2011) noted many colleges and universities are trying to deal with Internet plagiarism. Adopting honor codes, promoting awareness, strong enforcement policies, and antiplagiarism software are some of the methods institutions are enacting. One of the issues associated with these measures is the lack of antiplagiarism software adoption. A study was conducted to examine the behaviors affecting this decision to investigate the issue of antiplagiarism software adoption. Lee selected protection motivation theory because of its use investigating factors related to decision making. Lee proposed the faculty members would adopt antiplagiarism software when they perceive Internet plagiarism as a threat, find the software is an effective tool, and are capable of using the software. Lee expanded protection motivation theory for this study by including the effect of behavioral constructs moral obligation and social influence on behavioral

intention. Actual adoption of the antiplagiarism software is also examined as part of the research model. Lee hypothesized the constructs perceived threat severity, perceived threat vulnerability, response efficacy, self-efficacy, moral obligation, and social influence would positively influence the behavioral intention to adopt the antiplagiarism software. Response cost was hypothesized to influence behavioral intention negatively. Behavioral intention was also hypothesized to affect actual adoption, and the behavioral intention to implement antiplagiarism software would be higher than the actual adoption (Lee, 2011).

Testing of the model and hypotheses began by recruiting faculty members from two universities. Data from 218 survey responses were analyzed using partial least squares. Analysis of the data revealed the perceived severity of negative consequences, the probability of plagiarism occurring, software benefits, individual adoption capability, and implementation cost influenced the decision to adopt the antiplagiarism software. Threat appraisals had a strong influence on adoption behavioral intention. With knowledge gained from this study, universities could develop programs to increase the adoption of antiplagiarism software (Lee, 2011).

Yoon et al. (2012) examined the information security behaviors of students using an extended version of protection motivation theory. Subjective norm, a construct from the theory of reasoned action, was incorporated into the research model along with constructs from protection motivation theory. Subjective norm is an individual's action that is influenced by friends and peers. Protection motivation theory constructs included in the research model were perceived threat vulnerability, perceived threat severity,

response efficacy, self-efficacy, and response cost. Yoon et al. hypothesized these constructs would influence information security behavioral intention. Also, Yoon et al. hypothesized information security behavioral intention and security habits would influence actual information security behaviors. Security habits are those routine information security actions an individual develops through repeated action.

Yoon et al. (2012) surveyed students from a Korean university using an instrument recording responses using a 7-point Likert scale. Data gathered from the 202 completed surveys were analyzed using partial least squares methods. Hypotheses testing indicated perceived severity, response efficacy, and self-efficacy were a significant positive influence on behavioral intention. Response cost was also significant but was a negative influence. Perceived vulnerability and subjective norm were positive influences on behavioral intention but were not significant. Lastly, security habit was a significant positive influence on information security behaviors.

Meso et al. (2013) examined information security awareness and behavior of students after completing information security courses. Results from a preliminary survey indicated a 28% increase in information security attack awareness and 18% increase in malware attack awareness. However, the increase students' information security skill was only 8%, and information security behavior improved even less at a 4% increase. These results were motivation to conduct a study, using a theoretical foundation, to compare information security awareness and behavior improvements after course lectures and hands-on projects.

Meso et al. (2013) selected protection motivation theory as the theoretical foundation because of its ability to explain the behavioral intention to perform a protective activity. Threat appraisal protection motivation theory constructs included in the research model were perceived threat severity and perceived threat vulnerability. Coping appraisal protection motivation theory constructs response efficacy, self-efficacy and response cost were also included in the research model. Meso et al. hypothesized lecture knowledge would positively influence perceived threat severity, perceived threat vulnerability, response efficacy, and self-efficacy. Hands-on project experience was hypothesized to have a positive influence on perceived threat severity, perceived threat vulnerability, response efficacy, self-efficacy, and response cost. Perceived threat severity, perceived threat vulnerability, response efficacy, and self-efficacy were hypothesized to influence behavioral intention positively. Response cost was hypothesized to be a negative influence on behavioral intention (Meso et al., 2013).

A web-based survey was used to collect data from students taking an introductory computer course. Two groups of students were used as study participants. One group had only participated in course lectures on information security and the second had attended lectures and completed hands-on projects. Data obtained from the surveys was analyzed using partial least squares-structural equation modeling. Measurement model assessment indicated both reliability and validity as all values exceeded the recommended threshold values. Results from the hypotheses analysis were mixed with several of the hypotheses not supported by the data. Lecture knowledge hypotheses were marginally supported for perceived threat severity and perceived threat vulnerability and not supported for

response efficacy and self-efficacy. Hands-on experience hypotheses were supported for perceived threat vulnerability, response efficacy, self-efficacy, and response cost and not supported for perceived threat severity. Behavioral intention hypotheses perceived severity, response efficacy, and self-efficacy were supported, response cost was marginally supported, and perceived vulnerability was not supported (Meso et al., 2013).

Tsai et al. (2016) examined home computer online information security behaviors using a protection motivation theory as a theoretical foundation. Although researchers have previously examined home computer information security behavior using protection motivation theory, additional constructs were included in the research model. In addition to the protection motivation theory constructs, prior experience, subjective norms, personal responsibility, perceived security support, and habit strength were incorporated into the research model. Tsai et al. hypothesized all of the constructs, except response cost, would positively predict information security behavioral intention. Tsai et al. hypothesized response cost to predict information security behavioral intention negatively.

Tsai et al. (2016) posted a request for 1000 participants on Amazon's Mechanical Turk to test the proposed research model. Each participant receved an incentive of 76 cents at the conclusion of the survey. A total of 988 survey responses was received. Each survey item response was scored on a 5-point Likert scale. A hierarchical regression analysis was performed to test the hypotheses. Regression analyses were performed on three different models. The first model included only the constructs from protection motivation theory. In the second iteration of the model analysis, the constructs prior

experience, subjective norms, personal responsibility, perceived security support, and habit strength were included in the regression analysis. In the final iteration, demographic information was added to the regression analysis. Hypotheses tests revealed perceived threat severity, perceived threat vulnerability, self-efficacy, and perceived security support were not supported by the data. Analysis results of the construct threat severity did produce a significant result, but the result was negative and not positive as hypothesized. The remaining construct hypotheses prior experience, response efficacy, subjective norms, response costs, safety habit, personal responsibility were all supported by the data.

Tsai et al. (2016) took an unusual approach not found in other studies. Participants received an incentive of 76 cents after completing the survey. There was no discussion if this incentive was communicated to the participants before starting the survey. Tsai et al. indicated the institutional review board approved the study. Although providing an incentive could introduce some bias in the results, the amount of money paid may be small enough to avoid the bias problem.

Ifinedo (2012) investigated information security policy compliance with a research model combining the constructs from protection motivation theory and the theory of planned behavior. The research model includes the threat appraisal constructs perceived threat vulnerability and perceived threat severity and the coping appraisal constructs response efficacy, response cost, and self-efficacy from protection motivation theory. Coping appraisal constructs from the theory of planned behavior in the model were self-efficacy, attitude, and subjective norms. One of the constructs, self-efficacy, is

a coping appraisal behavior found in both theories. Ifinedo hypothesized each of these constructs would influence information security policy compliance behavioral intention.

Testing of the research model began by collecting data using two different approaches. In the first approach, noninformation technology managers from InfoCANADA were mailed a cover letter, survey, and a self-addressed, stamped envelope. A total of 68 survey responses was received. A second approach used a sample taken from Information Systems Audit and Control Association (ISACA) members. ISACA members were directed to an online version of the same survey. A total of 56 information technology professionals provided responses. In both cases, participants were encouraged to respond with an offer of four $100 gift certificates and a summary of the research results (Ifinedo, 2012).

Analysis of the data used partial least squares-structural equation modeling. Using this analysis provided an assessment of both the measurement and structural model. Of the seven hypotheses, only two were unsupported by the data. The protection motivation theory constructs perceived threat vulnerability, perceived threat severity, response efficacy, and self-efficacy significantly influenced information security policy compliance behavioral intention. Although the perceived threat severity relationship to information security policy compliance behavior was significant, the influence was negative and not positive as hypothesized. Response cost did not significantly influence information security policy compliance behavioral intention. Both hypotheses related to perceived threat severity and response cost were not supported and were rejected. Hypotheses regarding perceived threat vulnerability, response efficacy, and self-efficacy

were not rejected. The remaining theory of planned behavior constructs, attitude and subjective norms, had a significant influence on information security policy compliance behavior intention and the associated hypotheses were not rejected. (Ifinedo, 2012).

In a similar manner as studies incorporating five protection motivation theory constructs, studies incorporating four protection motivation theory constructs create new research models by incorporating additional behavioral constructs. A few of these research models merge constructs from one or more theories to create a new theoretical foundation. Theories used in combination with protection motivation theory include the theory of planned behavior, the theory of reasoned action, cognitive evaluation theory, and deterrence theory. Some research studies are briefly discussed to develop an understanding of how researchers develop new research models by merging different behavioral theories.

Four Theory Constructs

Researchers including four protection theory constructs eliminated the constructs response cost and reward from their research model. Johnston et al. (2015); Johnston and Warkentin (2010); Siponen et al. (2014); and Yoon and Kim (2013) created research models with four protection motivation theory constructs. Researchers expanded on protection motivation theory by including additional constructs from other theories into their research models.

Johnston and Warkentin (2010) examined the effect of fear appeals on an individual's behavioral intention to comply with an information security recommendation. A fear appeal is an existing external stimulus or threat either perceived

or not perceived by an individual. Communications including a fear appeal induce perceptions that a threat exists, indicates the threat severity, and the individual's threat vulnerability. A fear appeals research model was developed to study the effect of a fear appeal indicating an information security threat and implementation of a security remediation. Constructs from protection motivation theory served as the basis, and a social influence construct was added to the model. Social influence was considered a direct cause of behavioral intention and would contribute to determining the acceptance of a recommended information security remediation. Hypotheses derived from the model indicated the protection motivation constructs perceived threat severity and perceived threat vulnerability would have a negative influence on response efficacy and self-efficacy. Response efficacy, self-efficacy, and social influence would have a positive effect on behavioral intention.

Johnston and Warkentin (2010) developed a research model to test the fear appeals model and examine the effect of a fear appeal on implementing an information security threat mitigation. Because university faculty, staff, and students are vulnerable to spyware, this population was selected for the experiment. A fear appeal treatment communicating the severity and individual vulnerability related to spyware and recommended security mediation was developed. Participants were randomly selected from the population and placed into one of three different groups. The first group served as the experimental group and received a pretest survey, given the fear appeal treatment, and a posttest survey. Group two served as the control group and did not receive the fear appeal treatment. This group was provided both the pretest and posttest surveys. A third

group received the fear appeal treatment and a posttest survey to provide some assertion of testing internal validity (Johnston & Warkentin, 2010).

Results from the structural model analysis indicated support for the fear appeals model, with one exception. The data analysis did not support the hypothesized negative effect of perceived threat vulnerability. This data analysis result had demonstrated an inconsistency regarding protection motivation theory. Other researchers have found users' perception to be one of invulnerability and are less likely to be the target of an attack (Johnston & Warkentin, 2010). Johnston and Warkentin (2010) suggested a fear appeal should strongly indicate the probability of a security attack and the negative consequences to counter the perception of invulnerability.

Yoon and Kim (2013) developed a unique research model incorporating constructs from different theoretical foundations. Constructs from the theory of reasoned action were combined with protection motivation theory to examine information security behavioral intentions. Yoon and Kim hypothesized the constructs from protection motivation theory perceived threat severity, perceived threat vulnerability, response efficacy, and self-efficacy would influence attitude. Constructs moral obligation, organizational and subjective norms taken from the theory of reasoned action along with attitude were hypothesized to influence information security behavioral intention.

Yoon and Kim (2013) collected data from graduate business students employed in Korean companies. An e-mail invitation to the web-based survey was distributed to the participants. Responses from 162 surveys were used in the data analysis. The analysis was performed using partial least squares. Yoon and Kim noted using this approach was

well suited for complex models with latent variables and has minimal sample size requirements. Hypotheses testing indicated subjective norm, attitude, and moral obligation had a significant influence on behavioral intentions. In contrast, subjective norm did not have a significant influence on behavioral intentions. Three of the protection motivation theory constructs, perceived severity, response efficacy, and self-efficacy significantly influenced attitude. Perceived vulnerability did not have a significant influence on attitude.

Siponen et al. (2014) studied information security policy compliance behavior using a new research model. Siponen et al. combined the constructs from protection motivation theory, the theory of reasoned action, and the cognitive evaluation theory into a theoretical foundation. Protection motivation theory constructs perceived threat severity, perceived threat vulnerability, response efficacy, and self-efficacy were hypothesized to influence behavioral intention to comply with information security policies. The theory of reasoned action constructs attitude and normative beliefs were hypothesized to influence behavioral intention to comply with information security policies. The rewards construct taken from cognitive evaluation theory was also hypothesized to influence behavioral intention to comply with information security policies. Lastly, Siponen et al. hypothesized that behavioral intention would influence actual information security policy compliance.

Employees from Finnish companies served as the population for this research study. An invitation to complete an online survey was given to 2892 respondents. A total of 669 completed responses were analyzed and tested using structural equation modeling.

All of the construct variables, except response efficacy and rewards, had a significant contribution to the behavioral intention to comply with information security policies. Siponen et al. (2014) identified normative beliefs as having a highly significant affect on information security policy compliance intention. Response efficacy and rewards did not significantly influence the behavioral intention to comply with information security policies. Behavioral intention to comply with information security policies had a highly significant effect on actual information security policy compliance (Siponen et al., 2014).

Johnston et al. (2015) contended the typical fear appeal and protection motivation theory framework is deficient when used for information security research. An enhanced research framework integrating constructs from protection motivation theory and deterrence theory was proposed to address this deficiency. This framework expands on the work of Johnston and Warkentin (2010) and incorporates the constructs formal sanction certainty, formal sanction severity, informal sanction certainty, informal sanction severity, and sanction celerity (Johnston et al., 2015). The new model also includes additional protection motivation theory construct relationships not included in the Johnston and Warkentin (2010) research model. Johnston et al. suggested formal sanctions will have a different effect on compliance intention than informal sanctions.

Johnston et al. (2015) used a sequential mixed-methods research design to test the newly created research model. The quantitative portion of the research study incorporated an experimental and control group posttest-only research design with randomized participant selection. Only the experimental group received the fear appeal treatment, and both groups received the survey. Interviews with organizational managers were used for

the qualitative portion of the research study. Employees of a Finish municipal government served as the study population.

Data collection began by inviting 2,475 employees to participate in the study. A total of 559 employees indicated a willingness to participate and were randomly assigned to the experimental and control groups. Participants received an online web-based survey. A multi-stage data analysis was performed using structured equation modeling. The first stage data analysis included only the control variables. Protection motivation theory constructs were added for the second stage data analysis, and deterrence theory constructs were added for the third stage data analysis (Johnston et al., 2015). Because of the complexity of the model and the number of data analysis stages, only those constructs with insignificant results are presented for this discussion. Perceived threat vulnerability from protection motivation theory and formal sanction severity, formal sanction certainty, and sanction celerity results were not significant.

Three and Fewer Theory Constructs

The next set of research studies incorporating protection motivation theory constructs included a smaller subset of the constructs. Safa et al. (2015) and Tu, Turel, Yuan, and Archer (2015) included three protection motivation theory constructs and constructs from other theories for their research model. Menard, Gatlin, and Warkentin (2014) used a research model comprised of two protection motivation theory constructs and two convenience constructs to examine the behavioral intention to use a cloud-based backup. Research studies integrating three or two protection motivation theory constructs could be considered hybrid models because these models include an equal number of

constructs from protection motivation theory and the second set of theoretical constructs. It is unclear if these models should be considered protection motivation theory research models because they include only half, or less, of the total protection motivation theory constructs. Examples of these equally balanced construct models are presented to understand how these model types are used in information security behavior studies.

Safa et al. (2015) contended technology alone could not provide a secure information system environment. In addition to technology, the human element related to information security should be understood. Safa et al. developed a research model and included constructs from the theory of planned behavior and protection motivation theory to examine the attitude toward having an information security environment. Safa et al. hypothesized the protection motivation theory threat appraisal constructs perceived threat vulnerability and perceived threat severity would positively affect information security behavioral intention. Self-efficacy related to information security activities would also have a positive effect on information security behavioral intention. Constructs from the theory of planned behavior hypothesized to affect information security behavior included in the research model were attitude, subjective norms, and perceived behavioral control. Safa et al. also hypothesized that information security awareness would affect attitude, the organizational policy would affect subjective norms, and experience would affect perceived behavioral control. Testing of the research model began with collecting data from study participants.

Safa et al. (2015) developed a survey to measure each construct in the research model. The questionnaire included 43 questions and responses were recorded on a 5-

point Likert scale. Participants for the research study were selected from information security and information technology professionals employed in Malaysian companies. At the conclusion of the survey process, responses from 212 completed questionnaires were statistically analyzed. Confirmatory factor analysis was used to test the variable measurements. Structural equation modeling was used to test the research model and hypotheses. All hypotheses, except one hypothesis, significantly contributed to the information security behavioral intention. Perceived behavioral control did not significantly affect information security behavioral intention, and its hypothesis was rejected.

Tu et al. (2015) developed a research model integrating the constructs from protection motivation theory and social learning theory to examine coping intentions related to the loss or theft of a mobile device. One of the threat appraisal protection motivation theory constructs, perceived threat, was hypothesized to influence coping intentions positively. Protection motivation theory coping appraisal constructs self-efficacy and self-efficacy were hypothesized to influence coping intention positively. Sources of information used for protection motivation theory constructs were taken from social learning theory. Response knowledge was hypothesized to influence self-efficacy and response efficacy positively. Threat experience was hypothesized to have a positive effect on perceived threat. Social influence was hypothesized to have a positive influence on response knowledge, perceived threat, and coping intentions. Tu et al. contended the various environmental exposures to information regarding the loss of theft of a mobile device is a source of information. Rogers (1983) established these sources of information

as the initiator of the cognitive threat appraisal and coping appraisal processes. Tu et al. identified knowledge of information security measures, prior loss of theft experience, and social influence as sources of information.

To test their hypotheses and research model, Tu et al. (2015) engaged the services of a survey company to administer an online survey. A total of 339 completed responses were used for data analysis. Confirmatory factor analysis was used to determine model fit. Although the model was aligned with the data, the result was not significant. Covariance-based structural equation modeling was used to test the hypotheses. The data significantly supported all tested hypotheses. The research model explained coping intention variance of 59%.

Tu et al. (2015) took an unusual approach to the development of their research model. In Rogers' (1983) expanded and revised version of protection motivation theory, the threat appraisal process included the constructs perceived threat severity, perceived threat vulnerability, and response cost. Tu et al. combined perceived threat severity and perceived threat vulnerability into a single construct, perceived threat. Tu et al. acknowledged previous research supported the use of perceived threat severity and perceived threat vulnerability to examine behavioral intention but provided no explanation for the combining of constructs. By combining two constructs into one, some level of granularity in the analysis is lost.

Menard et al. (2014) identified data loss as a threat to data availability. Availability is a component of the security triad defined by the protection, integrity, and availability of information assets. The use of a cloud-based data backup solution was

suggested to mitigate this risk. However, it is unclear if the automatic nature or convenience of a backup solution affects the implementation decision. To examine the effect of a user's perception on the behavioral intention to implement a cloud-based data backup solution, Menard et al. developed a research model based on protection motivation theory and convenience factors. The constructs perceived threat severity and perceived threat vulnerability from protection motivation theory were used to examine the threat appraisal component of the research model. Menard et al. excluded the protection motivation theory constructs response efficacy and self-efficacy because their effect would be minimal. Ease of use of the cloud-based data backup was given as the reason for their exclusion. Perceived automaticity and perceived concurrency were the constructs used to examine the convenience factors. Perceived automaticity is the belief a user has about how easy the cloud-based data backup is to use. Perceived concurrency is the belief the cloud base data backup will make the data available to all user devices.

University students were invited to participate in a research survey to test the hypotheses that the four constructs would positively affect a cloud-based data backup implementation. A total of 152 responses were used for data analysis. Partial least squares-structural equation modeling analysis was used to test the hypotheses. The data supported all four hypotheses, but the dependent variable variance explained by the model was .091, lower than expected (Menard et al., 2014).

