FROM THE WEAKEST LINK TO THE BEST DEFENSE: EXPLORING THE FACTORS THAT AFFECT EMPLOYEE INTENTION TO COMPLY WITH INFORMATION SECURITY POLICIES.

A DISSERTATION SUBMITTED TO THE GRADUATE DIVISION OF
THE UNIVERSITY OF HAWAIʻI AT MĀNOA IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

COMMUNICATION AND INFORMATION SCIENCES

MAY 2013

By

Salvatore Aurigemma

Dissertation Committee:

Raymond Panko, Chairperson
Elizabeth Davidson
Rich Gazan
Daniel Suthers
Ronald Heck

Keywords: Information security policy, employee compliance intent, planned behavior, subjective norms, attitude, perceived behavioral control, self-efficacy, controllability, sanctions, threats, cost-benefit analysis

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

DEDICATION

To the women in my life that motivate me to strive to be a better man, son, brother, husband, and father – Joy, Martha, Doreen, Jacqueline, Colleen, Amanda, and Malia.

To the men in my life that showed me how to work hard and never give up on family, friends, or myself - Rudy, Bobby, Rudy Jr., and Joe.

This is a tribute to you.

ACKNOWLEDGMENTS

My work on this dissertation has been supported by a great number of people, more than I can possibly acknowledge in this small space. I wish to thank my committee members who were more than generous with their expertise and precious time. Special thanks go to my committee chair, Dr. Ray Panko, for his countless hours of patient mentoring. Thank you Dr. Dan Suthers, Dr. Elizabeth Davidson, Dr. Rich Gazan, and Dr. Ron Heck for not only agreeing to serve on my committee, but for the individual motivation and encouragement you provided during the journey of this dissertation. To say that I could not have done it without you would be a true understatement.

ABSTRACT

Information and information systems have become embedded in the fabric of contemporary organizations throughout the world. As the reliance on information technology has increased, so too have the threats and costs associated with protecting organizational information resources. To combat potential information security threats, organizations rely upon information security policies to guide employee actions. Unfortunately, employee violations of such policies are common and costly enough that users are often considered the weakest link in information security. The challenge for researchers and practitioners alike is to help transform employees from the weakest link to the best line of information security defense.

Building upon recent empirical research in information security policy behavioral compliance, this study provides a composite theoretical framework that captures key factors shown to impact an employee's behavioral intent to comply with related policies. The theoretical framework is tested and validated in a real organizational context employing a robust and well-defined set of information security policies, a first in this burgeoning line of research. This study also evaluates how behavioral intent to follow security policies varies for employees for both the general specter of information security policy compliance and specific guidance for three common security threats.

This study found that the primary factors affecting behavioral intent (subjective norms, organizational commitment, attitude, perceived behavioral control, and self-efficacy) had strong, positive relationships with intent to comply with information security policies when examined at a high level of general compliance. However, when the factors affecting behavioral intent and attitude towards a security behavior were

evaluated for specific information security threat contexts, individual factor importance and significance varied greatly. These results indicate that threat context plays an essential role in clarifying the roles of specific behavioral antecedents; there may be limited value in future research focusing on general information security threats. Finally, while this study failed to establish a significant relationship between behavioral compliance intent and an employee's perception of their ability to enforce of mandatory information security policy requirements on coworkers, it did highlight a potential gap in the composite theoretical framework for this important phenomenon that should be addressed in future research.

LIST OF TABLES

LIST OF FIGURES

TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION

Information systems are pervasive throughout the spectrum of modern international organizations including the education, military, government and commercial sectors. Worldwide spending on information technologies and services by the year 2014 is estimated to be $4 trillion (Gartner, 2012). Unfortunately, with the increased reliance of the U.S. economy on information and information systems come increased information security threats and associated costs. Information security concerns are not limited to the U.S.; information security compromises occur internationally on a daily basis with losses potentially in the range of hundreds of billions a year (United Nations, 2005).