Theoretical Foundation Expansion

The final category of research model is the expansion of behavioral theory by integrating protection motivation theory constructs. In this example, neutralization theory

is expanded by integrating constructs from multiple theories. Kim, Yang, and Park (2014) take a unique approach to their development of a research model by integrating constructs from four theoretical foundations. Planned action theory, rational choice theory, neutralization theory, and protection motivation theory are combined to explain the behavioral intention to comply with information security policies. Neutralization theory constructs denial of responsibility, denial of injury, condemnation, metaphor of ledger, appeal to loyalty, defense of necessity, and defense of ubiquity are hypothesized to influence behavioral intention. Rational choice constructs benefit of compliance, cost of compliance, and cost of noncompliance are hypothesized to influence an individual's attitude. From planned action theory attitude and subjective norms are hypothesized to influence behavioral intention. Lastly, self-efficacy and response efficacy constructs from protection motivation theory are hypothesized to influence behavioral intention.

Researchers visited randomly selected companies, presented the study's intentions and selected a few individuals from different organizational levels in the company. Each participant was provided a survey to gather responses regarding the behavioral intention to comply with information security policies. A total of 194 completed surveys were used for data analysis. Variable reliability and validity testing were performed using structural equation model analysis. Partial least squares analysis was used for reliability, validity, and hypotheses testing. Results of the hypotheses testing were mixed with the rejection of self-efficacy as an indicator of behavioral intention (Kim et al., 2014).

Although the study was described as a combination of four theories, not all of the constructs from all four theories were included in the research model. Only two of the

protection motivation theory constructs were included in the research model. A key element of protection motivation theory is the use of a fear appeal or source of information. A source of information was not included as part of the research model. An augmented neutralization theory model may be a better description of the theoretical foundation. Also, all of the neutralization techniques were combined into one hypothesis and not individually tested.

Sources of Information

In his seminal work examining fear appeals and developing protection motivation theory, Rogers (1975) stated that a persuasive communication containing the fear appeal would initiate the cognitive mediating process of evaluating and acting on the information in the communication. Rogers (1983) expanded on the fear appeal initiator of the cognitive mediating process by defining sources of information that would be the initiators of the cognitive mediating process. These sources of information would include verbal persuasion, observational learning, personality variables, and prior experience. Rogers included a fear appeal as a verbal persuasion. Although a source of information is necessary to begin the cognitive mediating process, not all of the research studies found in the literature define their sources of information.

Tu et al. (2015) provide a detailed discussion on sources of information in their study of mobile device loss or theft. Some examples of sources of information are presented and discussed. These include prior experience, social influence, verbal persuasion, and observational learning. Although a source of information is necessary for a cognitive mediating process to begin, some researchers use the original fear appeal

concept. Johnston and Warkentin (2010) use a fear appeal in their study of information security behaviors. A message communicating the effect, probability, and recommended remediation of spyware were provided to the survey participants at the start of the survey. Boss et al. (2015) expanded the use of fear appeal by developing a high and low fear appeal treatment. By having two levels of fear appeal, an analysis of the more effective fear appeal is possible. Johnston et al. (2015) incorporated two different fear appeals, one regarding password theft and another on USB theft, into their examination of the effectiveness of sanctions on behavioral intention. Another common element of these studies is their use of an experimental or quasi-experimental research design and the use of a control group.

Most research studies using a nonexperimental correlational research design did not specify a source of information as the initiator of the cognitive mediating process. Lee (2011); Ifinedo (2012); and Yoon et al. (2012) discuss different possible sources of information that would initiate the cognitive mediating process. Other researchers identified a specific source of information in their nonexperimental correlational studies. Vance et al. (2012) identified habit as the source of information used to initiate the cognitive mediating process. Meso et al. (2013) use information security course lectures and information security hands on projects as the source of information.

When conducting a research study using protection motivation theory as the theoretical foundation, defining a source of information is important to establishing the initiator of the cognitive mediating process. Articles found in the literature using a nonexperimental correlation research design seem to place less emphasis on defining the

source of information. Those studies using an experimental or quasi-experimental research design, defining the source of information is critical. In these studies, the source of information becomes the treatment provided to the experimental group. Using two groups in a study allows me to test the effectiveness of the treatment used in the study.

Study Results

Research studies found in the literature using protection motivation theory as their theoretical foundation incorporated from six to two of the protection motivation theory constructs. Because many of the protection motivation theory research models developed for these studies are unique, making a direct comparison of the results was difficult. Frequently constructs from different theories are incorporated along with protection motivation theory to develop a research model. Performing a side by side comparison would leave some gaps when one construct is present in one research model but not in the other.

Only protection motivation theory constructs used in the research model will be compared to facilitate a comparison of results. Also, studies will be grouped by the number of common protection motivation theory constructs used in the research model to permit a more direct comparison of results. This technique was also used in the prior discussion of study reviews. For this discussion, only the results from studies using six, five, or four protection motivation theory constructs will be included in the comparisons. Research studies using three or fewer constructs will be removed from the comparison because these studies either combine constructs or the protection motivation theory constructs are used to enhance another theoretical foundation.

Studies conducted by Boss et al. (2015); Dang-Pham and Pittayachawan (2015); Posey et al. (2014); and Vance et al. (2012) all included six protection motivation theory constructs. Because the Posey et al. (2014) study was qualitative, the study will not be included in the results comparison. The hypotheses for the remaining three quantitative studies were similar. Perceived threat vulnerability, perceived threat severity, response efficacy, and self-efficacy were all hypothesized to have a positive influence on behavioral intention. Rewards and response cost were hypothesized to have a negative influence on behavioral intention. A comparison of the results was mixed. Perceived threat vulnerability was not significant for all three studies. Response cost was significant for all studies. For the remaining protection motivation theory constructs, there was no agreement on the significance of the results.

Studies using five of the protection motivation theory constructs included studies by Crossler and Bélanger (2014); Crossler et al. (2014); Ifinedo (2012); Lee (2011); Meso et al. (2013); Tsai et al. (2016); and Yoon et al. (2012). All of the studies included the same protection motivation theory constructs and excluded the construct rewards. Hypotheses for all of the constructs were similar for all studies. Perceived threat vulnerability, perceived threat severity, response efficacy, and self-efficacy were hypothesized to have a positive effect on behavioral intention. Response cost was hypothesized to have a negative effect on behavioral intention. Only the response efficacy result was significant for all studies. For the remaining studies, the results were mixed. Examining the results for a common results trend found self-efficacy to be significant for all but one study. Other constructs had mixed significant and

nonsignificant results. Siponen et al. (2014) used a research model with five constructs but used a different model structure. The construct reward was included in the research model, and response cost was excluded. Because the Siponen et al. study was the only study using this research model form, it was excluded from the results comparison.

Johnston and Warkentin (2010); Yoon and Kim (2013); and Johnson et al. (2015) used a research model including four protection motivation theory constructs. Both rewards and resource costs were excluded from the research model. Johnston and Warkentin (2010) developed a unique research model, and two of the constructs were not hypothesized to influence behavioral intention and was excluded from the results comparison. Studies by Yoon and Kim (2013) and Johnson et al. had similar results. Perceived threat vulnerability was not significant for both studies. Perceived threat vulnerability, response efficacy, and self-efficacy results were significant for both studies.

Protection Motivation Theory Review

Protection motivation theory has been widely applied to the problem of information security compliance. Research models using constructs from protection motivation theory have various formulations. Research models have integrated from six to two protection motivation theory constructs. Constructs from multiple theoretical foundations have been integrated with protection motivation to create unique theoretical foundations. These new theoretical foundations served as the research models used to examine information security compliance behavioral intention. Because of the uniqueness of the research models, a comparison of results was difficult. Studies were grouped by

common constructs to facilitate a comparison of protection motivation theory studies. A common grouping permitted a comparison of studies using similar research models. Although there were some result commonalities among some studies, the differing results can be motivation for additional protection motivation theory studies.

Deterrence Theory Studies

Deterrence theory is based on the premise that before an individual decides to commit a crime, a risk-benefit analysis is conducted. If the benefits are greater than the risks, then the decision is to commit the crime (Johnston et al., 2015). When deciding to commit a crime if the person believes there is a high risk of getting caught, the punishment is severe (Siponen & Vance, 2010), and the punishment will be quick the motivation to commit the crime is diminished (Johnston et al., 2015). Deterrence theory has been applied to information security research because of the relevance of perceived sanction severity and perceived sanction certainty (D'Arcy & Devaraj, 2012). Siponen and Vance (2010) suggested the detection and punishment of computer violations will minimize the occurrence of computer abuse. Because of its relevance to information security research, studies examining information security compliance behavioral intention have incorporated deterrence theory constructs into their research models.

Siponen and Vance (2010) stated information security policy noncompliance is a problem for information system managers. Constructs from neutralization theory were merged with constructs from deterrence theory to examine the problem of information security policy noncompliance. Although prior research examining information security policy noncompliance has used deterrence theory as a theoretical foundation,

neutralization theory has not been used in these types of studies. Both deterrence theory and neutralization theory are taken from the field of criminology. Neutralization theory indicates individuals who violate the rules use the excuse an activity did no harm to justify their actions. Constructs from neutralization theory include theory defense of necessity, appeal to higher loyalties, condemn the condemners, metaphor of the ledger, denial of injury, and denial of responsibility were incorporated into the research model. Details on neutralization theory are discussed in a separate section of the literature review. Siponen and Vance (2010) included the deterrence theory constructs formal sanctions, informal sanctions, and shame in their research model. Siponen and Vance hypothesized neutralization, a combination of the six neutralization theory constructs, would have a positive effect on information security policy violation behavioral intention and the three deterrence theory constructs would negatively affect information security policy violation behavioral intention.

Data collection began with the development of an instrument based on prior validated instruments. Responses to the survey items were recorded on an eleven-point scale. Participants were selected from a population of organizations in Finland. Surveys were distributed to the participants, and 1449 responses were received. Theoretical model and hypotheses tests were performed using partial least squares-structural equation modeling. Hypotheses tests began with the deterrence theory constructs, and only informal sanctions had a significant effect on information security policy violation behavioral intention. In the second phase of hypotheses testing, neutralization constructs were incorporated and had a significantly strong effect on information security policy

violation behavioral intention. However, when the neutralization constructs were added to the analysis, the deterrence theory constructs were not significant.

Son (2011) identified an organization's employees as the weakest link in information security. Information security policy violations such as not changing a password or not logging off a computer put the organization at risk. Because deterrent certainty and deterrent severity have been identified as effective methods to prevent information asset misuse, deterrence theory was selected as the theoretical foundation to examine information security policy compliance behavioral intention. Deterrence theory constructs were categorized as either extrinsic or intrinsic motivation models. In the extrinsic motivation model are the constructs perceived deterrent certainty and perceived deterrent severity. Perceived legitimacy and perceived value congruence are part of the intrinsic motivation model. Son (2011) hypothesized all four of the deterrence theory constructs would have a positive effect on information security policy compliance behavioral intention.

To test the research model and hypotheses, Son (2011) used full-time employees as the target population. Panel members from a professional data collection company were used to gather the study sample. Invitations to participate in the study were sent to 2000 panel members using e-mail. Included in the e-mail was a link to an online web-based survey. Responses to the survey were recorded using a 7-point Likert scale. A total of 602 completed surveys were used in the study data analysis. Partial least squares-structural equation modeling was used for data analysis to validate the measurements and test research model. Son's (2011) analysis of the results indicated significant support for

the hypotheses related to perceived legitimacy and perceived value congruence. However, the hypotheses perceived deterrent certainty and perceived deterrent severity did not significantly support information security policy compliance.

Chen, Ramamurthy, and Wen (2013) identified information security policy compliance as a priority for information security management. Management strategies for ensuring information security compliance have included both negative and positive measures for enforcement. Management supporting a negative strategy suggests punishment for information security policy violations. Deterrence theory suggests that an increase in punishment and severity will discourage unwanted behaviors. Management advocating for a positive strategy use a reward as an incentive for information security policy compliance. Organizational theories include a reward as motivation to reinforce information security policy compliance positively. Finally, an argument could be made that both a reward and punishment could affect the cost-benefit decision an individual makes before performing a noncompliance behavior.

Chen et al. (2013) identified a gap in the literature examining the effects of two information security compliance enforcement strategies. To examine how incorporating both a negative and positive enforcement strategy would affect information security compliance, a research model incorporating these elements was developed. Chen et al. hypothesized punishment for noncompliance would have a positive effect on information security compliance, a reward for compliance would have a positive effect on information security compliance, and certainty of control would have a positive effect on information security compliance. Chen et al. also hypothesized that the certainty of

control would moderate the effect of both punishment and reward and reward moderates the effect of punishment. Participants were asked to review the policies related to four different scenarios and answer a series of questions to test the research model.

Chen et al. (2013) recruited employees from two mid-west companies to participate in the study. Using a web-based system, participants read each of the four information security policy questions and provide responses to the survey questions. Responses to the scenarios questions were recorded using a 7-point Likert scale. Several control variables were included in the survey. Organizational security culture responses were recorded using an 8-point Likert scale. Information security policy and information security training questions were recorded using a 4-point Likert scale. Responses related to security monitoring questions were scored using a 7-point Likert scale (Chen et al., 2013).

Data analysis began with exploratory factor analysis to test for model validity. Testing of the hypotheses used a one-way ANOVA. Because the study also examined the interaction of the independent variables, three one-way ANOVA analyses were performed. Analysis of the results indicated the severity of punishment, the significance of reward, and certainty of control all significantly contributed to information security policy compliance. These results also found severity of punishment and certainty of punishment acted as a deterrence to information security policy violations (Chen et al., 2013).

D'Arcy and Devaraj (2012) acknowledged that employees pose a significant risk to information technology security. Because deterrence theory has played an important

role in technology misuse research, deterrence theory was selected as the theoretical foundation for the study. D'Arcy and Devaraj suggested the deterrence theory constructs perceived certainty of sanctions and perceived severity of sanctions, along with informal sanctions and employment context would influence an individual's intention to misuse information technology. D'Arcy and Devaraj also investigated the relationship between formal and informal sanctions. A two-level research model was used to examine the influence of these constructs on intention to misuse information technology. The model is composed using three categories of constructs, formal sanction, informal sanctions, and employment context. Included in the formal sanctions category are perceived certainty of sanctions and perceived severity of sanctions. Social desirability pressure and moral beliefs comprise the informal sanctions category. Employment context includes virtual status and employment level constructs. A survey was developed and distributed to computer users in the United States to test the research model.

D'Arcy and Devaraj (2012) selected a sample of participants from a population of individuals using computers on a daily basis. Two groups of participants were used in the sample. The first group included employees from organizations in the United States and the second group was employed individuals participating in an evening MBA program. D'Arcy and Devaraj suggested using the employee participants would reduce the possible bias in the MBA responses. Invitations were extended to 600 employees, and 228 completed responses were received. Surveys were distributed in class to 273 MBA students and 183 completed responses were received. Responses from the survey were analyzed using partial least squares and covariance-based structural equation modeling.

Analysis of the results demonstrated model reliability and the hypotheses all indicated a significant influence on intention to misuse information technology. A goodness of fit test value of 0.54 exceeded the cutoff value of 0.36. Examining the relationship between formal and informal sanctions demonstrated both formal sanctions and informal sanctions had a direct and indirect significant effect on intention to misuse information technology (D'Arcy & Devaraj, 2012).

Because culture has an influential effect on attitude and behavior, Hovav and D'Arcy (2012) examined information technology misuse behavior between the United States and South Korean cultures. An extended version of deterrence theory was used as the theoretical foundation for the research study. Deterrence theory was augmented with information security countermeasures and cultural constructs. Prior studies found information security countermeasures influenced information system misuse behavior. These security countermeasures included both procedural and technical countermeasure constructs. Cultural constructs included power distance, individualism/collectivism, uncertainty avoidance, and long-term orientation. The deterrence theory construct, moral belief, was used as an informal sanction and perceived certainty of sanctions and perceived severity of sanctions were used as formal sanctions. Age and gender were used as social status constructs. Hovav and D'Arcy (2012) hypothesized procedural and technical countermeasures would have a positive influence on moral beliefs, perceived certainty of sanctions, and perceived severity of sanctions. Hovav and D'Arcy also hypothesized the influence would be greater for individuals from the United States than from South Korea. Formal sanctions, informal sanctions, and social status were

hypothesized to influence information technology misuse intention, and the effect would be greater for individuals from the United States than from South Korea.

Two samples were taken from part-time MBA students and company employees. One sample was taken from United States organizations and the second from South Korean organizations. For the United States sample, 269 completed responses were received from employees and 97 completed responses were received from part-time MBA students. For the South Korean sample, 145 usable responses were received from employees and 215 completed responses were received from MBA students (Hovav & D'Arcy, 2012). Hovav and D'Arcy noted the response rates from both countries were similar.

Hovav and D'Arcy (2012) conducted an analysis of the response data using partial least squares-structural equation modeling. Testing model convergent validity resulted in a value of 0.7 and exceeded the recommended value of 0.5. A multicollinearity test produced a result less than 2.2 for both samples and was below the 3.0 cutoff value. Hypotheses testing for the United States and South Korean samples were performed separately. There were significant statistical differences between perceived certainty of sanctions and perceived severity of sanctions between the two cultures. The perceived certainty of sanctions was stronger for the South Korean sample, and perceived severity of sanctions was stronger for the United States sample. Their combined influence on information technology misuse intention was greater for the South Korean sample but was not statistically significant. The effect of countermeasures was also greater for the South Korean sample but was not statistically significant. Because

perceived certainty of sanctions had a greater influence on information technology misuse intention with the South Korean sample and perceived severity of sanctions had a greater influence on information technology misuse intention with the United States sample, Hovav and D'Arcy (2012) contended that deterrence theory is culturally biased.

Cheng et al. (2013) found that prior research into information security compliance behavior failed to include participants from China. A theoretical model incorporating social control and deterrence theory was developed to examine the behaviors of Chinese employees to address this gap. Because an organization is considered a social group, Cheng et al. contended social control constructs apply to an organization. Social control in organizations is represented by policies the organization enact to discourage improper behaviors. Formal controls from deterrence theory serve to discourage behaviors through the use of sanctions.

Constructs used to develop the research model fall into either the formal control or information control categories. The deterrence theory constructs perceived certainty of sanctions and perceived severity of sanctions were included as formal controls. Social bond constructs include attachment, commitment, involvement, and belief. Subjective norm and co-worker behavior are social pressure constructs and are also informal controls (Cheng et al., 2013). Cheng et al. (2013) hypothesized all of the constructs, with the exception of co-worker behavior, would have a negative influence on the intention to violate information security policy. Co-worker behavior was hypothesized to have a positive influence on the intention to violate information security policy. Surveys were distributed on paper and through an online web-site to test the research model. Paper

surveys were distributed to Chinese employees and 87 completed responses were received. Invitations were e-mail through a professional survey website to 300 employees. A sample of 185 completed online surveys was included with the hard copy responses for data analysis.

To test both the measurement model and the structural model, Cheng et al. (2013) selected partial least squares-structural equation model analysis. Reliability testing scores for all constructs exceeded the recommended 0.7 level. Model validity tests exceed the 0.5 level, and construct correlations were lower than the 0.9 threshold. Structural model testing produced a result of 75.2% explanation of the variance related to the intention to violate information security policy. Hypotheses analysis indicated perceived severity of sanctions, attachment to job, attachment to the organization, commitment, belief, and subjective norm had a statistically significant negative relationship with the intention to violate information security policy. Co-worker behavior had a statistically significant negative relationship with the intention to violate information security policy. These results supported seven of the 11 hypotheses. The remaining four hypotheses related to perceived certainty of sanctions, attachment to immediate supervisor, attachment to co-workers, and involvement did not have a statistically significant relationship with the intention to violate information security policy.

Cheng, Li, Zhai, and Smyth (2014) conducted a study to examine the behavioral intention of an individual to use the Internet for personal purposes while at work. A research model incorporating deterrence theory constructs into neutralization theory was developed to examine this behavior. Cheng et al. hypothesized neutralization techniques

would have a positive effect on a person's behavioral intention to use the Internet for personal purposes while at work. These neutralization techniques include denial of responsibility, denial of injury, denial of victim, condemnation of condemner's, and appeal to higher loyalties. Deterrence theory constructs perceived severity of sanction and perceived certainty of sanction would have a negative influence, and perceived benefits will have a positive influence on a person's behavioral intention to use the Internet for personal purposes while at work.

A sample was selected from an organization's employees to test this model. These organizations also had Internet use policies stating no personal use of the Internet is permitted. Participants were invited to participate in the study either by receiving a paper survey or an e-mail with a link to the survey. A total of 230 completed surveys were received, 118 from the paper survey and 112 from the online survey. Responses to the survey were recorded using a 7-point Likert scale (Cheng et al., 2014).

Cheng et al. (2014) used partial least squares-structural equation modeling to analyze the measurement scales and test the hypotheses. Reliability results of the latent variables exceeded the 0.7 threshold and construct validity exceeded the 0.5 threshold. All construct validities were less than the 0.9 threshold. The model explained 65% of the variance of a person's behavioral intention to use the Internet for personal purposes while at work. Both neutralization and perceived benefits had a positive effect on a person's behavioral intention to use the Internet for personal purposes while at work. The perceived certainty of sanction was negatively related to a person's behavioral intention to use the Internet for personal purposes while at work. Contrary to the original

hypothesis, perceived severity of sanction did not have a significant relationship with a person's behavioral intention to use the Internet for personal purposes while at work.

Results Comparison

In a review of the literature regarding the use of deterrence theory to examine information system security behavior, D'Arcy and Herath (2011) found "inconsistent and sometimes contradictory findings" (p. 656). This inconsistency was also found in the results of the studies previously discussed in the literature review. First, there was a lack of commonality among the studies regarding deterrence theory constructs used in the research model. Constructs of deterrence theory include severity, certainty, and celerity of sanction (Onwudiwe et al., 2004). Only the study by Johnston, Warkentin, and Siponen (2015) included sanction severity, sanction certainty, and sanction celerity. For the remaining studies, research models included the deterrence theory constructs sanction severity, sanction certainty, or a construct combining both sanction severity and sanction certainty. Siponen and Vance (2010) used the combined deterrence theory construct sanction and divided the sanction into formal and informal sanctions. Results of the study indicated both constructs did not introduce a statistically significant influence on information security policy violation. D'Arcy and Devaraj (2012) used the combined deterrence theory construct formal sanction in a study examining information technology misuse. The combined construct resulted in formal sanction having a significant influence on information technology misuse.; Cheng et al. (2013); Cheng et al. (2014); and Hovav and D'Arcy (2012) included perceived sanction certainty and perceived sanction severity in their research models examining information security violation. Results were

inconsistent with perceived sanction certainty and had a significant effect for Cheng et al. (2014) and a nonsignificant effect for Hovav and D'Arcy and Cheng et al. (2013). Perceived sanction severity had a significant effect for Hovav and D'Arcy and Cheng et al. (2013) and a nonsignificant effect for Cheng et al. (2014). Son (2011) and Johnston, Warkentin, and Siponen (2015) hypothesized the deterrent theory constructs would have a positive effect on compliance but the manner in which there were used differed between the two studies. Son used perceived sanction certainty and perceived sanction severity and found them both had a nonsignificant effect on compliance. Johnston et al. divided sanction severity and sanction certainty into formal and informal sanctions. Only the informal sanctions had a significant result, and formal sanctions had a nonsignificant result. The third deterrence theory construct, sanction celerity was also nonsignificant. Another issue regarding the results comparison was the formulation of the hypotheses. Some studies examined compliance while others examined violations. Studies examining violations with deterrence theory constructs would have a negative influence (Siponen & Vance, 2010) and hypotheses regarding compliance would have a positive influence (Son, 2011).

Deterrence Theory Review

Deterrence theory is another behavioral theory used in studies examining information security compliance behavioral intention. Because deterrence theory originated in the field of criminology, studies reviewed from the literature examine the effect of sanctions on information security compliance behavioral intention. Several studies were briefly discussed to demonstrate how researchers used deterrence theory as a

theoretical foundation. Most of the studies reviewed created a unique research model using the constructs from deterrence theory and other behavioral constructs. These studies also differed in their hypotheses. Some studies examined the positive effect on compliance, others the negative effect on violations. Because of these differences, a direct comparison of results was open to interpretation on how to compare construct results. A review of the results did indicate mixed outcomes for those studies using the same constructs. Mixed results in the studies provide an opportunity for future research studies.

Neutralization Theory

Neutralization theory is based on the concept that people who obey the law and those who break the law "believe in the norms and values of the community in general" (Siponen & Vance, 2010, p. 489). When an individual decides to break the law or engage in antisocial behavior, using neutralization techniques allows them to perform the action. When someone uses neutralization techniques, they dismiss norms by justifying their improper behavior. In their seminal work on neutralization theory, Sykes and Matza (1957) proposed denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners, and appeal to higher loyalties as neutralization techniques. Later neutralization techniques were expanded when Klockars (1974) included metaphor of the ledger and Minor (1981) contributed the defense of the necessity.

In their examination of information security policy violations, Siponen and Vance (2010) used a combination of neutralization theory and deterrence theory as the study's

theoretical foundation. Six of the neutralization theory techniques denial of responsibility, denial of injury, condemnation of the condemners, appeal to higher loyalties, metaphor of the ledger, and the defense of the necessity were integrated with deterrence theory constructs to create a research model. A research model based on neutralization theory was also developed by Kim, Yang, and Park (2014) and included all seven neutralization techniques. This research model also included constructs from protection motivation theory, rational choice theory, planned action theory, and the theory of planned behavior.

Results from the Siponen and Vance (2010) study using the neutralization techniques indicated all of the constructs were a statistically significant contributor to information security policy violation behavioral intention. Additional details of the study were previously discussed in the discussion of deterrence theory. Kim et al. (2014) combined all of the neutralization techniques into a single construct. Results indicated neutralization significantly contributed to information security compliance behavioral intention. A prior discussion on protection motivation theory constructs included additional study details.

Theory of Planned Behavior

Fishbein and Ajzen (1975) proposed the theory of planned behavior as an extension of the theory of reasoned action. Ajzen (1991) suggested the theory of planned behavior can forecast an individual's behavioral intention based on "attitudes toward the behavior, subjective norms, and perceived behavioral control" (p. 179). Constructs of the theory of planned behavior include behavioral beliefs, normative beliefs, and self-efficacy and are considered "antecedents of attitudes, subjective norms, and perceived

behavioral control" (Bulgurcu et al., 2010, p. 527). Because of its theorized ability to forecast behavioral intentions, the theory of planned behavior has served as the theoretical foundation for studies examining information security compliance behavioral intention.

Bulgurcu et al. (2010) suggested that the attitude of the employee is influenced by the benefit and cost of compliance, the cost of noncompliance, and information security awareness. The theory of planned behavior and rational choice theory are combined to serve as the theoretical foundation for the study. Attitude, subjective norms, and perceived behavioral control are constructs taken from the theory of planned behavior and included in the study. Godlove (2012) suggested the lack of information security risk awareness by teleworkers makes it difficult for management to maintain the security of the organization's information assets. Godlove proposed a study to examine the teleworker's attitude to information security compliance behavior using the theory of planned behavior as the theoretical foundation. Ifinedo (2012) recognized the construct self-efficacy overlapped protection motivation theory and the theory of planned behavior and combined the two theories to examine information security policy behavioral intention. Sommestad, Karlzén, and Hallberg (2015) expanded the theory of planned behavior to include constructs from protection motivation theory and anticipated regret. Sommestad et al. hypothesized the constructs attitude, perceived norm, and perceived behavioral control from the theory of planned behavior combined with the constructs perceived vulnerability, perceived severity, response efficacy, self-efficacy, and response costs from protection motivation theory and anticipated regret would affect information

security policy behavioral intentions. Al-Mukahal and Alshare (2015) developed a research model based on deterrence theory, neutralization theory, and the theory of planned behavior. Al-Mukahal and Alshare hypothesized that information security policy awareness, employee trust, information security policy simplicity, and policy effect on work environment would be related to the quantity of information security policy violations.

Survey Service Provider

Obtaining a sufficient number of research study participants can be a challenge. Some researchers use students from their academic institutions. Boss et al. (2015) surveyed MBA and psychology students for a study examining information security behaviors. Yoon, Hwang, and Kim (2012) created a study of students examining perceptions affecting information security behaviors. Crossler and Bélanger (2014) developed an information security practice index and surveyed business students to examine behaviors related to information security. A scholar-practitioner conducting research without a relationship with an academic institution would have difficulty using students as participants. An alternative would be to enlist the services of a survey service provider.

Using a survey service provider offers researchers another source of research participants. Son (2011) obtained participants from a survey company for a research study. Tsai et al. (2016) used Amazon's Mechanical Turk to obtain participants for a study examining home security behaviors. Bulgurcu et al. (2010) used the services of a research company to provide participants for a study examining information security

policy compliance. Although a specific survey service provider was not mentioned in the literature reviewed, SurveyMonkey offers an online web-based survey service.

SurveyMonkey offers a suite of survey services to a wide variety of customers, including academic researchers. Symonds (2011) examined the applicability of SurveyMonkey to be used as a library assessment tool. Because there was little budget available, library staff used SurveyMonkey low-cost services for online surveys. Although a formal study was not conducted, the assessment and resource planning team found SurveyMonkey to be an adequate question-based assessment tool.

Although SurveyMonkey use was not explicitly stated in prior information security behavioral research, the SurveyMonkey service has been used in other studies. Studies in the medical field have used SurveyMonkey as a service provider. Reitz and Anderson (2013) identified the ease of developing a survey using SurveyMonkey and its ability to reach a large population for nurse workforce studies. SurveyMonkey was used to appraise the effectiveness of the Robert Wood Johnson Foundation Nurse Faculty Scholars program (Hickey et al., 2014). SurveyMonkey has also been used in behavioral studies. Wright and Khatri (2015) used SurveyMonkey to recruit 1,078 nurses to participate in their study of bullying psychological and behavioral responses.

Summary and Conclusions

Using purely technical measures to implement information security is inadequate. Nontechnical measures should be included to ensure a secure information system environment. Because nontechnical security measures involve people, researchers have conducted studies to examine how an individual's perceptions can affect information

security compliance behavioral intention. Theories from criminology and psychology have served as the theoretical foundation for studies examining information security compliance. These theories include deterrence theory and neutralization theory from criminology and protection motivation theory and the theory of planned behavior from psychology. Protection motivation theory and deterrence theory were frequently used in the reviewed literature. These two theories will also serve as the theoretical foundation for this dissertation. Several studies using protection motivation theory and deterrence theory were reviewed to demonstrate how these theories were enhanced and expanded to study information security compliance. Studies using neutralization theory and the theory of planned behavior were summarized to complete the review of the literature regarding information security compliance. Because this dissertation will use SurveyMonkey, a brief review of information security compliance studies using a survey service provider was provided. An additional discussion on the use of SurveyMonkey in research studies provided insight on how a survey service provider was used in research.

A generalization of the literature reviewed is a lack of common research models among studies examining information security compliance behavioral intention. Using a theory as the basis of a theoretical foundation, researchers have developed unique research models by combining constructs from one or more theories. The use of unique research models poses a problem for a direct comparison of results. Although it is possible to compare the results of similar constructs used in multiple studies, it is unknown if the other constructs used in the research model influence the main theoretical

constructs. Because of these unique research models and a lack of comparative studies, researchers have a large amount of material available for use in future research.

Chapter 3 will describe the experimental study used to examine information security policy behavioral intention. A discussion of the research design and study methodology will be discussed to provide the steps used to conduct the study. The research design discussion is followed by the data analysis plan and the methods used to mitigate threats to study validity. Because of the need to protect study participants, the chapter concludes with those ethical procedures used to protect the participants and the associated research data.

Chapter 3: Research Method

The purpose of this quantitative, experimental study was to examine the relationship of constructs from a combination of protection motivation theory and deterrence theory and information security compliance behavioral intention. The constructs from protection motivation of perceived threat vulnerability, perceived threat severity, response efficacy, and self-efficacy were the first half of the independent variables. The second half of the independent variables, informal sanction certainty, informal sanction severity, formal sanction certainty, and formal sanction severity, are constructs from deterrence theory. The relationship between the independent variables and the dependent variable information security policy behavioral intention was examined in this dissertation. The participants for this study were individuals indicating that their job function is information technology and their job level is intermediate or entry-level professionals who are SurveyMonkey audience members. Control and intervening variables were not applicable to the study because the focus was on the relationship between the independent and dependent variables.

The purpose of this chapter is to describe the research tools and techniques used in this dissertation. A description of the research method is provided along with a discussion supporting the selected research design method. The study population and methods of selecting participants are also provided. Data collected from the participants were recorded on an instrument. Details on the data collection method and instrument use are described. Methods relevant to the protection of participants and their personally identifiable information were implemented during the study. With the data collection

process defined, the focus will move to the data analysis methods. The previously presented research questions are included with the relevant statistical methods used to analyze each variable. Descriptive and inferential statistical methods were used to provide an analysis of the data represented by each variable.

Research Design and Rationale

A quantitative, experimental, posttest-only control group design was selected as the research design for this dissertation. This research design includes two groups: one experimental group and one control group. A survey was provided to the experimental group after receiving an experimental treatment. When the experimental group receives their survey, the control group also receives a survey, but the control group does not receive the experimental treatment. In addition to including two groups and an experimental treatment, participants must be randomly selected and assigned to one of the two groups. See Figure 1 for a diagram of the research design.

O_n = observation at time n
X = experimental treatment
R = random assignment of participants

R X O_1 Experimental group
R O_1 Control group

Figure 1. Research design.

A similar research design without the random assignment of participants is a quasi-experimental design (Singleton & Straits, 2010).

A version of the posttest-only control group design was used by Johnston and Warkentin (2010) in their examination of fear appeals effect on information security compliance behavioral intention. A posttest only design was incorporated into the pretest-posttest control group research design. Singleton and Straits (2010) defined true experimental research designs as designs containing two or more groups, and participants are randomly selected. Designs incorporating these elements contribute to the minimization of internal validity. The posttest-only control group design is a true experimental design and includes random assignment of participants and two groups. An experimental treatment is introduced to the experimental group before the administration of a survey. A control group is the second group, and only the survey is administered to the group. Johnston et al. (2015) used a posttest-only control group research design in a mixed-method study of information security compliance behavioral intention. Participants were randomly selected and assigned to the experimental and control groups. Each of the participants in the experimental group received a fear appeal treatment followed by the survey. Control group participants did not receive the experimental treatment and only received the survey. Johnston and Warkentin (2010) selected this design to determine if any changes in the group observation during the posttest were related to the experimental treatment and not some external influence. Siponen and Vance (2010) encouraged the use of a posttest measure after an information communication to examine behavior changes.

Variables included in the research design included the eight independent variables derived from the theoretical foundation and the dependent variable information security

policy compliance behavioral intention. A research model diagram is presented in Figure 2.

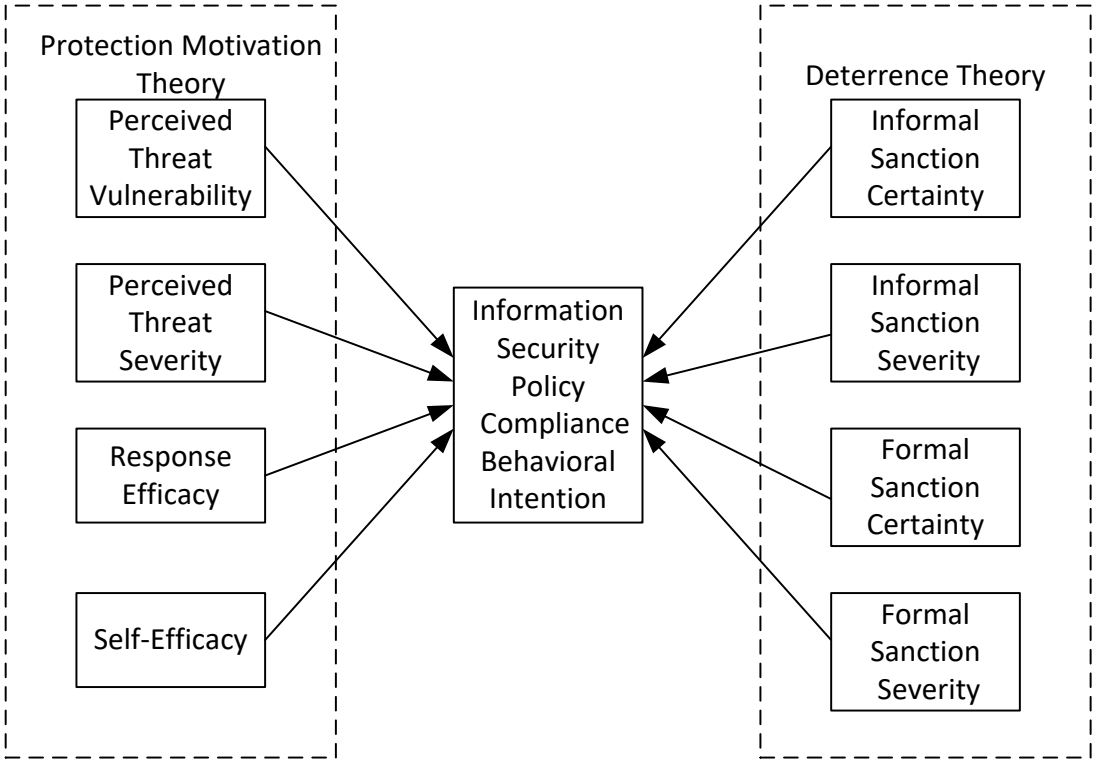

Figure 2. Research model.

Four of the independent variables, perceived threat vulnerability, perceived threat severity, response efficacy, and self-efficacy, are constructs from protection motivation theory. The remaining four independent variables, formal sanction certainty, formal sanction severity, informal sanction certainty, and informal sanction severity, are constructs taken from deterrence theory. Because the focus of the research was on the independent and dependent variables, no mediating or moderating variables were included in the research design.

Methodology

In this section, the methodology developed to conduct the research study is discussed. Elements of the methodology include the population, sample determination, participant recruitment, survey instrument, and the experimental treatment. SurveyMonkey was used as the survey service provider, and many of the aspects related to population, sampling, and recruitment were determined by the processes and procedures of SurveyMonkey. I determined the study elements that included establishing the sampling criteria, instrument development, and providing the experimental treatment. Details of each element are described to define the methodology used in the study.

Population

The population for this study was information technology professionals in intermediate or entry-level position professionals who were over the age of 18 located in the United States and were members of the SurveyMonkey audience. Respondent members of this population were recruited to participate in SurveyMonkey surveys. There are more than 45 million members in the SurveyMonkey audience. SurveyMonkey offers a diverse population of respondents to academic researchers. After a member joins the SurveyMonkey community, they become a SurveyMonkey contribute member. When joining the SurveyMonkey audience, members complete an individual profile and provide gender, age, location, and other possible characteristics used to select a survey sample. After a SurveyMonkey contribute member completes a survey, a contribution is made to a charity selected by the member. Members are also eligible to enter a sweepstake (SurveyMonkey Audience for Academics, 2016).

Sampling and Sampling Procedures

A random sample of participants was selected from the SurveyMonkey audience. SurveyMonkey performed the random selection of participants. Eligible participants were selected by matching the dissertation sample criteria to the profile information provided by the SurveyMonkey contribute member. Dissertation sample inclusion criteria included individuals self-reporting their job function as information technology and their job level as intermediate or entry-level professionals, over the age of 18, and located in the United States. This sample criteria were provided to SurveyMonkey for participant selection. Siponen and Warkentin (2010) used a random sample for participant group assignment in their study of information security policy violation behavioral intention.