Capturing the true cost and occurrence of information security incidents is a difficult task. It is estimated that organizations only discover a fraction of actual security incidents (Whitman, 2003). Additionally, many organizations are reluctant to admit security breaches due to a variety of reasons, such as negative publicity or reputation damage (Richardson, 2011; Hoffer & Straub, 1989; Panko, 2009). The information insecurity dilemma is not limited to small organizations with limited information security resources. Case in point — in January, 2012, Symantec, a leading information security company, was forced to admit that it was hacked in 2006 only after those responsible threatened to post source code for several of Symantec's flagship security products, Norton Antivirus Corporate Edition, Norton Internet Security, Norton Systemworks and PCanywhere (Symantec, 2012). The hacker collective, Anonymous, reportedly tried to extort $50,000 from Symantec before it posted the stolen source code for PCanywhere online in February, 2012 (Symantec, 2012). Symantec is not the only information security giant to

fall victim to security compromises; since 2010, RSA Inc. and Verisign, both companies at the forefront of digital encryption and security technology, were hacked by what is now being called Advanced Persistent Threats (APTs) (Andress, 2011; Reeder, 2012). An APT is defined as a technologically sophisticated entity engaged in information warfare (use of IT to gain an advantage over an adversary) in support of long-term goals (Cloppert, 2009). Neither RSA Inc. nor Verisign openly admitted the security compromises nor the extent of the damage from the incidents until open press reporting increased the pressure for greater disclosure from the companies.

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."

Bruce Schneier (2002), Secrets and Lies

The Importance of Employees for Information Security

There are numerous threats to the confidentiality, integrity, and availability of organizational information and information systems (Panko, 2009). While there are many security mechanisms designed to mitigate the information security risks from relevant threats, it is often incumbent upon individual users to employ the security technologies and/or procedures faithfully and properly for them to be effective: information security depends on the effective behavior of humans (Siponen, 2005; Stanton, Stam, Mastrangelo & Jolton, 2005; Vroom & von Solms 2004; Workman 2007; Panko 2009). In a report by the U.S. National Security Telecommunications and Information Systems Security

Committee (NSTISSC), the greatest potential threat to government information resources was said to come from "insiders with legitimate access to those systems" (NSTISSAM, 1999). For example, the recent successful APT attacks against RSA Inc. and Internet giant Google both started when employees were tricked into opening email attachments that activated malicious software that exploited vulnerabilities in Internet Explorer and Adobe Flash software (Andress, 2012). While the damage done to RSA and Google was primarily conducted by complex computer software remotely operated via computer networks, it was human error that opened the organizations to attack.

There is ample concern and important research on the information security dangers of organizational insiders. An international survey conducted by Cisco Solutions reports that 39 percent of IT professionals worldwide were more concerned about the threat from their own employees than outside threats (Cisco, 2008). There are generally two types of insider security risks—those from malicious and non-malicious employees (NSTISSAM, 1999; Brackney & Anderson, 2004). Adapted from criminology literature (Wells, 2005), malicious insiders are defined as employees that violate information security policies for gain using deception as their principal modus operandi. Non-malicious insiders are defined as employees that fail to fulfill the requirements of information security policies with counterproductive behavior that may be common and even silently condoned in the workplace.

In the well-respected 2010/2011 Computer Security Institute (CSI) Computer Crime and Security Survey, over 60% of respondents reported losses due to security compromises from non-malicious insiders, compared to 41% from malicious insiders (Richardson, 2011). One relevant example of losses due to non-malicious insiders is the

recent case where the University of Hawaii settled a class-action lawsuit in January, 2012 in part over the inadvertent posting to the web of personal information (names, social security numbers, addresses, birth date) of 40,000 people by a faculty member; in total, five data security breaches, including the aforementioned, cost the University of Hawaii $550,000 in credit monitoring fees, not to mention indeterminate reputation damage (Moscaritolo, 2010; Kaplan, 2012).

To assist users in ensuring information security during the use of information technologies and resources, organizations provide employees with information security policies (ISPs) (Panko, 2009; Ernst & Young, 2011). An ISP describes employee roles and responsibilities, addressing specific security issues, in protecting the information resources of their organization (Panko, 2009). Unfortunately, occurrences of employee non-compliance with the guidance provided in their ISPs is significant (Stanton et al. 2005), resulting in billions of dollars annually in losses to their organizations (Calluzzo & Cante, 2004). It is for this reason that non-malicious employees are often considered the weakest link in information security (Mitnick et al., 2002; Warkentin & Willison, 2009; Zhang, Reithel & Li, 2009).

Given the importance of the employee in information security, it is essential to identify and better understand the determinants of security behavior. Behavioral compliance research findings can help focus organizational efforts toward improving employee compliance with ISPs (Zhang et al., 2009; Herath & Rao, 2009; Workman, Bommer & Straub, 2008; Ng, Kankanhalli & Xu, 2009; Bulgurcu, Cavusolgu & Benbasat, 2010; D'arcy, Hovav & Galetta, 2009; Johnson & Warkentin 2010, Guo, Yuan, Archer & Connelly, 2011). The challenge for organizations is to know how to

transform users from the biggest information security vulnerability to the first line of ISP compliance defense (Straub & Welke 1998, Ng et al., 2009). In order to address this challenge, research is required on employee security behavior, attitudes about security, and on methods to enhance employee compliance.

Behavioral Compliance with Information Security Policies

At the essence of extent behavioral ISP compliance research is the notion that a person's intention to take an action, given some actual control over the behavior in question, generally leads to that actual behavior taking place (Fishbein & Ajzen, 1975). As such, the theory of planned behavior (TPB), which links behavioral intent with expected behavior, is a cornerstone of recent ISP behavioral compliance research. According to the TPB, human behavioral intention to perform an action is guided by subjective norms, attitude towards the behavior, and perceived behavioral control (PBC) (Ajzen, 1991); the TPB is depicted in Figure 1. Understanding the antecedents to behavioral intent to comply with ISPs is essential to growing the knowledge base on information security and focusing the efforts of organizations as they develop and implement mechanisms to improve their employees' compliance (Bulgurcu et al., 2010).

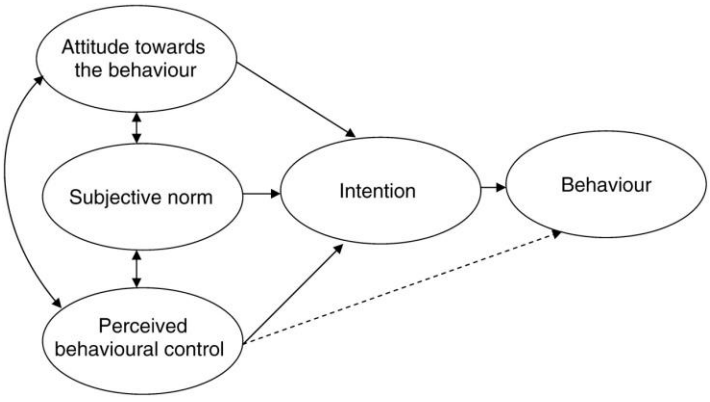

Figure 1: Theory of Planned Behavior Model

Significant empirical research effort has been expended, particularly in the past five years, towards obtaining a better understanding of the factors affecting employee behavioral intent to comply with information security policies. A review of the literature in the next chapter shows some commonalities in the supporting theories used in related research. However, the varied conceptual implementations of these theories have resulted in a confusing array of behavioral compliance models and operational constructs that make comparison of results challenging at the least. Additionally, the treatment of information security threats in the respective studies on ISP behavioral compliance is inconsistent with some studies addressing ISP compliance as a general "all or nothing" event and others assessing ISP compliance for very specific information security threats in isolation. According to Ajzen (1991), the relative importance of the variables (attitude, norms, perceived behavioral control) on behavioral intent is expected to vary across behaviors and situations. Yet, none of the studies in this research stream compares possible compliance behavioral intent differences between the overall ISP and context-specific information security threat guidance contained in an organization's actual ISP. Thus, it may very well be that some of the antecedents of ISP compliance will vary depending on the type of information security threat, and organizations must tailor their ISP implementation accordingly. One size may not fit all; in fact, one size may not fit any particularly well.

One area missing from research on ISP behavioral compliance is the impact of a person's perceived ability to follow ISP guidance if that guidance requires enforcing the policy on other members of an organization. For example, if an organization's ISP requires its employees to enforce a rule on others, such as not bringing personal

electronics into a sensitive work area, will an employee's perceived ability to comply with the ISP vary if the person they must interact with someone of a notably higher rank/status in the organization? Research in social status has shown that people are far more likely to look for rule violations when they are interacting with those that are of lower status than themselves than with peers or those of higher status than themselves (Cummins, 1999). For any organization that operates in an environment of status stratification (such as the military, hospitals, banking and finance, prisons, etc.), the impact of employee status on ISP compliance is a potentially important avenue to explore.

In terms of the TPB, the perceived behavioral control (PBC) variable accounts for potential constraints on an action as perceived by an employee (Armitage & Conner, 2001). Ajzen (1991) argues that the perceived impact of specific factors may inhibit or facilitate behavioral intent as an antecedent to PBC. With respect to this study, enforcing ISP actions on fellow employees is the specific antecedent of PBC being explored.