Scholars who have examined information security policy compliance behavioral intention indicated that there was no agreement on how to calculate a sample size for studies using partial least squares-structural equation modeling data analysis. Most researchers invited a large number of individuals to participate in a study and used all of the completed survey responses in their data analysis. For these studies, the number of completed surveys became the sample size. Urbach and Ahlemann (2010) suggested that the sample size should be within the range of 30 to 100 participants. Hair, Sarstedt, Pieper, and Ringle (2012) recommended a rule of thumb that establishes a minimum sample size equal to 10 times the number of independent variables. Ringle, Sarstedt, and Straub (2012) conducted a review of partial least squares-structural equation modeling research published in MIS Quarterly and found a wide variety of sample sizes ranging from 17 to 1,449. A total of 109 models were reviewed, and the sample size mean was

238.12 and median was 198. There was no recommended method of calculating a sample size included in the review. Dang-Pham and Pittayachawan (2015) noted the difficulty in determining a sample size for partial least squares-structural equation modeling. Hair et al. (2017) provided a table of recommended partial least squares-structural equation modeling sample size based on an 80% statistical power. Other factors used to determine sample size are significance level, the number of independent variables, and a minimum R^2. Hair et al. stated that an R^2 value of 0.20 would be considered high for behavior studies. Because I examined behaviors, a minimum R^2 of 0.25 was selected from the table. A value of 0.25 is close to the Hair et al. stated value of 0.20. Using the R^2 value of 0.25, a significance level of 5%, and eight independent variables, a sample size of 54 were used for both the experimental group and the control group.

Procedures for Recruitment, Participation, and Data Collection

I decided to use a survey service provider for the recruitment, participation, and data collection. SurveyMonkey has recruited over 45 million people who are willing to participate in surveys. SurveyMonkey randomly selected participants matching the dissertation sample criteria. Participants received an e-mail from SurveyMonkey inviting them to complete a survey. Included in the e-mail were instructions to begin the survey. A link to a web-based survey was included in the invitation that linked to the additional instructions or survey questions (SurveyMonkey Audience's Answers to the ESOMAR 28 Questions, 2013). Before beginning the survey, all participants received an informed consent document online, and they must affirmatively indicate that they were willing to participate in the survey before beginning the survey. If they are not willing to

participate, they can exit from the survey process. Participants completed the online survey, and SurveyMonkey collected the response data. Those participants randomly assigned by SurveyMonkey to the experimental group received the experimental treatment online before beginning the posttest survey. Once they had completed the survey process, the participant exieds from the study. There was no poststudy follow-up.

Instrumentation and Operationalization of Constructs

For this dissertation, instruments from two different studies were combined. Because the research model merges the constructs from protection motivation theory and deterrence theory, two prior instruments were merged. Appendix A includes the constructs, statements, questions, and their associated sources used to develop the instrument. The first half of the merged instrument was used in a study conducted by Siponen et al. (2014). A copy of the permitted use letter is provided in Appendix B. Siponen et al. conducted a study on behavioral intention to comply with information security policies. A population of Finnish corporate employees was used for the study. Protection motivation theory was used as the theoretical foundation. Four protection motivation theory constructs, perceived threat severity, perceived threat vulnerability, response efficacy, and self-efficacy, were used in the research model. These are the same protection motivation theory constructs used in this dissertation model. Because Siponen et al. examined information security policy behavioral intention using four constructs from protection motivation theory and I examined the same outcome using the same constructs, this use of the instrument was appropriate.

Siponen et al. (2014) performed content validation of the instrument during a pilot test and reported the reliability and validity tests supported all of the instrument constructs. Convergent validity was assessed using confirmatory factor analysis for each of the constructs. Factor loadings were calculated for all constructs, and all factor loadings exceeded the 0.5 threshold. Discriminant validity was determined using correlations between all pairs of constructs. All correlations exceeded the 0.9 threshold value. Variance extracted values exceeded the threshold value of 0.5 for all constructs. Cronbach's alphas were calculated to determine internal consistency. All values exceeded the recommended threshold value of 0.6. Composite reliability was calculated, and all results exceeded the 0.7 threshold value. These results indicated all constructs had a high internal consistency.

Siponen and Vance (2010) conducted a study on the behavioral intention to violate information security policy using deterrence theory as a theoretical foundation. The instrument used by Siponen and Vance was used as the second half of the merged instrument used for this dissertation. A copy of the permission of use letter is provided in Appendix C. A population of Finnish administrative personnel was used for the survey. Siponen and Vance created a research model using the constructs of formal sanctions and informal sanctions from deterrence theory. Deterrence theory constructs included in the instrument were formal sanction certainty, formal sanction severity, informal sanction certainty, and informal sanction severity. These four constructs were merged to create constructs of formal sanctions and informal sanctions used in the research model. Because the instrument included all four deterrence theory constructs, all four of the

deterrence theory constructs were used for this dissertation model. Siponen and Vance examined information security policy behavioral intention using constructs from deterrence theory, and I was also examining information security policy compliance behavioral intention using the same deterrence theory constructs. Using the Siponen and Vance instrument was appropriate for this dissertation.

Siponen and Vance (2010) performed a bootstrap analysis to test convergent validity. When the indicators load values have a significant *t* test with their latent constructs, convergent validity is demonstrated. All indicator loadings were significant at the .001 level indicating convergent validity. Another test of convergent validity is an analysis of the average variance extracted values. Average variance extracted is a measure of variance explained by latent constructs. This variance should exceed the threshold value of 0.5 for all measurement items. All construct average variance extracted values exceeded the threshold value and indicated convergent validity.

Experimental Treatment

An experimental treatment is a basic element of experimental research design. By using an experimental treatment, a researcher is examining the effect of the treatment on the participants. An experimental group receives the experimental treatment, and the control group does not receive the experimental treatment to measure this effect. A posttest survey is administered to both groups of participants. If analysis of the survey groups indicates a difference, this difference can be attributed to the experimental treatment (Singleton & Straits, 2010). Scholars using protection motivation theory use a fear appeal as an experimental treatment. Johnston et al. (2015) used scenarios related to

information security measures as a fear appeal in a study on information security compliance behavioral intention. For this dissertation, a fear appeal explaining an information security policy was used as an experimental treatment. Son (2011) used a communication defining an information security policy and employee responsibilities as an experimental treatment. This information security policy communication was used in Son's study of information security policy compliance. Full-time employees taken from a national data collection company were participants used in the Son study. Son's information security policy communication was used in this dissertation as the experimental treatment. Appendix D contains a copy of the permission of use letter. The experimental treatment for this research study is presented in Appendix E.

Data Analysis Plan

The data analysis included descriptive and inferential statistics. Descriptive statistics were calculated for research question survey responses and demographic data. Partial least squares-structural equation modeling was the method for calculating inferential statistics and was used to examine any relationships between the independent and dependent variables. Smart PLS software, version 3.0 was used for statistical calculations. Research questions and hypotheses, threats to validity, and ethical consideration are also discussed as part of the data analysis plan.

Research Questions and Hypotheses

This dissertation focuses on the following research questions:

RQ1–What is the effect of informal sanction certainty on an individual's information security policy compliance behavioral?

$H_0$1: Informal sanction certainty will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a1: Informal sanction certainty will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ2–What is the effect of informal sanction severity on an individual's behavioral intention to comply with information security policies?

$H_0$2: Informal sanction severity will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a2: Informal sanction severity will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ3–What is the effect of formal sanction certainty on an individual's behavioral intention to comply with information security policies?

$H_0$3: Formal sanction certainty will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a3: Formal sanction certainty will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ4–What is the effect of formal sanction severity on an individual's behavioral intention to comply with information security policies?

$H_0$4: Formal sanction severity will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a4: Formal sanction severity will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ5– What is the effect of perceived threat vulnerability on an individual's behavioral intention to comply with information security policies?

$H_0$5: Perceived threat vulnerability will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a5: Perceived threat vulnerability will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ6–What is the effect of perceived threat severity on an individual's behavioral intention to comply with information security policies?

$H_0$6: Perceived threat severity will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a6: Perceived threat severity will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ7–What is the effect of response efficacy on an individual's behavioral intention to comply with information security policies?

$H_0$7: Response efficacy will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a7: Response efficacy will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ8–What is the effect of self-efficacy on an individual's behavioral intention to comply with information security policies?

$H_0$8: Self-efficacy will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a8: Self-efficacy will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

Analysis Plan

Descriptive statistics were calculated for responses from survey research questions and participant demographic data. Descriptive statistical calculations included mean, median, frequency, and standard deviation. The first step in the data analysis process was model validation. Gefen and Straub (2005) suggested a method for examining model validity. Confirmatory factor analysis calculates the model measurement item loadings of the latent constructs. Convergent validity is demonstrated when the measurement item loads on latent constructs are significant at the 0.05 level. Discriminant validity is demonstrated when the average variance extracted for each latent construct is larger than the correlation between latent construct pairs. A bootstrap technique is used to generate average variance expected values, and the results should exceed the 0.50 threshold value. Composite reliability scores, calculated during the partial least squares analysis, should exceed the threshold values of 0.7 to demonstrate construct measurement reliability (Johnston et al., 2015).

Partial least squares-structural equation modeling analysis was used to test the hypotheses. Siponen and Vance (2010) suggested that partial least squares analysis is preferred for model prediction rather than testing theory. A complete partial least squares-structural equation modeling analysis was conducted to analyze the relationships between the independent and dependent variable. All tests for significance were measured at the 0.05 level.

Threats to Validity

Singleton and Straits (2010) identified three threats to validity, measurement validity, internal validity, and external validity. A description of each type of validity is provided to explain how each threat affects the research analysis. Along with a description, methods used to mitigate the different threats are discussed.

Measurement Validity

Singleton and Straits (2010) found measurement threat as an effect that occurs during the response process because of self-censoring. Although this is a problem in laboratory experiments, the reactive measurement effect also occurs during survey and field research. Research participants are often placed in a situation they have not previously experienced. Participants become aware that they may be asked to do something unusual and suspect they have not been informed of the actual purpose of the research. When participants become aware of perceiving expected behaviors, these perceptions may influence their behavior.

Singleton and Straits (2010) suggested that participants may misunderstand the communicated expectations. A method reducing the bias introduced by the misunderstanding is to measure the dependent variable after the independent variable manipulation. Because a control group was used in this dissertation research, the control group could contribute to the reduction of bias. Johnston et al. (2015) used partial least squares-structural equation modeling to validate the measurement model. Partial least squares composite reliability scores greater than 0.70 indicates construct measurement reliability. These validity tests also include convergent and discriminant validity tests.

External Validity

External validity is described by Singleton and Straits (2010) as the generalization of the study results. Generalization refers to the ability of study results applicability outside of the study framework. If a study is generalizable, results of the study would be similar for participants with different populations and locations. If a study lacks internal validity, it cannot be inferred that the manipulated independent variable caused a change in the dependent variable and it would not be logical the results can be generalized. Because sample selection can limit external validity, care should be taken when generalizing results to different groups. By replicating a study, the generalization of the theories and hypotheses increases.

Johnston et al. (2015) determined convergent validity by calculating the loading of indicators of their respective latent constructs. Indicator loadings must be significant at the 0.05 level to demonstrate convergent validity. Convergent validity is also determined by the amount of variance found in latent construct measurements. Average variance extracted values for all constructs should exceed 0.50 to indicate a high level of convergent validity. Discriminant validity is demonstrated when the indicator loadings differences between an intended construct and other constructs are 0.10 or greater.

Internal Validity

Singleton and Straits (2010) identified internal validity as a threat to establishing a causal relationship. When a study has high internal validity, there is confidence the independent variable causes a change in the dependent variable. The research design

establishes internal validity, and a true experiment includes the following design requirements

- random assignment;
- independent variable manipulation;
- dependent variable measurement;
- a minimum of one control group; and
- consistent conditions for all groups.

Research designs with the previously defined requirements eliminate the possibility of extraneous variables affecting the study results. Studies incorporating these requirements are internally valid. Random assignment of participants to the experimental and control groups establish approximate equal groups and nullifies any difference between participants. Group equivalence is also achieved by treating the experimental and control groups in the same manner.

This dissertation used a posttest-only control group research design. Participants were randomly assigned to the experimental group and control group satisfying the first requirement. Independent variable manipulation is achieved through the use of an experimental treatment and a posttest survey. The survey included elements to measure the dependent variable. A control group was used, and participants assigned to this group will receive the posttest survey but did not receive the experimental treatment. Finally, all groups will experience consistent conditions of completing a web-based survey. Through the incorporation of true experiment requirements, this dissertation research model could achieve internal validity.

Construct Validity

Construct validity is complex because it requires assessment using statistical analysis and practical procedures. Demonstrating construct validity involves determining if the results from an instrument are "significant, meaningful, useful, and have a purpose" (Creswell, 2008, p. 173). Statistical analysis includes

- examining results relationships;
- results support the theory as expected; and
- correlate results with other variables for similarities and differences (Creswell, 2008).

If the statistical analysis results indicate there is a good fit between the theoretical model and the study data is an indicator construct validity has been achieved (Da Veiga & Eloff, 2010). Using confirmatory factor analysis to determine construct validity is achieved by analyzing item loading for each construct. Construct validity is verified if the loading values exceed 0.6 (Meso et al., 2013). Construct validity also includes reliability, convergent validity, and discriminant validity (Chu & Chau, 2014).

Practical procedures can be used for understanding the results and include

- examining the significances of data interpretation;
- examining data relevance and use; and
- examining the significance of using the study results (Creswell, 2008).

Ethical Procedures

Several precautionary measures were taken to ensure the ethical treatment of individuals participating in the research study. Before any activities that involve

participants, Institutional Review Board approval was obtained. An application with all necessary materials was submitted to the Institutional Review Board to initiate the approval process (Walden IRB approval no. 03-02-17-0117835).

Because a survey service provider was used for recruitment and data collection, I am removed from direct communications with the participants. This separation does not relieve me from ensuring the survey service provider is conducting business in an ethical manner. SurveyMonkey was used as the survey service provider, and a review of their policies and privacy guidelines was conducted.

All potential participants were required to provide informed consent by acknowledging in the affirmative that they agree to participate in the study and understand their responsibilities needed to complete the survey. Any potential participant who does not agree with the information in the informed consent form can indicate they do not wish to participate and the survey process will terminate. The participant also had the ability to exit from the survey process at any point in the survey.

Data collected from the survey did not contain any personally identifiable information. As part of completing the SurveyMonkey profile process, SurveyMonkey contribute members may have provided SurveyMonkey personally identifiable information. This information remained with SurveyMonkey and was not be provided to me. At the conclusion of the survey process, survey response data and participant demographics were downloaded from SurveyMonkey. Survey data was stored in a password-protected file on a password protected computer. Survey data was archived on

optical media in a password protected file. Data stored on the computer and archived on optical media will be destroyed seven years after the publication of the dissertation.

SurveyMonkey will collect survey data, and I will have no knowledge or influence on the selection of participants. Using a third-party survey service provider eliminates the possibility of a conflict of interest between the participants and me. SurveyMonkey does offer an incentive to their SurveyMonkey contribute members in the form of a contribution to a charity selected by the member. Because this arrangement is between SurveyMonkey and the survey participant, there is no conflict of interest with me.

Summary

The research method presented in the chapter described the research design, methodology, data analysis plan, and threats to validity. A quantitative experimental posttest-only control group research design was used for this dissertation. A description of the methodology included the elements population, sampling, participant recruitment, instrument development, and experimental treatment. The data analysis plan begins with the research questions and hypotheses describing the independent and dependent variables and their relationships. Analysis of the data included descriptive and inferential statistics. Variable relationships were analyzed using partial least squares-structural equation modeling and SmartPLS 3.0 software. Threats to validity include measurement, external, internal, and construct validity. Methods used to determine these validity factors were discussed. Concluding the chapter is a discussion on those ethical procedures implemented to protect study participants.

Chapter 4: Results

The purpose of this quantitative, experimental study was to examine the relationship between constructs from protection motivation theory and deterrence theory and information security policy compliance behavioral intention. Protection motivation theory constructs were merged with constructs from deterrence theory to develop a research model. Protection motivation theory constructs included in the research model were perceived threat vulnerability, perceived threat severity, response efficacy, and self-efficacy. Included in the research model were the deterrence theory constructs: formal sanction certainty, formal sanction severity, informal sanction certainty, and informal sanction severity. The following research questions were developed to examine the theory constructs effect on information security policy compliance behavioral intention:

RQ1–What is the effect of informal sanction certainty on individual's behavioral intention to comply with information security policies?

$H_0$1: Informal sanction certainty will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a1: Informal sanction certainty will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ2–What is the effect of informal sanction severity on an individual's behavioral intention to comply with information security policies?

$H_0$2: Informal sanction severity will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a 2: Informal sanction severity will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ3–What is the effect of formal sanction certainty on an individual's behavioral intention to comply with information security policies?

$H_0$3: Formal sanction certainty will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a3: Formal sanction certainty will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ4–What is the effect of formal sanction severity on an individual's behavioral intention to comply with information security policies?

$H_0$4: Formal sanction severity will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a4: Formal sanction severity will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ5–What is the effect of perceived threat vulnerability on an individual's behavioral intention to comply with information security policies?

$H_0$5: Perceived threat vulnerability will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a5: Perceived threat vulnerability will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ6–What is the effect of perceived threat severity on an individual's behavioral intention to comply with information security policies?

$H_0$6: Perceived threat severity will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a6: Perceived threat severity will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ7–What is the effect of response efficacy on an individual's behavioral intention to comply with information security policies?

$H_0$7: Response efficacy will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a7: Response efficacy will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

RQ8–What is the effect of self-efficacy on an individual's behavioral intention to comply with information security policies?

$H_0$8: Self-efficacy will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a8: Self-efficacy will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

Chapter 4 begins with a review of the data collection process used to gather survey responses. Following the data collection process discussion is a description of the experimental treatment implementation and study results. The study results include the descriptive statistics of the survey responses, a partial least squares-structural equation modeling model analysis, and the hypotheses analysis.

Data Collection

Data collection for the study began with the development of the web-based SurveyMonkey survey. Appendix A includes the statements and questions used to create the survey. On March 4, 2017, the SurveyMonkey audience population described in Chapter 3 received the survey, and the data collection concluded on March 9, 2017. A sample size of 54 responses for the experimental group and 54 responses for the control group was the plan described in Chapter 3, but SurveyMonkey suspended the survey before receiving 54 completed responses for each group. SurveyMonkey has a policy where surveys with an above-average abandonment rate are paused (Buying Responses with SurveyMonkey Audience, 2017). The number of individuals beginning the survey but not completing the survey determines the abandonment rate. Restarting a survey a second time is possible, but a second paused survey resulted in suspending the survey. SurveyMonkey support notified me that the survey had an above-average abandonment rate causing a survey pause. SurveyMonkey restarted the survey, but a second above-average abandonment rate caused the survey suspension. At the conclusion of the survey, there were 34 completed survey responses from the experimental group, and 33 completed survey responses from the control group. Because the number of responses did not equal the sample size, the survey was relaunched to gather additional responses. The survey was distributed a second time to the SurveyMonkey audience population on March 14, 2017, and the data collection concluded on March 21, 2017. This survey experienced a similar abandonment rate as the first survey. An additional 39 responses for the experimental group and 40 responses for the control group were received. A total

of 73 responses for the experimental group and 73 responses for the control group were received. The recommendations section of Chapter 5 includes a discussion on the feedback received from SurveyMonkey regarding the causes of a high abandonment rate and suggestions for improvement.

Basic demographic information for the control and experimental group responses included age and gender. Age information provided by SurveyMonkey is in age ranges and not individual ages. For the control group, 13 respondents were aged 18 to 29, 22 were aged 30 to 44, 33 were aged 45 to 59, and five were 60 and older. Experimental group respondents had three aged 18 to 29, 15 aged 30 to 44, 36 aged 45 to 59, and 19 aged 60 and older. Gender for the control group was 33 female respondents and 40 male respondents. For the experimental group, 28 respondents were female, and 45 were male. A description was not provided regarding sample population representation or proportionality to the larger population because of the random selection of participants. The study results section includes additional demographic descriptive statistics.

Experimental Treatment

Each experimental group participant received an experimental treatment regarding information security policies and associated employee responsibilities. Appendix E presents the full text of the experimental treatment. Administration of the experimental treatment was completed as planned. Before the start of the survey, participants in the experimental group were asked to read the experimental treatment. After reading the experimental treatment, the experimental group participant began the survey. There were no adverse events associated with the experimental treatment reported.

Study Results

The process of data analysis started with a download of the survey responses from SurveyMonkey. Before initiating a download, the responses were filtered to include only completed responses. This filter is a part of the SurveyMonkey response analysis process. Although the intention of applying the filter was to provide only completed responses, some of the responses were not complete. Several survey responses were removed from the dataset because they had missing data items. I removed three survey responses from the dataset, two from the control group and one from the experimental group. The data set included a respondent ID field used to identify each survey response uniquely. The respondent IDs were examined using Microsoft Excel to identify any duplicate respondent IDs. No duplicate respondent IDs were identified indicating no individual provided more than one survey response. Adding data variable names to the data set uniquely identified each dataset field. The constructs column of Appendix A contains the data variable name used for each of the individual survey responses.

Demographic Information

Demographic information provided by SurveyMonkey included gender and age group. SurveyMonkey does not provide individual ages. I included two additional demographic questions regarding information security policy training and awareness. Because there were two groups of respondents, each of the demographic descriptive statistics is provided by the participant group. Gender for the control group was 43.7% female and 56.3% male. For the experimental group, the gender was 38.9% female and 61.1% male. Table 1 presents additional gender frequency information.

Table 1

Participant Gender Frequency

Participant Gender Frequency			
Group	Female	Male	Total
Control	31	40	71
	43.7%	56.3%	
Experimental	28	44	72
	38.9%	61.1%	

Age groups were divided into ranges of 18 to 29 years, 30 to 44 years, 45 to 59 years, and 60 years and older. Ages for the control group were 13 aged 18 to 29, 22 aged 30 to 44, 31 aged 45 to 59, and five for 60 and over. Experimental group participants age groups were three aged 18 to 29, 14 aged 30 to 44, 36 aged 45 to 59, and 19 for 60 and over. Table 2 contains both age group counts and percentages.

Table 2

Participant Ages by Group

Participant Ages					
Group	18 - 29	30 - 44	45 - 59	60+	Total
Control	13	22	31	5	71
	18.3%	31.0%	43.7%	7.0%	
Experimental	3	14	36	19	72
	4.2%	19.4%	50.0%	26.4%	

The survey included two additional questions regarding information security policy training and awareness. Each participant responded to questions about his or her information security policy training and awareness of his or her organization's information security policy. The control group respondents indicated that 93.0% had received information security policy training, and 7.0% did not receive any training. For

the experimental group, 86.1% indicated that they had received training, and 13.9% did not receive any training. Table 3 presents additional information on group counts and percentages.

Table 3

Information Security Policy Training

	Received Training		
Group	No	Yes	
Control	5	66	71
	7.0%	93.0%	
Experimental	10	62	72
	13.9%	86.1%	

Table 4 presents participant information security policy awareness counts and percentages. This information indicates that 95.8% of the control group and 93.1% of the experimental group were aware of their organization's information security policy.

Table 4

Information Security Policy Awareness

	Policy Awareness		
Group	No	Yes	
Control	3	68	71
	4.2%	95.8%	
Experimental	5	67	72
	6.9%	93.1%	

The next step in the data analysis process was the partial least squares-structural equation modeling analysis of the survey responses.

Model Development

The steps used to conduct a partial least squares-structural equation modeling analysis follow the method described by Hair et al. (2017). Steps included in the Hair et al. method were used to develop the structural model, specify the measurement model, data collection, model estimation, measurement model evaluation, and assessing results. Because the study included two groups, the process was performed twice, once for the control group responses and a second time for the experimental group responses. I used the SmartPLS 3.0 software package to perform all partial least squares-structural equation modeling calculations.

Structural model. Development of the structural model began with creating the model variables and variable relationships. The research model presented in Figure 1 served as the theoretical framework for the structural model. Each box of the research model became a structural model variable, and the relationships of the research model were replicated in the structural model. Figure 3 displays a diagram of the structural.

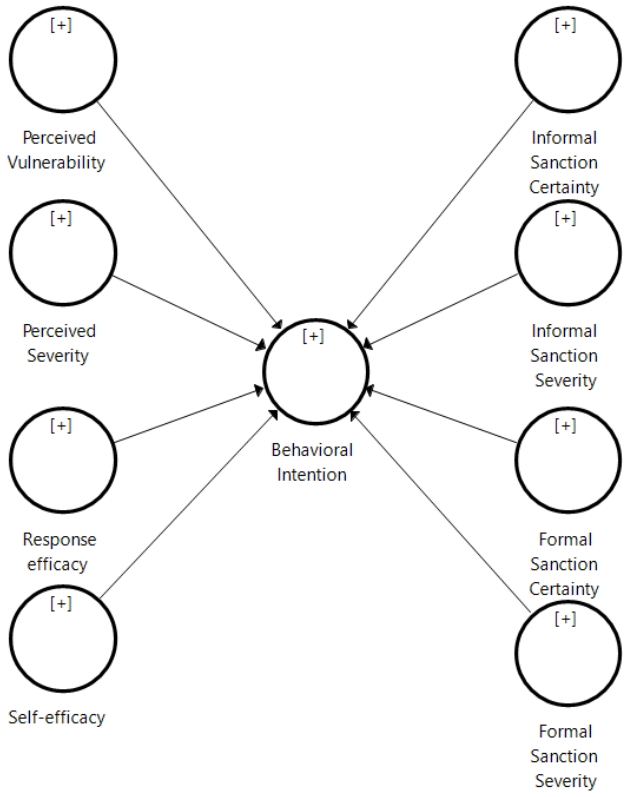

Figure 3. Partial least squares-structural equation modeling structural model.

Measurement model. Developing the measurement model was the next step and required assigning constructs to the variables. Constructs used in the model are described in Appendix A and were assigned to the associated variable. Figure 4 displays the measurement model diagram.

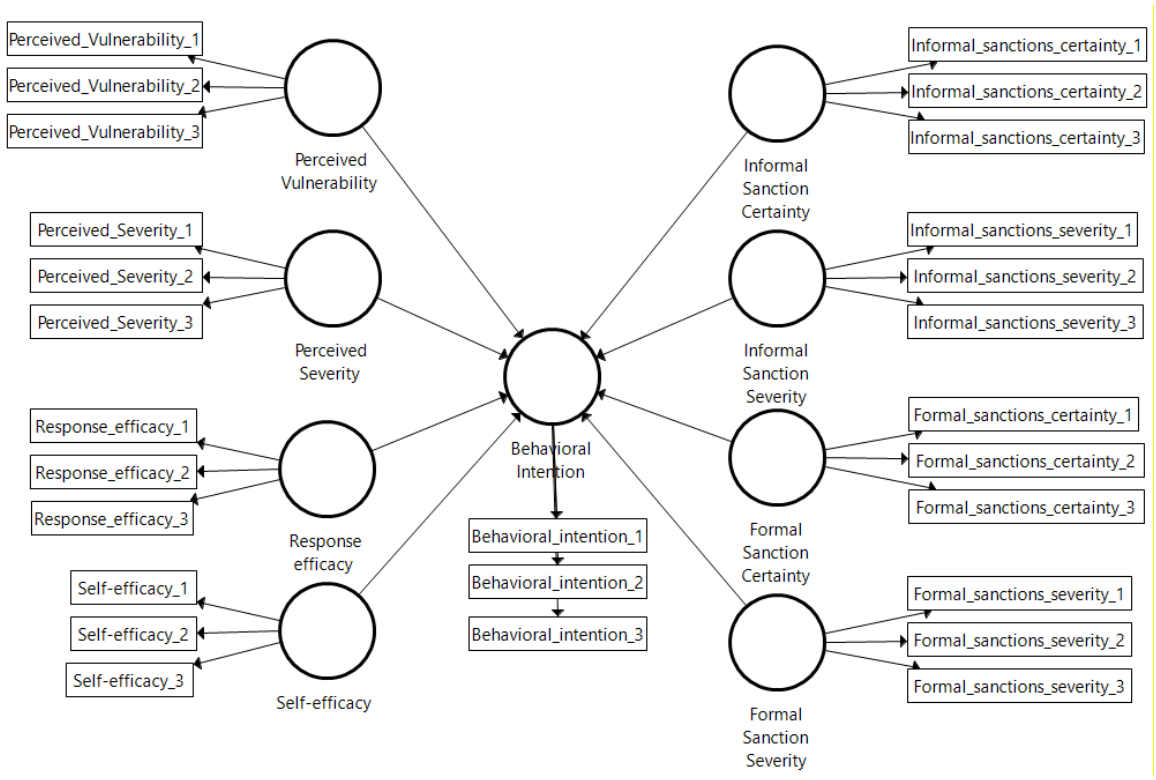

Figure 4. Partial least squares-structural equation modeling measurement model.

Because there were two groups included in the study, I created two models in SmartPLS, one for the control group and a second model for the experimental group. The structural model in Figure 3 and the measurement model in Figure 4 were identical for both groups. Assigning the constructs to the variable establishes a connection between the variable and the survey response data. Data collection concluded before the development of the partial least squares-structural equation modeling model. For the data collection step of the process, the corresponding response data were imported into each model. Calculation of the survey response descriptive statistics occurred as part of the data importation process.

Descriptive Statistics

Table 5 presents the construct descriptive statistics of the control group data, and Table 6 presents the experimental group data construct descriptive statistics.

Table 5

Control Group Descriptive Statistics

Control Group	Mean	Median	Standard Deviation
Behavioral_intention_1	4.704	5	0.758
Behavioral_intention_2	4.676	5	0.765
Behavioral_intention_3	4.521	5	0.853
Self-efficacy_1	4.479	5	0.802
Self-efficacy_2	4.366	5	0.953
Self-efficacy_3	4.31	5	1.001
Perceived_Severity_1	4.211	5	1.006
Perceived_Severity_2	4.437	5	0.945
Perceived_Severity_3	4.577	5	0.725
Perceived_Vulnerability_1	3.887	4	1.015
Perceived_Vulnerability_2	4.183	4	0.969
Perceived_Vulnerability_3	3.93	4	1.117
Response_efficacy_1	4.127	4	0.933
Response_efficacy_2	4.535	5	0.766
Response_efficacy_3	4.521	5	0.767
Formal_sanctions_certainty_1	4.014	4	1.193
Formal_sanctions_certainty_2	4.07	4	1.142
Formal_sanctions_certainty_3	4.268	5	1.034
Formal_sanctions_severity_1	4.366	5	1.065
Formal_sanctions_severity_2	4.38	5	1.053
Formal_sanctions_severity_3	4.296	5	1.093
Informal_sanctions_certainty_1	4.113	4	1.082
Informal_sanctions_certainty_2	4.155	5	1.109
Informal_sanctions_certainty_3	4.268	5	1.006
Informal_sanctions_severity_1	4.042	5	1.261
Informal_sanctions_severity_2	4.268	5	1.174
Informal_sanctions_severity_3	4.099	5	1.246

Table 6

Experimental Group Descriptive Statistics

Experimental Group	Mean	Median	Standard Deviation
Behavioral_intention_1	4.611	5	0.657
Behavioral_intention_2	4.431	5	0.779
Behavioral_intention_3	4.375	5	0.716
Self-efficacy_1	4.542	5	0.644
Self-efficacy_2	4.125	4	0.849
Self-efficacy_3	4.153	4	0.952
Perceived_Severity_1	4.153	4	0.908
Perceived_Severity_2	4.458	5	0.744
Perceived_Severity_3	4.347	5	0.819
Perceived_Vulnerability_1	3.667	4	1.041
Perceived_Vulnerability_2	4.319	4	0.779
Perceived_Vulnerability_3	3.819	4	0.962
Response_efficacy_1	3.875	4	0.985
Response_efficacy_2	4.472	5	0.707
Response_efficacy_3	4.278	4	0.768
Formal_sanctions_certainty_1	4.125	4	0.957
Formal_sanctions_certainty_2	4.181	4	0.918
Formal_sanctions_certainty_3	4.194	4	0.892
Formal_sanctions_severity_1	4.236	4	0.874
Formal_sanctions_severity_2	4.042	4	1.020
Formal_sanctions_severity_3	4.000	4	0.943
Informal_sanctions_certainty_1	3.903	4	1.069
Informal_sanctions_certainty_2	4.181	5	1.058
Informal_sanctions_certainty_3	4.181	5	0.976
Informal_sanctions_severity_1	3.917	4	1.010
Informal_sanctions_severity_2	4.000	4	1.080
Informal_sanctions_severity_3	3.903	4	1.095

With the structural and measurement models created in SmartPLS and data imported into the models, the next step in the process is the model estimation.

Model Estimation

Model estimation is the process of applying the partial least squares-structural equation modeling algorithm to the model and data. The SmartPLS calculate function initiates the model estimation. Hair et al. (2017) recommend using a stop criterion of 1 x 10^{-7} and 300 maximum iterations. Results of the model estimation include the path coefficients and quality criteria. Table 7 presents the path coefficients for the control and experimental groups.

Table 7

Variable Path Coefficients

	Control Group Behavioral Intention	Experimental Group Behavioral Intention
Formal Sanction Certainty	-0.220	0.066
Formal Sanction Severity	0.148	-0.353
Informal Sanction Certainty	0.063	0.248
Informal Sanction Severity	-0.012	0.124
Perceived Severity	0.084	0.245
Perceived Vulnerability	0.160	0.050
Response efficacy	0.332	0.115
Self-efficacy	0.467	0.373

Quality criteria of the results are presented in the measurement model validation and assessing results discussion.

Measurement Model Validation

A quality criteria evaluation of the measurement and structural models examines the metrics indicating the predictive abilities of the model. An evaluation of the

measurement model includes examining internal consistency, convergent validity, and discriminant validity (Hair et al., 2017). Internal consistency includes calculating Cronbach's alpha and composite reliability. Calculations of Cronbach's alpha and composite reliability are part of the SmartPLS quality criteria calculations. Table 8 presents the Cronbach's alpha for both the control and experimental groups.

Table 8

Variable Cronbach's Alpha

	Control Group Cronbach's Alpha	Experimental Group Cronbach's Alpha
Behavioral Intention	0.929	0.884
Formal Sanction Certainty	0.924	0.938
Formal Sanction Severity	0.942	0.938
Informal Sanction Certainty	0.912	0.921
Informal Sanction Severity	0.914	0.902
Perceived Severity	0.817	0.717
Perceived Vulnerability	0.874	0.695
Response efficacy	0.816	0.781
Self-efficacy	0.741	0.725

Cronbach's alpha values of 0.70 and greater are considered acceptable (Hair et al., 2017). All the Cronbach's alpha values for the control group were acceptable. The experimental group's Cronbach's alpha value for Perceived Vulnerability was not acceptable. All the remaining experimental group Cronbach's alpha values were acceptable. Table 9 presents the composite reliability values for the control and experimental groups.

Table 9

Variable Composite Reliability

	Control Group	Experimental Group
	Composite Reliability	Composite Reliability
Behavioral Intention	0.955	0.928
Formal Sanction Certainty	0.952	0.960
Formal Sanction Severity	0.963	0.960
Informal Sanction Certainty	0.944	0.950
Informal Sanction Severity	0.946	0.938
Perceived Severity	0.889	0.838
Perceived Vulnerability	0.922	0.828
Response efficacy	0.890	0.873
Self-efficacy	0.852	0.840

Composite reliability values in the range between 0.70 and 0.90 are acceptable. Values exceeding 0.95 are not acceptable (Hair et al., 2017). Several of the composite reliability values fall into the unacceptable range.

Examining convergent validity includes calculating indicator reliability and average variance extracted. Indicator reliability is also called outer loadings, and all indicators should be statistically significant. Outer loading values greater than .708 are considered significant (Hair et al., 2017). Table 10 presents the outer loading values for both the control and experimental groups.

Table 10

Construct Outer Loadings

	Control Group Outer Loadings	Experimental Group Outer Loadings
Behavioral_intention_1	0.937	0.886
Behavioral_intention_2	0.972	0.916
Behavioral_intention_3	0.899	0.900
Formal_sanctions_certainty_1	0.931	0.922
Formal_sanctions_certainty_2	0.959	0.954
Formal_sanctions_certainty_3	0.906	0.954
Formal_sanctions_severity_1	0.957	0.938
Formal_sanctions_severity_2	0.958	0.959
Formal_sanctions_severity_3	0.924	0.930
Informal_sanctions_certainty_1	0.923	0.894
Informal_sanctions_certainty_2	0.911	0.937
Informal_sanctions_certainty_3	0.930	0.956
Informal_sanctions_severity_1	0.956	0.913
Informal_sanctions_severity_2	0.867	0.936
Informal_sanctions_severity_3	0.947	0.892
Perceived_Severity_1	0.800	0.850
Perceived_Severity_2	0.878	0.776
Perceived_Severity_3	0.879	0.759
Perceived_Vulnerability_1	0.874	0.678
Perceived_Vulnerability_2	0.904	0.866
Perceived_Vulnerability_3	0.899	0.805
Response_efficacy_1	0.621	0.671
Response_efficacy_2	0.955	0.915
Response_efficacy_3	0.954	0.900
Self-efficacy_1	0.621	0.802
Self-efficacy_2	0.920	0.761
Self-efficacy_3	0.870	0.828

All the outer loading values are significant except response_efficacy_1 and self-efficacy_1 for the control group and perceived_vulnerability_1 and response_efficacy_1

for the experimental group indicating these constructs do not demonstrate convergent validity. Table 11 presents the average variance extracted values for the control and experimental groups.

Table 11

Variable Average Variance Extracted

	Control Group	Experimental Group
	Average Variance Extracted	Average Variance Extracted
Behavioral Intention	0.876	0.812
Formal Sanction Certainty	0.869	0.890
Formal Sanction Severity	0.895	0.888
Informal Sanction Certainty	0.849	0.864
Informal Sanction Severity	0.854	0.835
Perceived Severity	0.728	0.634
Perceived Vulnerability	0.797	0.619
Response efficacy	0.736	0.699
Self-efficacy	0.663	0.636

Average variance extracted values exceeding 0.50 indicate the construct explains more than half the indicator variance (Hair et al., 2017). All the average variance extracted values exceed the 0.50 threshold and are acceptable.

Examining a model's cross loadings and Fornell-Larcker criterion determines discriminant validity. Demonstration of discriminant validity occurs when the construct's correlation is greater than the other construct's correlation. In this case, the construct's outer loadings would be greater than the cross loadings of the other constructs. The bolded values in the tables identify the construct's outer loadings. These values should be

greater than the other construct's cross loadings. Table 12 presents the cross loadings for the control group.

Table 12

Control Group Constructs Cross Loadings

Control Group	Behavioral Intention	Formal Sanction Certainty	Formal Sanction Severity	Informal Sanction Certainty	Informal Sanction Severity	Perceived Severity	Perceived Vulnerability	Response efficacy	Self-efficacy
Behavioral_intention_1	**0.937**	0.296	0.447	0.439	0.409	0.682	0.537	0.694	0.682
Behavioral_intention_2	**0.972**	0.282	0.443	0.454	0.468	0.689	0.554	0.694	0.689
Behavioral_intention_3	**0.899**	0.315	0.367	0.442	0.497	0.706	0.526	0.632	0.660
Formal_sanctions_certainty_1	0.258	**0.931**	0.552	0.688	0.515	0.387	0.504	0.490	0.195
Formal_sanctions_certainty_2	0.311	**0.959**	0.641	0.692	0.506	0.365	0.461	0.448	0.263
Formal_sanctions_certainty_3	0.313	**0.906**	0.733	0.744	0.528	0.295	0.465	0.437	0.239
Formal_sanctions_severity_1	0.400	0.699	**0.957**	0.765	0.619	0.457	0.461	0.462	0.233
Formal_sanctions_severity_2	0.448	0.686	**0.958**	0.769	0.682	0.513	0.523	0.498	0.254
Formal_sanctions_severity_3	0.423	0.588	**0.924**	0.812	0.734	0.461	0.504	0.420	0.255
Informal_sanctions_certainty_1	0.454	0.734	0.744	**0.923**	0.761	0.469	0.595	0.649	0.262
Informal_sanctions_certainty_2	0.340	0.744	0.762	**0.911**	0.717	0.371	0.489	0.350	0.225
Informal_sanctions_certainty_3	0.493	0.644	0.780	**0.930**	0.748	0.543	0.619	0.547	0.292
Informal_sanctions_severity_1	0.457	0.474	0.603	0.746	**0.956**	0.518	0.489	0.525	0.311
Informal_sanctions_severity_2	0.463	0.615	0.783	0.781	**0.867**	0.505	0.471	0.453	0.354
Informal_sanctions_severity_3	0.429	0.438	0.595	0.704	**0.947**	0.514	0.464	0.514	0.261
Perceived_Severity_1	0.453	0.374	0.497	0.498	0.533	**0.800**	0.613	0.598	0.395
Perceived_Severity_2	0.639	0.274	0.363	0.351	0.459	**0.878**	0.524	0.512	0.562
Perceived_Severity_3	0.742	0.325	0.456	0.478	0.459	**0.879**	0.606	0.728	0.585
Perceived_Vulnerability_1	0.468	0.501	0.440	0.613	0.515	0.601	**0.874**	0.649	0.270
Perceived_Vulnerability_2	0.599	0.414	0.497	0.516	0.427	0.658	**0.904**	0.566	0.277
Perceived_Vulnerability_3	0.450	0.465	0.462	0.556	0.447	0.529	**0.899**	0.600	0.233
Response_efficacy_1	0.336	0.537	0.521	0.612	0.531	0.431	0.700	**0.621**	0.219
Response_efficacy_2	0.753	0.432	0.427	0.485	0.482	0.708	0.568	**0.955**	0.510
Response_efficacy_3	0.669	0.389	0.397	0.494	0.451	0.679	0.585	**0.954**	0.445
Self-efficacy_1	0.377	0.151	0.032	0.100	0.155	0.197	0.054	0.195	**0.621**
Self-efficacy_2	0.734	0.253	0.311	0.344	0.397	0.653	0.370	0.500	**0.920**
Self-efficacy_3	0.589	0.197	0.223	0.197	0.217	0.550	0.212	0.416	**0.870**

All the control group outer loadings are greater than the other cross loadings except response_efficacy_1 and self-efficacy_1 indicating these constructs do not demonstrate discriminant validity. Table 13 presents the experimental group cross loadings.