Statement of the Problem

Researchers have attempted to answer the call of practitioners to explain the factors affecting non-malicious employee behavioral intent to comply with organizational information security policies. However, proposed behavioral ISP compliance models are disjointed when taken as a whole, adding confusion instead of clarity to future research and practice. Using the theory of planned behavior as the overarching framework for evaluating behavioral intent and amplifying the components of the TPB through relevant empirical research in this topic, a composite ISP compliance theoretical framework is

presented in this paper to be applied in a specific organizational context against a set of actual information security threats. Common definitions of the specific threats being evaluated in this study are:

- *Phishing***:** an information security attack that uses authentic-looking email messages or websites to trick users into taking harmful actions or revealing personal or confidential information. Subcategories of phishing include *spear phishing* (phishing aimed at a specific or group with tailored information meant to enhance tricking the recipients) and *whaling* (spear-phishing aimed at an organization's top executives).
- *Tailgating:* The act of gaining access to a secured area by following someone with legitimate access.
- *Removable flash media*: unauthorized use of removable media (thumb drives, flash drives, CDs, DVDs, external hard drives) that may put corporate information resources at risk via unwanted information leakage and threats to the integrity of information systems through the introduction of malicious software.

The information security threat from non-malicious employees is an almost ubiquitous international problem regardless of organization type, size, or even information security acumen. One specific organization that is aware and concerned about the insider security threat is the United States (US) Department of Defense (DoD) (NSTISSAM, 1999; Brackney & Anderson, 2004). From the well-publicized 2010 Wikileaks release of tens of thousands of pages of classified military documents to the numerous publicized attacks against DoD employees using techniques such as phishing,

the DoD has a history of being challenged by the conundrum of employee compliance with information security policies. The present study will be conducted in a DoD setting and address the following research questions:

1. Using the composite framework for ISP behavioral compliance presented in this paper, what is the relative importance of specific antecedents of behavioral intent for employees?
2. How does behavioral intent to comply with the ISP, and its measured antecedents, vary for employees when presented with the overall guidance of the ISP and specific guidance for phishing, tailgating, and the use of removable flash media?
3. Does an employee's perceived ability to follow the information security policy vary if they are required to monitor/interact with other employees of different rank/status across the general ISP guidelines and for specific security threats?

CHAPTER 2. LITERATURE REVIEW AND STUDY CONTEXT

In preparation for this study, a comprehensive literature review of information security behavioral compliance (and non-compliance) was conducted starting with journal articles published from the year 2000. Four high-quality peer-review journals (Management Information Systems Quarterly (MISQ), Decision Support Systems (DSS), European Journal of Information Systems (EJIS), and Journal of Management Information Systems (JMIS)), have published relevant empirical and theory-based research on the topic. Anderson and Argwal (2010) present an excellent, albeit not all-inclusive, summary of related behavioral information security literature over the past 20 years, which was used as a starting point in the literature review process.

Significant research effort has been expended, especially in the past five years, towards obtaining a better understanding of the antecedents of employee information security policy (ISP) behavioral compliance. A review of the literature shows some commonalities in the supporting theories used in related research. However, the varied conceptual implementations of these theories have resulted in a confusing array of behavioral compliance models and operational constructs that make comparison of results challenging for both researchers and practitioners.

A total of 12 papers directly related to ISP compliance were used to inform this study, as shown in Table 1. A quick glance at the Cited Theories column of Table 1 shows some explicit theoretical commonalities among the publications with the use of the Theory of Reasoned Action/Theory of Planned Behavior (7), General Deterrence Theory (4), and the Protection Motivation Theory (6). A more detailed examination of Table 1 shows that, while all of the studies model behavioral intent to comply or not-comply with an

organization's ISP, no other single construct exists in all the studies. Of the 12 studies, there are 104 defined variables; however, 33 of the variables essentially equate to three core TPB constructs of Subjective Norm, Perceived Behavioral Control, and Behavioral Intent (all of which are defined below). Nomenclature for the construct Behavioral Intent varies (nine different labels) as does Subjective Norms (five different labels). In some cases, it is fairly easy to discern construct congruence (see Self-efficacy), and in other cases it is difficult without a very careful review of variable operationalization in the individual study. For example, Johnson and Warkentin (2010) use the term Social Influence to mean the same thing as Subjective Norms. A lack of consistent construct naming conventions is confusing for not only the casual reader, but also one that takes the time to closely review the studies in Table 1.