Table 13

Experimental Group Constructs Cross Loadings

Experimental Group	Behavioral Intention	Formal Sanction Certainty	Formal Sanction Severity	Informal Sanction Certainty	Informal Sanction Severity	Perceived Severity	Perceived Vulnerability	Response efficacy	Self-efficacy
Behavioral_intention_1	**0.886**	0.397	0.279	0.527	0.314	0.494	0.349	0.510	0.604
Behavioral_intention_2	**0.916**	0.428	0.307	0.443	0.400	0.465	0.337	0.430	0.553
Behavioral_intention_3	**0.900**	0.355	0.258	0.364	0.316	0.572	0.431	0.512	0.507
Formal_sanctions_certainty_1	0.400	**0.922**	0.504	0.708	0.580	0.401	0.250	0.511	0.361
Formal_sanctions_certainty_2	0.400	**0.954**	0.594	0.706	0.621	0.331	0.223	0.470	0.370
Formal_sanctions_certainty_3	0.434	**0.954**	0.647	0.782	0.600	0.401	0.256	0.526	0.373
Formal_sanctions_severity_1	0.327	0.568	**0.938**	0.716	0.719	0.514	0.230	0.493	0.336
Formal_sanctions_severity_2	0.315	0.580	**0.959**	0.705	0.789	0.572	0.345	0.493	0.348
Formal_sanctions_severity_3	0.217	0.611	**0.930**	0.663	0.786	0.544	0.365	0.444	0.246
Informal_sanctions_certainty_1	0.421	0.735	0.650	**0.894**	0.728	0.471	0.311	0.468	0.373
Informal_sanctions_certainty_2	0.482	0.740	0.727	**0.937**	0.702	0.497	0.313	0.516	0.423
Informal_sanctions_certainty_3	0.479	0.697	0.684	**0.956**	0.700	0.515	0.306	0.557	0.356
Informal_sanctions_severity_1	0.364	0.599	0.675	0.717	**0.913**	0.453	0.391	0.438	0.274
Informal_sanctions_severity_2	0.371	0.618	0.806	0.731	**0.936**	0.517	0.347	0.520	0.279
Informal_sanctions_severity_3	0.298	0.518	0.732	0.632	**0.892**	0.397	0.278	0.398	0.262
Perceived_Severity_1	0.554	0.436	0.530	0.559	0.483	**0.850**	0.474	0.588	0.478
Perceived_Severity_2	0.378	0.305	0.490	0.404	0.439	**0.776**	0.472	0.570	0.298
Perceived_Severity_3	0.387	0.174	0.336	0.261	0.255	**0.759**	0.513	0.490	0.448
Perceived_Vulnerability_1	0.227	0.132	0.181	0.196	0.283	0.314	**0.678**	0.293	0.143
Perceived_Vulnerability_2	0.365	0.271	0.266	0.261	0.255	0.476	**0.866**	0.422	0.279
Perceived_Vulnerability_3	0.359	0.186	0.301	0.314	0.353	0.594	**0.805**	0.418	0.348
Response_efficacy_1	0.316	0.488	0.598	0.612	0.610	0.598	0.430	**0.671**	0.352
Response_efficacy_2	0.550	0.430	0.319	0.387	0.307	0.587	0.416	**0.915**	0.428
Response_efficacy_3	0.447	0.459	0.457	0.476	0.437	0.581	0.405	**0.900**	0.403
Self-efficacy_1	0.609	0.391	0.301	0.423	0.273	0.459	0.268	0.404	**0.802**
Self-efficacy_2	0.405	0.224	0.255	0.243	0.217	0.388	0.239	0.354	**0.761**
Self-efficacy_3	0.406	0.278	0.235	0.277	0.203	0.377	0.312	0.356	**0.828**

For the experimental group, all the outer loadings exceeded the other construct's cross loadings demonstrating discriminant validity. The other measure of discriminant validity is the Fornell-Larcker criterion. The Table 14 and Table 15 presents the Fornell-Larcker criterion results for the control group and experimental group, respectively.

Table 14

Control Group Fornell-Larcker Criterion

	Behavioral Intention	Formal Sanction Certainty	Formal Sanction Severity	Informal Sanction Certainty	Informal Sanction Severity	Perceived Severity	Perceived Vulnerability	Response efficacy	Self-efficacy
Behavioral Intention	**0.936**								
Formal Sanction Certainty	0.318	**0.932**							
Formal Sanction Severity	0.449	0.695	**0.946**						
Informal Sanction Certainty	0.476	0.761	0.826	**0.922**					
Informal Sanction Severity	0.488	0.554	0.718	0.807	**0.924**				
Perceived Severity	0.739	0.372	0.505	0.511	0.555	**0.853**			
Perceived Vulnerability	0.576	0.510	0.525	0.625	0.515	0.674	**0.892**		
Response efficacy	0.720	0.490	0.487	0.575	0.539	0.723	0.673	**0.858**	
Self-efficacy	0.723	0.252	0.262	0.286	0.336	0.617	0.293	0.482	**0.814**

Table 15

Experimental Group Fornell-Larcker Criterion

Experimental Group	Behavioral Intention	Formal Sanction Certainty	Formal Sanction Severity	Informal Sanction Certainty	Informal Sanction Severity	Perceived Severity	Perceived Vulnerability	Response efficacy	Self-efficacy
Behavioral Intention	**0.901**								
Formal Sanction Certainty	0.437	**0.943**							
Formal Sanction Severity	0.312	0.618	**0.942**						
Informal Sanction Certainty	0.497	0.778	0.740	**0.929**					
Informal Sanction Severity	0.380	0.636	0.807	0.762	**0.914**				
Perceived Severity	0.566	0.401	0.575	0.532	0.503	**0.796**			
Perceived Vulnerability	0.413	0.258	0.325	0.333	0.374	0.604	**0.787**		
Response efficacy	0.539	0.533	0.509	0.554	0.498	0.690	0.488	**0.836**	
Self-efficacy	0.618	0.390	0.337	0.414	0.297	0.521	0.342	0.471	**0.797**

Bolded items in the table are the square root of the construct's average variance expected. This value should be greater than the construct's correlation with the other constructs. This condition is satisfied for both groups because the square root of the average variance expected is greater than the other constructs demonstrating discriminant validity. All the measurement model evaluation methods provide insight into construct measure validity. Structural model evaluation methods examine the model's ability to predict dependent variable variance (Hair et al., 2017).

Structural Model Validation

In assessing the results of the structural model, the coefficients of determination, predictive relevance, size and significance of the path coefficients, and f^2 and q^2 effect sizes were included (Hair et al., 2017). The primary analysis method for structural model validation is the coefficients of determination or R^2 values. Table 16 presents the R^2 values for the control and experimental groups.

Table 16

Coefficients of Determination

	Control Group		Experimental Group	
	R Square	R Square Adjusted	R Square	R Square Adjusted
Behavioral Intention	0.752	0.720	0.540	0.482

In addition to the R^2 value is the R^2 adjusted value. An R^2 adjusted calculation takes model complexity and sample size into consideration to avoid complex model bias (Hair et al., 2017). Hair et al. (2017) stated defining an acceptable R^2 is dependent on model complexity and research discipline. Model complexity and research discipline variability

make defining a rule for acceptable R^2 values difficult. Hair et al. identified an R^2 value of 0.20 as high for consumer behavior research. Hair et al. also defined R^2 values of 0.75, 0.50, and 0.25 respectively as substantial, moderate, and weak values for marketing research. Predictive relevance, or Q^2, is the next step in the analysis of the structural model.

A blindfolding calculation was performed on the model to determine predictive relevance. The output from the blindfolding calculation was a construct crossvalidated redundancy report. Table 17 presents a construct crossvalidated redundancy report for the control and experimental groups.

Table 17

Construct Crossvalidated Redundancy Report

	Construct Crossvalidated Redundancy					
	Control Group			Experimental Group		
	SSO	SSE	Q² (=1-SSE/SSO)	SSO	SSE	Q² (=1-SSE/SSO)
Behavioral Intention	213	93.246	0.562	216	140.105	0.351
Formal Sanction Certainty	213	213		216	216	
Formal Sanction Severity	213	213		216	216	
Informal Sanction Certainty	213	213		216	216	
Informal Sanction Severity	213	213		216	216	
Perceived Severity	213	213		216	216	
Perceived Vulnerability	213	213		216	216	
Response efficacy	213	213		216	216	
Self-efficacy	213	213		216	216	

The Q^2 value for the variable Behavioral Intention is greater than zero for both the control and experimental groups. The Q^2 value for Behavioral Intention is 0.562 and 0.351 for the control and experimental groups respectively. Although the path coefficient

calculations are part of the partial least squares algorithm, an additional calculation is necessary to compute path coefficient significance.

A bootstrapping process calculates additional statistical information on the path coefficients. The output from the bootstrapping calculation includes the path coefficients, *t* values, and p-values for each variable. Each of the path coefficient's p-value is used to determine if the path coefficient is statistically significant. Bootstrapping calculation results for the control group are presented in Table 18. Table 19 presents the experimental group bootstrapping results.

Table 18

Control Group Path Coefficient Statistics

Control Group	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	t Statistics (|O/STDEV|)	p Values	Significance ($p < 0.05$)
Formal Sanction Certainty -> Behavioral Intention	-0.22	-0.205	0.112	1.964	0.050	No
Formal Sanction Severity -> Behavioral Intention	0.148	0.139	0.135	1.092	0.276	No
Informal Sanction Certainty -> Behavioral Intention	0.063	0.065	0.162	0.392	0.695	No
Informal Sanction Severity -> Behavioral Intention	-0.012	0.002	0.123	0.100	0.920	No
Perceived Severity -> Behavioral Intention	0.084	0.088	0.126	0.668	0.505	No
Perceived Vulnerability -> Behavioral Intention	0.16	0.149	0.109	1.470	0.142	No
Response efficacy -> Behavioral Intention	0.332	0.306	0.133	2.495	0.013	Yes
Self-efficacy -> Behavioral Intention	0.467	0.472	0.103	4.524	0.000	Yes

Table 19

Experimental Group Path Coefficient Statistics

Experimental Group	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	t Statistics (|O/STDEV|)	p Values	Significance ($p < 0.05$)
Formal Sanction Certainty -> Behavioral Intention	0.066	0.061	0.158	0.416	0.678	No
Formal Sanction Severity -> Behavioral Intention	-0.353	-0.344	0.182	1.943	0.053	No
Informal Sanction Certainty -> Behavioral Intention	0.248	0.207	0.203	1.222	0.222	No
Informal Sanction Severity -> Behavioral Intention	0.124	0.152	0.198	0.629	0.53	No
Perceived Severity -> Behavioral Intention	0.245	0.244	0.165	1.479	0.14	No
Perceived Vulnerability -> Behavioral Intention	0.05	0.044	0.111	0.454	0.65	No
Response efficacy -> Behavioral Intention	0.115	0.12	0.203	0.568	0.57	No
Self-efficacy -> Behavioral Intention	0.373	0.381	0.143	2.599	0.01	Yes

A 95% significance level was used to determine path coefficient significance. A p-value less than 0.05 would indicate a statistically significant path coefficient. Examining the bootstrapping results tables indicates only the self-efficacy path coefficient for the control group and self-efficacy and response efficacy path coefficients for the experimental group are significant. The final step in the model structure analysis is the calculation of the f^2 and q^2 effect sizes.

The f^2 and q^2 effect sizes provide additional information about the quality of the model estimations (Hair et al., 2017). A change in the R^2 value when a construct is removed is analyzed to determine if the change has a substantive effect. The measurement of this change is the f^2 effect size. Values of 0.02, 0.15, and 0.35 are considered small, medium, and large effect sizes, respectively. Table 20 presents the f^2 effect size calculations results for the control and experimental group variables.

Table 20

Variable f^2 Effect Size

	Control Group		Experimental Group	
	Behavioral Intention	Effect Size	Behavioral Intention	Effect Size
Formal Sanction Certainty	0.073	Medium	0.003	Small
Formal Sanction Severity	0.025	Medium	0.076	Medium
Informal Sanction Certainty	0.002	Small	0.033	Medium
Informal Sanction Severity	0.000	Small	0.009	Small
Perceived Severity	0.008	Small	0.044	Medium
Perceived Vulnerability	0.038	Medium	0.003	Small
Response efficacy	0.167	Large	0.012	Small
Self-efficacy	0.496	Large	0.202	Large

Only the Self-efficacy variable for the experimental group has a large effect size. For the control group, the response efficacy and self-efficacy variables had a large effect size. The remaining variables for both groups had either small or medium effect sizes. Calculation of the q^2 effect sizes is calculated using the previously defined Q^2 values. Because the q^2 effect size calculation uses the difference in the Q^2 values and only one variable had a positive Q^2 value, calculation of the q^2 effect sizes was not possible. A final inter-group response difference statistical analysis will be the final step of the study results.

Group Difference Analysis

Because the study includes two groups of participants, a comparison of group survey responses was performed to analyze statistical differences between the groups. For each construct, a comparison was made between the response mean and the standard deviation. An algorithm described by Aczel and Sounderpandian (2006) for calculating a *Z* test statistic compared the statistical difference between two means. The mean statistical difference test used a null hypothesis assuming there was no statistical difference between the means. Elements included in the algorithm were construct mean and standard deviation, significance level, and sample size. A 95% significance level and sample size of 71 and 72 for the control and experimental groups, respectively, were used for all calculations. Table 21 presents a summary of the mean statistical difference *Z* test calculations.

Table 21

Construct Mean Statistical Difference Comparison

	Control Group		Experimental Group			
	Mean μ_1	Standard Deviation	Mean μ_2	Standard Deviation	p-value	μ_1-μ_2=0
Behavioral_intention_1	4.704	0.758	4.611	0.657	0.433	Not Reject
Behavioral_intention_2	4.676	0.765	4.431	0.779	0.058	Not Reject
Behavioral_intention_3	4.521	0.853	4.375	0.716	0.268	Not Reject
Self-efficacy_1	4.479	0.802	4.542	0.644	0.605	Not Reject
Self-efficacy_2	4.366	0.953	4.125	0.849	0.110	Not Reject
Self-efficacy_3	4.310	1.001	4.153	0.952	0.337	Not Reject
Perceived_Severity_1	4.211	1.006	4.153	0.908	0.718	Not Reject
Perceived_Severity_2	4.437	0.945	4.458	0.744	0.883	Not Reject
Perceived_Severity_3	4.577	0.725	4.347	0.819	0.075	Not Reject
Perceived_Vulnerability_1	3.887	1.015	3.667	1.041	0.201	Not Reject
Perceived_Vulnerability_2	4.183	0.969	4.319	0.779	0.355	Not Reject
Perceived_Vulnerability_3	3.930	1.117	3.819	0.962	0.525	Not Reject
Response_efficacy_1	4.127	0.933	3.875	0.985	0.116	Not Reject
Response_efficacy_2	4.535	0.766	4.472	0.707	0.609	Not Reject
Response_efficacy_3	4.521	0.767	4.278	0.768	0.058	Not Reject
Formal_sanctions_certainty_1	4.014	1.193	4.125	0.957	0.540	Not Reject
Formal_sanctions_certainty_2	4.070	1.142	4.181	0.918	0.522	Not Reject
Formal_sanctions_certainty_3	4.268	1.034	4.194	0.892	0.647	Not Reject
Formal_sanctions_severity_1	4.366	1.065	4.236	0.874	0.425	Not Reject
Formal_sanctions_severity_2	4.380	1.053	4.042	1.020	0.051	Not Reject
Formal_sanctions_severity_3	4.296	1.093	4.000	0.943	0.083	Not Reject
Informal_sanctions_certainty_1	4.113	1.082	3.903	1.069	0.243	Not Reject
Informal_sanctions_certainty_2	4.155	1.109	4.181	1.058	0.886	Not Reject
Informal_sanctions_certainty_3	4.268	1.006	4.181	0.976	0.600	Not Reject
Informal_sanctions_severity_1	4.042	1.261	3.917	1.010	0.513	Not Reject
Informal_sanctions_severity_2	4.268	1.174	4.000	1.080	0.156	Not Reject
Informal_sanctions_severity_3	4.099	1.246	3.903	1.095	0.318	Not Reject

Results of the *Z* test statistic indicated no p-value was less than 0.05 indicating there was no statistical difference between the means and could not reject the null hypothesis for all constructs.

Hypotheses Testing

Path coefficient values and their corresponding statistical significance were used for hypotheses testing. These values would determine if a null hypothesis was rejected or not rejected. For the reader's convenience Table 22 and Table 23 repeat the presentation of the path coefficient values of the control and experimental groups, respectively.

Table 22

Control Group Path Coefficient Statistics

Control Group	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	t Statistics (|O/STDEV|)	p Values	Significance ($p < 0.05$)
Formal Sanction Certainty -> Behavioral Intention	-0.22	-0.205	0.112	1.964	0.050	No
Formal Sanction Severity -> Behavioral Intention	0.148	0.139	0.135	1.092	0.276	No
Informal Sanction Certainty -> Behavioral Intention	0.063	0.065	0.162	0.392	0.695	No
Informal Sanction Severity -> Behavioral Intention	-0.012	0.002	0.123	0.100	0.920	No
Perceived Severity -> Behavioral Intention	0.084	0.088	0.126	0.668	0.505	No
Perceived Vulnerability -> Behavioral Intention	0.16	0.149	0.109	1.470	0.142	No
Response efficacy -> Behavioral Intention	0.332	0.306	0.133	2.495	0.013	Yes
Self-efficacy -> Behavioral Intention	0.467	0.472	0.103	4.524	0.000	Yes

Table 23

Experimental Group Path Coefficient Statistics

Experimental Group	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	t Statistics (|O/STDEV|)	p Values	Significance ($p < 0.05$)
Formal Sanction Certainty -> Behavioral Intention	0.066	0.061	0.158	0.416	0.678	No
Formal Sanction Severity -> Behavioral Intention	-0.353	-0.344	0.182	1.943	0.053	No
Informal Sanction Certainty -> Behavioral Intention	0.248	0.207	0.203	1.222	0.222	No
Informal Sanction Severity -> Behavioral Intention	0.124	0.152	0.198	0.629	0.53	No
Perceived Severity -> Behavioral Intention	0.245	0.244	0.165	1.479	0.14	No
Perceived Vulnerability -> Behavioral Intention	0.05	0.044	0.111	0.454	0.65	No
Response efficacy -> Behavioral Intention	0.115	0.12	0.203	0.568	0.57	No
Self-efficacy -> Behavioral Intention	0.373	0.381	0.143	2.599	0.01	Yes

Hypotheses analysis begins with the control group.

RQ1–What is the effect of informal sanction certainty on individual's behavioral intention to comply with information security policies?

$H_0$1: Informal sanction certainty will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a1: Informal sanction certainty will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

Each of the constructs used a 5-point Likert scale for participant responses. The path coefficient for informal sanction certainty was -0.063 with a p-value of .392 indicating the path coefficient was not significant. Because the path coefficient was not significant, H_a1 was rejected, and $H_0$1 was not rejected. This result indicated informal sanction certainty did not have an effect on an individual's information security policy compliance behavioral intention.

RQ2–What is the effect of informal sanction severity on an individual's behavioral intention to comply with information security policies?

$H_0$2: Informal sanction severity will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a2: Informal sanction severity will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

The path coefficient for informal sanction severity was -0.012 with a p-value of .920 indicating the path coefficient was not significant. Because the path coefficient was

not significant, H_a2 was rejected, and H_02 was not rejected. This result indicated informal sanction severity did not have a positive effect on an individual's information security policy compliance behavioral intention.

RQ3–What is the effect of formal sanction certainty on an individual's behavioral intention to comply with information security policies?

H_03: Formal sanction certainty will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a3: Formal sanction certainty will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

The path coefficient for formal sanction certainty was -0.220 with a p-value of .050 indicating the path coefficient was not significant. Because the path coefficient was not significant, H_a3 was rejected, and H_03 was not rejected. This result indicated formal sanction certainty did not have a positive effect on an individual's information security policy compliance behavioral intention.

RQ4–What is the effect of formal sanction severity on an individual's behavioral intention to comply with information security policies?

H_04: Formal sanction severity will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a4: Formal sanction severity will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

The path coefficient for formal sanction severity was 0.148 with a p-value of .276 indicating the path coefficient was not significant. Because the path coefficient was not

significant, H_a4 was rejected, and H_04 was not rejected. This result indicated formal sanction severity did not have a positive effect on an individual's information security policy compliance behavioral intention.

RQ5–What is the effect of perceived threat vulnerability on an individual's behavioral intention to comply with information security policies?

H_05: Perceived threat vulnerability will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a5: Perceived threat vulnerability will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

The path coefficient for perceived threat vulnerability was 0.160 with a p-value of .142 indicating the path coefficient was not significant. Because the path coefficient was not significant, H_a5 was rejected, and H_05 was not rejected. This result perceived threat vulnerability did not have a positive effect on an individual's information security policy compliance behavioral intention.

RQ6–What is the effect of perceived threat severity on an individual's behavioral intention to comply with information security policies?

H_06: Perceived threat severity will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a6: Perceived threat severity will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

The path coefficient for perceived threat severity was 0.084 with a p-value of .505 indicating the path coefficient was not significant. Because the path coefficient was not

significant, H_a6 was rejected, and H_06 was not rejected. This result indicated perceived threat severity did not have a positive effect on an individual's information security policy compliance behavioral intention.

RQ7–What is the effect of response efficacy on an individual's behavioral intention to comply with information security policies?

H_07: Response efficacy will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a7: Response efficacy will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

The path coefficient for response efficacy was 0.332 with a p-value of .013 indicating the path coefficient was significant. Because the path coefficient was significant, H_a7 was not rejected, and H_07 was rejected. This result indicated response efficacy did have a positive effect on an individual's information security policy compliance behavioral intention.

RQ8–What is the effect of self-efficacy on an individual's behavioral intention to comply with information security policies?

H_08: Self-efficacy will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a8: Self-efficacy will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

The path coefficient for self-efficacy was 0.467 with a p-value of 0.000 indicating the path coefficient was significant. Because the path coefficient was significant, H_a8 was

not rejected, and H_{08} was rejected. This result indicated self-efficacy did have a positive effect on an individual's information security policy compliance behavioral intention. Hypotheses analysis continues with the experimental group.

RQ1–What is the effect of informal sanction certainty on individual's behavioral intention to comply with information security policies?

$H_0$1: Informal sanction certainty will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a1: Informal sanction certainty will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

The path coefficient for informal sanction certainty was 0.248 with a p-value of .222 indicating the path coefficient was not significant. Because the path coefficient was not significant, H_a1 was rejected, and $H_0$1 was not rejected. This result indicated informal sanction certainty did not have an effect on an individual's information security policy compliance behavioral intention.

RQ2–What is the effect of informal sanction severity on an individual's behavioral intention to comply with information security policies?

$H_0$2: Informal sanction severity will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a 2: Informal sanction severity will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

The path coefficient for informal sanction severity was 0.124 with a p-value of .530 indicating the path coefficient was not significant. Because the path coefficient was

not significant, H_a2 was rejected, and H_02 was not rejected. This result indicated informal sanction severity did not have an effect on an individual's information security policy compliance behavioral intention.

RQ3–What is the effect of formal sanction certainty on an individual's behavioral intention to comply with information security policies?

H_03: Formal sanction certainty will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a3: Formal sanction certainty will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

The path coefficient for formal sanction certainty was 0.660 with a p-value of 0.678 indicating the path coefficient was not significant. Because the path coefficient was not significant, H_a3 was rejected, and H_03 was not rejected. This result indicated formal sanction certainty did not have an effect on an individual's information security policy compliance behavioral intention.

RQ4–What is the effect of formal sanction severity on an individual's behavioral intention to comply with information security policies?

H_04: Formal sanction severity will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a4: Formal sanction severity will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

The path coefficient for formal sanction severity was -0.353 with a p-value of .053 indicating the path coefficient was not significant. Because the path coefficient was

not significant, H_a4 was rejected, and H_04 was not rejected. This result indicated formal sanction severity did not have a positive effect on an individual's information security policy compliance behavioral intention.

RQ5–What is the effect of perceived threat vulnerability on an individual's behavioral intention to comply with information security policies?

H_05: Perceived threat vulnerability will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a5: Perceived threat vulnerability will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

The path coefficient for perceived threat vulnerability was 0.050 with a p-value of .650 indicating the path coefficient was not significant. Because the path coefficient was not significant, H_a5 was rejected, and H_05 was not rejected. This result perceived threat vulnerability did not have a positive effect on an individual's information security policy compliance behavioral intention.

RQ6–What is the effect of perceived threat severity on an individual's behavioral intention to comply with information security policies?

H_06: Perceived threat severity will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a6: Perceived threat severity will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

The path coefficient for perceived threat severity was 0.245 with a p-value of .140 indicating the path coefficient was not significant. Because the path coefficient was not

significant, H_a6 was rejected, and H_06 was not rejected. This result indicated perceived threat severity did not have a positive effect on an individual's information security policy compliance behavioral intention.

RQ7–What is the effect of response efficacy on an individual's behavioral intention to comply with information security policies?

H_07: Response efficacy will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a7: Response efficacy will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

The path coefficient for response efficacy was 0.115 with a p-value of .570 indicating the path coefficient was not significant. Because the path coefficient was not significant, H_a7 was rejected, and H_07 was not rejected. This result indicated response efficacy did not have a positive effect on an individual's information security policy compliance behavioral intention.

RQ8–What is the effect of self-efficacy on an individual's behavioral intention to comply with information security policies?

H_08: Self-efficacy will have a nonpositive affect on an individual's information security policy compliance behavioral intention.

H_a8: Self-efficacy will have a statistically significant positive affect on an individual's information security policy compliance behavioral intention.

The path coefficient for self-efficacy was 0.373 with a p-value of 0.010 indicating the path coefficient was significant. Because the path coefficient was significant, H_a8 was

not rejected, and $H_0$8 was rejected. This result indicated self-efficacy did have a positive effect on an individual's information security policy compliance behavioral intention.

Summary

Data collection began with the development of an online survey and distributed to SurveyMonkey audience participants. A suspension of the survey occurred because of excessive survey abandonment, and an insufficient number of completed responses were received. The survey was distributed to SurveyMonkey audience participants a second time to obtain additional responses. Data analysis started with descriptive statistics of the control and experimental groups' demographics and responses. Survey responses were further analyzed using partial least squares-structural equation modeling. Results from this analysis provided information related to the quality of the measurement and structural models. Path coefficients calculated during the partial least squares-structural equation modeling process were used to test each research question and hypothesis. Hypotheses testing indicated the response efficacy and self-efficacy research questions in the control group and the self-efficacy research questions in the experimental group were statistically significant. Results of the hypotheses testing also indicated the remaining hypotheses were not statistically significant for both participant groups and not supported by the data.

Chapter 5 includes a summary of the statistical results and interpretation of the findings. The interpretation also includes a discussion on the lack of statistically significant results for many of the variables. Following the interpretation of the findings is a discussion on study limitations, recommendations, and implications. Included in the

implication discussion is a description of the effect of this research on social change. Chapter 5 closes with the conclusions developed as a result of this study.

Chapter 5: Discussion, Conclusions, and Recommendations

Interpretation of Findings

Interpretation of the findings begins where the data analysis ended, examining the statistical differences between the two study groups. These statistical differences may provide a basis for understanding the finding of other areas of the study. Table 21 presents a comparison of the construct response means. For all of the study constructs, there was no statistically significant difference between the responses from the control and experimental groups. One reason for this lack of statistically significant difference between the groups could be the fear appeal presented in the experimental treatment did not invoke a change in motivation to comply with an organization's information security policies. Rogers (1975) noted a communication with a high level of fear appeal has a greater influence on motivation than a low level of fear appeal. Because there was no statistically significant difference between the group receiving the experimental treatment and the group that did not receive the experimental treatment, the fear appeal contained in the experimental treatment may not have aroused an emotion sufficient enough to influence an individual's behavior. A similar outcome was identified by Boss et al. (2015) in a study incorporating a high and a low-level fear appeal. Boss et al. found that a high-level fear appeal had two times the influence on behavioral intention than a low-level fear appeal. The Boss et al. high-level fear appeal model constructs all had a significant influence on behavioral intention. The high-level fear appeal significance contrasted with the Boss et al. low-level fear appeal model where some of the constructs did not have a significant influence on behavioral intention.

Another reason for the lack of construct response statistically significant difference could have been the selected population of information technology professionals. Construct responses from the control group indicated a high level of information security policy compliance. Many of the control group construct response averages were between four and five. Both groups had a high level of information security policy awareness, 95.8% for the control group and 93.1% for the experimental group. Given this high level of information security policy awareness, the fear appeal in the experimental treatment may not have been sufficient enough to increase information security policy behavioral intention for information technology professionals. The next step in the interpretation of the findings was examining the validity of the partial least squares-structural equation modeling model, starting with the measurement model.

Determining measurement model validity includes examining the results from Cronbach's alpha, composite reliability, indicator reliability, average variance extracted, cross loadings, and Fornell-Larcker criteria calculations (Hair et al., 2017). Table 8 presents the Cronbach's alpha calculation results. All of the results, except one variable in one group, exceeded the 0.700 threshold. The value of the single exception was .695 close enough to be considered acceptable. All of the composite reliability results presented in Table 9 exceeded the 0.700 threshold and are considered acceptable. Several of the composite reliability values exceeded the 0.950 threshold. All of the constructs are measuring the same thing and may not be a valid measure (Hair et al., 2017). Given the one item that was only slightly below the threshold and the remaining Cronbach's alpha

and composite reliability values exceeded the recommended thresholds, demonstrating internal consistency of the model.

Indicator reliability and average variance extracted value results are used to determine convergent validity. Indicator reliability, or outer loadings, results were presented in Table 10. Except for three outer loadings results, all of the outer loadings exceeded the recommended 0.708 threshold. Indicators with a value of 0.40 to 0.70 should be considered for removal. Removal of an indicator should be done to ensure that there are no reductions in the composite reliability and average variances values (Hair et al., 2017). Removal of indicators to determine the effects of their removal was beyond the scope of this study. Table 11 presents the average variance extracted values. All of the values exceed the recommended 0.50 threshold. Except three of the outer loadings, all of the values exceeded their respective threshold and demonstrated convergent validity.

Construct cross loadings and Fornell-Larcker criterion analyses are used to determine discriminant validity. A review of the cross loadings presented in Table 12 and Table 13 indicated that all but two cross loadings were greater than their corresponding variable cross loadings. This result demonstrates discriminant validity for a majority of the constructs. A second approach to determining discriminant validity is the Fornell-Larcker criterion. When the indicator values are greater than the correlation with the remaining variables, discriminant validity is demonstrated (Hair et al., 2017). All control group Fornell-Larcker criterion presented in Table 14 and all experimental group Fornell-Larcker criterion presented in Table 15 have indicator values that are greater than the remaining variable correlation values demonstrating discriminant validity.

Taking a holistic view of the measurement model validity analyses, with a few exceptions, internal consistency, convergent validity, and discriminant validity demonstrated model validity. The measurement model was validated by a majority of the analyses conducted. Several individual calculations were outside the acceptable range with some inconsistencies between the control and experimental groups and between tests. These inconsistencies offer an opportunity for investigation by future researchers. Following the interpretation of the measurement model is an interpretation of the results from the structural model analysis.

Analysis of the structural model included calculating coefficients of determination, predictive relevance, size and significance of the path coefficients, and f^2 and q^2 effect sizes. Calculating the R^2 determines the coefficient of determination value for the model. For this study, the R^2 value for the control group was 0.752 and 0.540 for the experimental group. An R^2 value of 0.20 is considered acceptable for behavioral studies (Hair et al., 2017). Johnston et al. (2015) examined the effect of a fear appeal using constructs from both protection motivation theory and deterrence theory. An R^2 value of 0.32 was the result of the calculation for the model examining compliance behavioral intention (Johnston et al., 2015). In another study using protection motivation theory, the model used by Johnston and Warkentin (2010) had an R^2 value of 0.271. Siponen and Vance (2010) developed a model using deterrence theory and the model analysis produced an R^2 value of 0.470. The R^2 value of both the control and experimental groups exceeded the level recommended by Hair et al. and the other model

values found in the literature. Because the study R^2 values exceeded these benchmark values, both the control and experimental groups R^2 values are considered acceptable.

The model Q^2 values determine predictive relevance. Table 15 presents the construct crossvalidated redundancy report. The Q^2 value for behavioral intention is 0.562 for the control group and 0.351 for the experimental group. Values of Q^2 greater than zero indicate the model's predictive relevance is acceptable (Hair et al., 2017). Because both the control and experimental groups' Q^2 values exceed zero, the model's predictive relevance is acceptable. Other studies examined for comparison of results did not report a Q^2 value.

Tables 16 and 17 presents the model path coefficients and their associated statistical significance. For the control group, the path coefficients for response efficacy and self-efficacy are statistically significant. For the experimental group, only the self-efficacy path coefficient is statistically significant. Boss et al. (2015) had a similar result in a study examining a fear appeal. Two levels of fear appeal, high and low, were used as an experimental treatment to examine their effect on students. Results of the low fear appeal model analysis indicated nonsignificant path coefficients for most of the relationships. A similar situation could be occurring with this dissertation study. The fear appeal included in the experimental treatment could be considered low for the information technology population used in the study. A low fear appeal could have a small effect on the study population producing nonsignificant model path coefficients.

Table 18 presents the model f^2 effect sizes. Both response efficacy and self-efficacy had a large effect size for the control group. For the experimental group, self-

efficacy had a large effect size. In both cases, variables with large effect sizes matched the significant path coefficients of each model. No effect size calculation for q^2 was possible because the individual variable Q^2 values were not greater than zero.

Although the model had an acceptable R^2 value and predictive relevance, the path coefficient relevance and the effect sizes indicated the self-efficacy variable made a statistically significant contribution and the remaining seven variables did not make a statistically significant contribute to the model. Self-efficacy's statistically significant contribution could be related to information technology professional confidence in complying with information security policies. A possible explanation for the nonstatistcally significant findings could be the fear appeal communication did not cause a change in the participants' motivation because the effect of the fear appeal was low. An analysis of the intergroup responses indicated there was not a statistically significant difference between the groups' responses. Information technology professionals could already possess a high level of information security policy awareness, and a low level fear appeal communication may not change an individual's compliance intention.

Limitations of the Study

Study limitations described in Chapter 1 included relying on participants self-reporting their responses, demographic accuracy, and possible bias introduced by the study population. Participants self-reported their responses to the survey and actual measure of behavioral attention were not included in the study. The survey did not request additional participant demographic information. SurveyMonkey provided all participant demographic information. Because the study population was information

technology professionals, this might introduce bias into the results. Information technology professionals could have a higher level of information security policy awareness. An analysis of the participant responses indicated there was not a statistically significant difference in the construct responses. A lack of statistically significant differences between the group responses could support the argument that information technology professionals could have a higher level of information security policy awareness. The introduction of this information security policy awareness bias is a limitation of the study. These results may not be generalizable to the general public because information technology professionals could possess a greater behavioral intention to comply with information security policies. Another limitation discovered during the study is the possible low-level fear appeal communication. A low level fear appeal would not provide sufficient motivation to change an individual's behavior. Because a low-level fear appeal would not change an individual's behavior, this could also account for the lack of statistically significant difference between the control and experimental groups' construct responses.

Recommendations

Results of the measurement model and the structural model analysis indicated the model was acceptable. Participant construct response analysis indicated there was not a statistically significant difference between the groups. It is recommended future research include a different population to address this issue. Selecting a population that does not include information technology professionals may eliminate the possible bias introduced by this population. Because information technology professionals may possess a greater

level of information security policy compliance behavioral intention, excluding information technology professionals from the population may result in statistically significant differences between the group responses. The lack of a statistically significant difference between the study groups may also be related to using a low-level fear appeal. A recommendation to resolve this problem could be to develop a more strongly worded fear appeal communication. This type of fear appeal could provide a greater emotional response to motivate a change in behavior. It may be difficult to determine if a fear appeal communication is strong enough to get the required response. A recommendation to verify the effect of a fear appeal communication is to conduct one or more pilot studies. Pilot studies could help to develop a strong fear appeal communication. Another recommendation addresses the problems encountered during the data collection process.

During the data collection process, SurveyMonkey identified some problems with the survey and survey process. A problem with the survey identified by SurveyMonkey support was the length of the consent form. SurveyMonkey provides survey construction guidelines, and one guideline is the length of the consent form. The SurveyMonkey guideline recommends a maximum of 250 characters for the consent form (SurveyMonkey Audience for Academics, 2016). The consent form used in the survey contained about 500 words. SurveyMonkey support recommended changing the consent form, but because the survey used an Institutional Review Board (IRB) approved consent form, the consent form was not modified. A recommendation to develop a smaller consent form for studies using the SurveyMonkey audience could mitigate this problem. A smaller consent form may reduce the number of abandoned surveys. If the

abandonment rate is excessive, SurveyMonkey will suspend the survey. Another issue identified by SurveyMonkey support was the applicability of using the SurveyMonkey audience for academic surveys. It is difficult to determine if the consent form length or the appropriateness of the SurveyMonkey audience contributed to the high survey abandonment rate. I anticipated SurveyMonkey audience members would be more receptive to completing surveys because they have volunteered to become survey recipients. A recommendation for future research is to not use SurveyMonkey audience participants for academic research. Selecting a group outside of the SurveyMonkey audience may be a better population for academic research. A change in the demographic information collection is also recommended to increase the level of data analysis.

SurveyMonkey provides a limited amount of respondent demographic information. By requesting demographic information as part of the survey, obtaining additional detail information on the participants is possible. Age demographic information provided in the SurveyMonkey information was age ranges and not the participant's age in years. By analyzing individual ages instead of age ranges may allow researchers greater insight to the respondents.

The discussion included several recommendations for future researchers. These recommendations included changes to the study population, stronger fear appeal communication, and survey changes. A change in the population away from information technology professionals may reduce information security policy compliance bias. A strongly worded fear appeal communication may produce the emotion needed to change an individual's behavior. If possible, modify the consent form to meet the SurveyMonkey

guidelines. Changing the survey participants to a population outside of the SurveyMonkey audience may improve the survey response rate. Adding additional demographic information requests to the survey may provide additional details about the participant. All of the recommendations suggested are intended to improve the research and data analysis of future studies.