Beyond naming conventions, the implementation of the above constructs in compliance models varies between studies, even when using the same or similar theoretical bases. A visual comparison of the models in the Table 1 studies confuses more than clarifies where the studies converge, diverge, or shed new light on the behavioral intent phenomenon. Finally, many of the studies in Table 1use methods that are tailored towards exploratory models and theory development. Whether for parsimony or other reasons, many of these studies focus on different theoretical antecedents of behavioral intent. By doing so, they ignore other empirically validated factors that may potentially alter structural model analysis results via mediating effects or mere presence in the model.

Authors	Title & Publication	Cited Theories	Related Constructs
Al-Omari, A., El-Gayar, O., & Deokar, A. (2012)	Security Policy Compliance: User Acceptance Perspective. 2012 45th Hawaii International Conference on System Sciences (pp. 3317-3326)	Technology Acceptance Model, Theory of Reasoned Action	Subjective Norm, Self-efficacy, Controllability, Information Security, Security Policies, SETA Program, Computer Monitoring, Perceived Usefulness of Protection, Perceived Ease of Use, Intention to Comply
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.	Theory of Planned Benefits, Rational Choice Theory	Information Security Awareness; Perceived Benefit of Compliance; Intrinsic Benefit; Safety of Resources; Rewards; Perceived Cost of Compliance; Work Impediment; Perceived Cost of Non-compliance, Intrinsic Cost, Vulnerability of Resources, Sanctions, Attitude, Normative Beliefs, Self Efficacy to Comply, Intention to Comply
D'Arcy, J., Hovav, A., & Galletta, D. (2009).	User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research, 20(1), 79-98.	General Deterrence Theory	Security Policies, SETA Program, Computer Monitoring, Perceived Certainty of Sanctions, Perceived Severity of Sanctions, IS Misuse Intention
Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011)	Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. Journal of Management Information Systems, 28(2), 203-236.	Composite Behavior Model (extension of the Theory of Reasoned Action and Theory of Planned Benefits)	Attitude Toward Security Policy, Relative Advantage for Job Performance, Perceived Security Risks, Perceived Sanctions, Work Group Norm, Perceived Identity Match, Attitude Towards Non-Malicious Security Violation (NMSV), NMSV Intention
Herath, T., & Rao, H. R. (2009a)	Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106–125.	Theory of Planned Benefits, Protection Motivation Theory, General Deterrence Theory	Punishment Severity, Detection Certainty, Perceived Probability of Security Breach, Perceived Severity of Security Breach, Security Breach Concern Level, Response Efficacy, Response Cost, Security Policy Compliance Intention, Security Policy Attitude, Self-efficacy, Subjective Norm, Descriptive Norm, Resource Availability, Organizational Commitment
Herath, T., & Rao, H. R. (2009b)	Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154-165.	General Deterrence Theory, Agency Theory	Severity of Penalty, Certainty of Detection, Normative Beliefs, Peer Behavior, Policy Compliance Intention, Perceived Effectiveness
Ifinedo, P. (2011)	Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security.	Theory of Planned Benefits, Protection Motivation Theory	Perceived Vulnerability, Perceived Severity, Response Efficacy, Response Cost, Self-efficacy, Attitude Towards Compliance with ISSP, Subjective Norms, ISSP Compliance Behavioral Intention
Johnston, A. C., & Warkentin, M. (2010)	Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly, 34(1).	Protection Motivation Theory	Perceived Threat Severity, Perceived Threat Susceptibility, Response Efficacy, Social Influence, Self Efficacy, Behavioral Intent
Ng, B.-Y., Kankanhalli, A., & Xu, Y. (Calvin). (2009)	Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815-825.	Protection Motivation Theory	Behavior, Perceived Susceptibility, Perceived Severity, Perceived Benefits, Perceived Barriers, Cues to Action, General Security Orientation, Self-efficacy, Technical Controls, Security Familiarity
Pahnila, S., Siponen, M., & Mahmood, A. (2007)	Employees' behavior towards IS security policy compliance. System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on (p. 156b-156b).	Theory of Reasoned Action, General Deterrence Theory, Protection Motivation Theory, Social Cognitive Theory	Intention to Comply, Attitude Towards Complying, Habits, Facilitating Conditions, Normative Beliefs, Information Quality, Sanctions, Threat Appraisal, Coping Appraisal, Rewards
Workman, M., Bommer, W. H., & Straub, D. (2008).	Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24(6), 2799-2816.	Protection Motivation Theory, Social Cognitive Theory	Perceived Severity, Vulnerability, Locus of Control, Self-efficacy, Response Efficacy, Response Cost, Subjective Omission of Security
Zhang, J., Reithel, B. J., & Li, H. (2009)	Impact of perceived technical protection on security behaviors. Information Management & Computer Security, 17(4), 330-340.	Theory of Planned Benefits	Subjective Norms, Perceived Behavioral Control, Attitude, Perceived Security Protection Mechanism, Behavioral Intention