Implications

An information technology professional's noncompliance with information security policy could result in inadequate information security. Threats to the United States' critical cyber infrastructure from cybercriminals are constantly increasing. By conducting this study, information could be added to the body of knowledge and assist with mitigating the problem of information security noncompliance. Information security policy compliance by information technology professionals is crucial to the security of electronic data. An examination of information security policy compliance behavioral intention could promote social change in information security and contribute to securing the country's critical cyber infrastructure.

A gap in the literature existed related to studies of information security policy compliance behavioral intention combining protection motivation theory and deterrence theory. This study provided a theoretical contribution by demonstrating the applicability of research models merging the constructs of protection motivation theory and deterrence theory to exam information security compliance behavioral intention. An experimental contribution made by the study is how important a fear appeal communication is to motivating behavioral change. As was demonstrated in the study, a low level fear appeal

communication will not produce the necessary behavioral change. Identifying the level of a fear appeal communication also has practical implications.

Management using a fear appeal communication to motivate a change in information security policy compliance should ensure the communication produces the desired results. A low level fear appeal communication will have little to no effect on motivating an individual to change his or her behavior. This study has a practical implication for the development of an appropriate fear appeal communication. A methodology was presented for testing a fear appeal communication before implementation. Through the use of two groups, a fear appeal communication, and a survey, management can test the fear appeal communication appropriateness to verify the fear appeal results. There are also implications for future academic researchers.

Some recommendations were made to assist future researchers. In addition to the theoretical contributions and practical implications, future researchers should incorporate some of the recommendations to improve their online survey technique. Creating a survey that complies with the online survey provider guidelines can improve the survey response rate. Determining the appropriateness of the population and survey respondents is important to a successful online survey data collection process. Learning more about the expectations of the survey participants may help in the design of an online survey.

Improving information security is an important management objective. Conducting a study examining information security policy compliance behavioral intention has both theoretical and practical implications. Conducting this study made a contribution to the theoretical knowledge base. This study also provided a practical

methodology for developing information security policy compliance communications. Researchers also benefited from the study by learning from the recommendations to improve future research.

Social Change Impact

Vance et al. (2012) identified information security policy noncompliance as the cause for a majority of the information security breaches. Positive social change could be achieved by changing the information security behaviors of information technology professionals. Increasing the information security policy compliance behaviors of information technology professionals could result in improved information security and information asset protection. Improved information security policy compliance behavior could promote positive social change in information technology security and contribute to securing society's critical information assets.

Conclusions

Encountering an unexpected outcome may provide a greater learning experience than an expected outcome. Building on the work of others is the foundation of academic research. The purpose of this quantitative experimental study was to examine a combination of protection motivation theory and deterrence theory constructs that relate to the information security policy behavioral intention of information technology professionals. A research model was developed to test the effect of a fear appeal communication on motivating a behavioral change. Testing of the research model indicated it was appropriate for the study, but achieved an unintended result. The data analysis indicated there was no change in behavior. Although this was not the expected

result, the result provided insight into the effect of the fear appeal communication. By not obtaining the desired result, more was learned about the topic. Sharing this information improved insight with the desire to increase the knowledge on information security policy compliance behavior. Future researchers can build on the knowledge to offer additional information security behavior improvements and contribute to the information security knowledgebase.

References

Aczel, A. D., & Sounderpandian, J. (2006). *Complete business statistics*. Boston, MA: McGraw-Hill.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. Retrieved from http://www.journals.elsevier.com/organizational-behavior-and-human-decision-processes/

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

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613-643, A1-A15. Retrieved from http://www.misq.org

Beccaria, C. (1819). *An essay on crimes and punishments* (E. Ingraham, Trans.). Philadelphia, PA: Philip H. Nicklin.

Bentham, J. (1907). *An introduction to the principles of morals and legislation*. Oxford, England: Clarendon Press.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837-864. Retrieved from http://misq.org/

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548. Retrieved from http://misq.org/

Buying Responses with SurveyMonkey Audience. (2017) Retrieved from https://help.surveymonkey.com/articles/en_US/kb/SurveyMonkey-Audience

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. http://dx.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. http://dx.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*, 447-459. http://dx.doi.org/10.1016/j.cose.2013.09.009

Chu, A. M., & Chau, P. Y. (2014). Development and validation of instruments of information security deviant behavior. *Decision Support Systems*, *66*, 93-101. http://dx.doi.org/10.1016/j.dss.2014.06.008

Creswell, J. W. (2008). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research*. Upper Saddle River, NJ: Pearson/Merrill Prentice Hall.

Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database, 45*(4), 51-71. http://dx.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. http://dx.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. http://dx.doi.org/10.2308/isys-50704

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. http://dx.doi.org/10.1016/j.cose.2014.11.002

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences, 43*(6), 1091-1124. http://dx.doi.org/10.1111/j.1540-5915.2012.00383.x

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. http://dx.doi.org/10.1057/ejis.2011.23

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196-207. https://doi.org/10.1016/j.cose.2009.09.002

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

Furnell, S., & Rajendran, A. (2012). Understanding the influences on information security behaviour. *Computer Fraud & Security, 2012*(3), 12-15. http://dx.doi.org/10.1016/s1361-3723(12)70053-2

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems, 16*(1), 91-109. http://aisel.aisnet.org/cais/

Godlove, T. (2012). Examination of the factors that influence teleworkers' willingness to comply with information security guidelines. *Information Security Journal: A Global Perspective, 21*(4), 216-229. http://dx.doi.org/10.1080/19393555.2012.668747

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Thousand Oaks, CA: Sage Publications.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing theory and Practice*, *19*(2), 139-152. https://doi.org/10.2753/mtp1069-6679190202

Hair, J. F., Sarstedt, M., Pieper, T. M., & Ringle, C. M. (2012). The use of partial least squares structural equation modeling in strategic management research: A review of past practices and recommendations for future applications. *Long range planning*, *45*(5), 320-340. https://doi.org/10.1016/j.lrp.2012.09.008

Hickey, K. T., Hodges, E. A., Thomas, T. L., Coffman, M. J., Taylor-Piliae, R. E., Johnson-Mallard, V. M., & Gates, M. G. (2014). Initial evaluation of the Robert Wood Johnson foundation nurse faculty scholars program. *Nursing Outlook*, *62*(6), 394-401. http://dx.doi.org/10.1016/j.outlook.2014.06.004

Hobbes, T. (1904). *Leviathan: Or, The matter, forme & power of a commonwealth, ecclesiasticall and civil*. Cambridge, England: University Press.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management*, *49*(2), 99-110. http://dx.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. http://dx.doi.org/10.7763/ijiet.2015.v5.522

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95. http://dx.doi.org/10.1016/j.cose.2011.10.007

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

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549-566. Retrieved from http://misq.org/

Johnston, A. C., Warkentin, M., & Siponen, M. T. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, *39*(1), 113-134. Retrieved from http://www.misq.org/

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. http://dx.doi.org/10.1155/2014/463870

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

Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems*, *50*(2), 361-369. http://dx.doi.org/10.1016/j.dss.2010.07.009

Menard, P., Gatlin, R., & Warkentin, M. (2014). Threat protection and convenience: Antecedents of cloud-based data backup. *Journal of Computer Information Systems*, *55*(1), 83-91. http://dx.doi.org/10.1080/08874417.2014.11645743

Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. *Journal of Information Privacy and Security*, *9*(1), 47-67. http://dx.doi.org/10.1080/15536548.2013.10845672

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

Onwudiwe, I., Odo, J. & Onyeozili, E. (2005). Deterrence theory. In M. Bosworth (Ed.), *Encyclopedia of Prisons & Correctional Facilities* (Vol. 2, pp. 234-237). Thousand Oaks, CA: SAGE Publications Ltd. http://dx.doi.org/10.4135/9781412952514.n91

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security*, *31*(5), 673-680. http://dx.doi.org/10.1016/j.cose.2012.04.004

Piggin, R. (2014). Industrial systems: Cyber-security's new battlefront. *Engineering & Technology*, *9*(8), 70-74. https://doi.org/10.1049/et.2014.0810

Posey, C., Roberts, T. L., Lowry, P. B., & 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. http://dx.doi.org/10.2139/ssrn.2418233

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34*(4), 757-778. Retrieved from http://misq.org/

Reitz, O. E., & Anderson, M. A. (2013). A comparison of survey methods in studies of the nurse workforce. *Nurse researcher, 20*(4), 22-27. http://dx.doi.org/10.7748/nr2013.03.20.4.22.e286

Ringle, C. M., Sarstedt, M., & Straub, D. (2012). A critical look at the use of PLS-SEM in MIS Quarterly. *MIS Quarterly, 36*(1). Retrieved from http://misq.org/

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

Rogers, R.W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), *Social Psychophysiology*. New York, NY: Guilford Press.

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. http://dx.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. C*omputers & Security*, *56*, 70-82. https://doi.org/10.1016/j.cose.2015.10.006

Shackelford, S. J., Proia, A. A., Martell, B., & Craig, A. N. (2015). Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. *Texas International Law Journal*, *50*(2), 305-355. Retrieved from http://www.tilj.org/content/journal/50/14%20SHACKELFORD%20PUB%20PROOF.pdf

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177-191. http://dx.doi.org/10.1016/j.cose.2015.01.002

Singleton, R., & Straits, B. C. (2010). *Approaches to social research*. New York, NY: Oxford University Press.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224. http://dx.doi.org/10.1016/j.im.2013.08.006

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: An empirical study. *IFIP International Federation for Information Processing*, 133–144. http://dx.doi.org/10.1007/978-0-387-72367-9_12

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487-502. Retrieved from http://misq.org/

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. http://dx.doi.org/10.1108/imcs-08-2012-0045

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, *48*(7), 296-302. http://dx.doi.org/10.1016/j.im.2011.07.002

Stanwick, P. A., & Stanwick, S. D. (2014). A security breach at target: A different type of bulls eye. *International Journal of Business and Social Science, 5*(12), 61-64. Retrieved from http://ijbssnet.com/

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255-276. http://dx.doi.org/10.1287/isre.1.3.255

Straub, D. W., Carlson, P. J., & Jones, E. H. (1993). Deterring cheating by student programmers: A field experiment in computer security. *Journal of Management Systems*, *5*(1), 33-48. Retrieved from http://www.aom-iaom.org/jms.html

Straub D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, 45-60. Retrieved from http://misq.org/

SurveyMonkey Audience's Answers to the ESOMAR 28 Questions. (2013). Retrieved from http://help.surveymonkey.com/servlet/servlet.FileDownload?file=01530000002gvZ9

SurveyMonkey Audience for Academics. (2016). Retrieved from http://help.surveymonkey.com/articles/en_US/kb/How-do-Academics-use-SurveyMonkey-Audience

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

Symonds, E. (2011). A practical application of SurveyMonkey as a remote usability-testing tool. *Library Hi Tech*, *29*(3), 436-445. http://dx.doi.org/10.1108/07378831111174404

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. http://dx.doi.org/10.1016/j.cose.2016.02.009

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management*, *52*(4), 506-517. http://dx.doi.org/10.1016/j.im.2015.03.002

Urbach, N., & Ahlemann, F. (2010). Structural equation modeling in information systems research using partial least squares. *Journal of Information Technology Theory and Application*, *11*(2), 5-40. Retrieved from http://aisel.aisnet.org/jitta/

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3), 190-198. http://dx.doi.org/10.1016/j.im.2012.04.002

Vagias, W. M. (2006). *Likert-type scale response anchors*. Clemson International Institute for Tourism & Research Development, Department of Parks, Recreation and Tourism Management. Clemson University. Retrieved from https://www.clemson.edu/centers-institutes/tourism/documents/sample-scales.pdf

Wall, J. D., Palvia, P., & Lowry, P. B. (2013). Control-related motivations and information security policy compliance: The role of autonomy and efficacy. *Journal of Information Privacy and Security*, *9*(4), 52-79. http://dx.doi.org/10.1080/15536548.2013.10845690

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, *59*(4), 329-349. http://dx.doi.org/10.1080/03637759209376276

Wright, W., & Khatri, N. (2015). Bullying among nursing staff: Relationship with psychological/behavioral responses of nurses and medical errors. *Health Care Management Review*, *40*(2), 139-147. http://dx.doi.org/10.1097/hmr.0000000000000015

Yoon, C., Hwang, J. W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education*, *23*(4), 407-415. Retrieved from http://jise.org/

Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. *Information Technology & People*, *26*(4), 401-419. http://dx.doi.org/10.1108/itp-12-2012-0147

Appendix A: Constructs, Statements and Questions

Protection Motivation Theory

Constructs	Item	Source
Behavioral intention 1	I intend to comply with information security polices	Siponen, Mahmood, & Pahnila (2014)
Behavioral intention 2	I intend to recommend others to comply with information security policies	Siponen, Mahmood, & Pahnila (2014)
Behavioral intention 3	I intend to assist others in complying with information security policies	Siponen, Mahmood, & Pahnila (2014)
Self-efficacy 1	I can comply with information security policies by myself	Siponen, Mahmood, & Pahnila (2014)
Self-efficacy 2	I can use information security measures if I can call for help if I get stuck	Siponen, Mahmood, & Pahnila (2014)
Self-efficacy 3	I can use information security measures if someone tells me what to do as I go along	Siponen, Mahmood, & Pahnila (2014)
Perceived Severity 1	An information security breach in my organization would be a serious problem for me	Siponen, Mahmood, & Pahnila (2014)
Perceived Severity 2	An information security breach in my organization would be a serious	Siponen, Mahmood, & Pahnila (2014)
Perceived Severity 3	Information security breaches are becoming more and more serious	Siponen, Mahmood, & Pahnila (2014)
Perceived Vulnerability 1	I could be subjected to a serious information security threat	Siponen, Mahmood, & Pahnila (2014)
Perceived Vulnerability 2	My organization could be subjected to a serious information security threat	Siponen, Mahmood, & Pahnila (2014)
Perceived Vulnerability 3	More and more serious information security threats are being faced by my organization	Siponen, Mahmood, & Pahnila (2014)
Response efficacy 1	The information security personnel in our organization keep information system security breaches down	Siponen, Mahmood, & Pahnila (2014)
Response efficacy 2	Complying with information security policies in our organization keep information system security breaches down	Siponen, Mahmood, & Pahnila (2014)
Response efficacy 3	Having information security policies in our organization keep information system security breaches down	Siponen, Mahmood, & Pahnila (2014)

From "Employees' adherence to information security policies: An exploratory field study," by M. Siponen, M. A. Mahmood, and S. Pahnila, 2014, *Information & Management, 51*(2), pp. 223-224. Copyright 2013 by Elsevier B.V. Used with permission.

Deterrence Theory

Constructs	Item	Source
Formal sanctions—certainty 1	What is the chance you would receive sanctions if you violated the company information security policy?	Siponen & Vance (2010)
Formal sanctions—certainty 2	What is the chance that you would be formally sanctioned if management learned that you had violated company information security policy?	Siponen & Vance (2010)
Formal sanctions—certainty 3	What is the chance that you would be formally reprimanded if management learned you had violated company information security policy?	Siponen & Vance (2010)
Formal sanctions—severity 1	How much of a problem would it be if you received severe sanctions if you violated the company information security policy?	Siponen & Vance (2010)
Formal sanctions—severity 2	How much of a problem would it create in your life if you were formally sanctioned for violating the company information security policy?	Siponen & Vance (2010)
Formal sanctions—severity 3	How much of a problem would it create in your life if you were formally reprimanded for violating the company information security policy?	Siponen & Vance (2010)
Informal sanctions—certainty 1	How likely is it that you would lose the respect and good opinion of your co-workers for violating the company information security policy?	Siponen & Vance (2010)
Informal sanctions—certainty 2	How likely is it that you would jeopardize your promotion prospects if management learned that you had violated company information security policy?	Siponen & Vance (2010)
Informal sanctions—certainty 3	How likely is it that you would lose the respect and good opinion of your manager, if management learned that you had violated company IT security policies?	Siponen & Vance (2010)
Informal sanctions—severity 1	How much of a problem would it create in your life if you lost the respect and good opinion of your coworkers for violating the company information security policy?	Siponen & Vance (2010)
Informal sanctions—severity 2	How much of a problem would it create in your life if you jeopardized your future job promotion prospects for violating the company information security policy?	Siponen & Vance (2010)
Informal sanctions—severity 3	How much of a problem would it create in your life if you lost the respect of your manager for violating the company information security policy?	Siponen & Vance (2010)

Appendix B: Use Permission Siponen, Mahmood, and Pahnila (2014)

ELSEVIER LICENSE
TERMS AND CONDITIONS

Oct 13, 2016

This Agreement between David A Brown ("You") and Elsevier ("Elsevier") consists of your license details and the terms and conditions provided by Elsevier and Copyright Clearance Center.

License Number	3967160599833
License date	Oct 13, 2016
Licensed Content Publisher	Elsevier
Licensed Content Publication	Information & Management
Licensed Content Title	Employees' adherence to information security policies: An exploratory field study
Licensed Content Author	Mikko Siponen,M. Adam Mahmood,Seppo Pahnila
Licensed Content Date	March 2014
Licensed Content Volume Number	51
Licensed Content Issue Number	2
Licensed Content Pages	8
Start Page	217
End Page	224
Type of Use	reuse in a thesis/dissertation
Portion	full article
Format	both print and electronic
Are you the author of this Elsevier article?	No
Will you be translating?	No
Order reference number	
Title of your thesis/dissertation	Examining the Behavioral Intention of Individuals' Compliance with Information Security Policies
Expected completion date	May 2017
Estimated size (number of pages)	125
Elsevier VAT number	GB 494 6272 12
Requestor Location	David A Brown 321 Discovery Lane EGG HARBOR TOWNSHIP, NJ 08234 United States Attn: David A Brown
Total	0.00 USD
Terms and Conditions	

Appendix C: Use Permission

MIS Quarterly
Carlson School of Management
University of Minnesota
Suite 4-339 CSOM
321 19th Avenue South
Minneapolis, MN 55455

October 28, 2016

David Brown
Walden Capella University

Permission to use material from
MIS Quarterly in Dissertation Research

Permission is hereby granted for David Brown to use material from "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," M. Siponen and A. Vance, *MIS Quarterly* (34:3), September 2010, pp. 486-502, specifically the measurement items in Appendix A, Table A1, and as additional reference material as needed, in his doctoral dissertation tentatively titled "Examining the Behavioral Intention of Individuals' Compliance with Information Security Policies," being completed at Walden University.

In addition to the citation information for the work, the legend for the material should include

Permission to use this material also extends to distribution of the dissertation through ProQuest Information and Learning in electronic format, and to any academic journal articles resulting from the dissertation. Any additional usage, including revisions or editions of the dissertation, will require separate permissions and may be subject to a fee.

Janice I. DeGross
Manager

Appendix D: Use Permission Son (2011)

ELSEVIER LICENSE
TERMS AND CONDITIONS

Oct 13, 2016

This Agreement between David A Brown ("You") and Elsevier ("Elsevier") consists of your license details and the terms and conditions provided by Elsevier and Copyright Clearance Center.

License Number	3967160887691
License date	Oct 13, 2016
Licensed Content Publisher	Elsevier
Licensed Content Publication	Information & Management
Licensed Content Title	Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies
Licensed Content Author	Jai-Yeol Son
Licensed Content Date	October 2011
Licensed Content Volume Number	48
Licensed Content Issue Number	7
Licensed Content Pages	7
Start Page	296
End Page	302
Type of Use	reuse in a thesis/dissertation
Intended publisher of new work	other
Portion	full article
Format	both print and electronic
Are you the author of this Elsevier article?	No
Will you be translating?	No
Order reference number	
Title of your thesis/dissertation	Examining the Behavioral Intention of Individuals' Compliance with Information Security Policies
Expected completion date	May 2017
Estimated size (number of pages)	125
Elsevier VAT number	GB 494 6272 12
Requestor Location	David A Brown 321 Discovery Lane EGG HARBOR TOWNSHIP, NJ 08234 United States Attn: David A Brown
Total	0.00 USD

Appendix E: Fear Appeal Communication

Information System Security Policy Communication

To maintain the integrity, confidentiality, and availability of information resources, most organizations establish a written statement, often called information system security policy, information technology security policy, or other names. An information system security policy generally describes employees' responsibilities for protecting corporate information from potential security incidents. Examples include employees' responsibilities with regard to use of computers, e-mail communications, and Internet/network resources.