Table 1: Information Security Policy Behavioral Compliance Studies

Elucidating the results of the research in the area of ISP behavioral compliance requires a theoretical anchor point; a theory common to the majority of the respective studies. Such a theoretical frame of reference would better allow readers to understand the contributions and differences in individual studies while staying grounded in the context of the general body of research to date. In this paper, we use the theory of planned behavior as the guiding framework for understanding the basic antecedents of behavioral intention to comply with ISPs, as well as illuminate the contributions of the supporting studies identified in Table 2. By using the TPB to structure evaluation of related research, we are able to generate a composite ISP behavioral compliance framework with normalized constructs. The result is a more parsimonious theoretical model in which to judge past and future research in this important area.

Theoretical Foundation – The Theory of Planned Behavior

The theory of planned behavior (TPB) extends the theory of reasoned action (Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1975) and is considered one of the most influential frameworks for the study of human action (Armitage & Conner, 2001; Ajzen 2001, Zhang et al., 2009). According to TPB, human behavioral intention to perform an action is guided by subjective norms, attitude towards the behavior, and perceived behavioral control (Ajzen, 1991; Ajzen 2002). Given some actual control over the behavior in question, people are expected to follow their intentions when confronted with an appropriate impetus. Thus, behavioral intention is assumed to be the immediate antecedent of actual behavior (Ajzen, 2002). Numerous reviews (Blue, 1995; Conner and Sparks, 2005; Godin, 1993; Manstead and Parker, 1995) and meta-analyses (Armitage

and Conner, 2002; Ajzen, 1991; Godin and Kok, 1996; Hausenblas, Carron & Mack, 1997) have provided support to the efficacy of the TPB in predicting behavioral intent. As noted by Armitage and Conner (2002), the TPB accounted for approximately 40% of the variance in behavioral intent in 185 independent studies published in 1997 and earlier.

In the context of ISP behavioral compliance, the TPB model states that the more favorable an employee's attitude and normative beliefs towards following ISP-related actions, and the greater the feeling of behavioral control over those actions, the stronger the intention to comply with the ISP (Zhang et al., 2009). Figure 2 provides the generic TPB model.

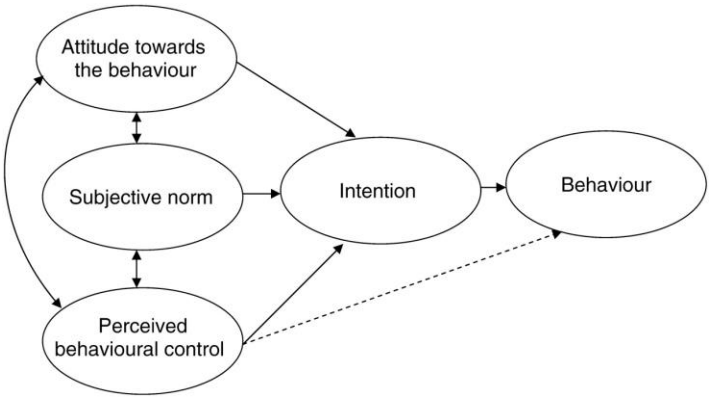

Figure 2: Theory of Planned Behavior Model

The use of the TPB in ISP behavioral compliance literature is well established. As shown in Table 2, the TPB (or TRA) is used explicitly in seven of the twelve studies presented. In the remaining five studies, core constructs of the TPB are employed, allowing cross-evaluation with TPB-based studies. For example, in Johnston and Warkentin (2010), the primary theory used to derive their model is protection motivation theory. However, Johnston and Warkentin also add the constructs normative beliefs and self-efficacy to their model, effectively emulating the TPB model shown in Figure 2.

The TPB has been used successfully in other information security contexts, such as insider security contravention (Workman, 2007) and computer abuse (Lee and Lee, 2002). Lee and Lee (2002) define computer abuse as intentional acts associated with computers in which a victim could or did suffer and which a perpetrator could or did benefit. Using the TPB model, they posited criminology-based theories to better illuminate the constructs of normative beliefs, attitude and perceived behavioral control. Lee and Lee's (2002) focus on computer abuse may have a different focus than the papers identified in Table 2 (understanding general ISP behavioral compliance), but the approach they take in expanding the knowledge of individual TPB constructs with promising theories is consistent with ISP compliance-related literature. A discussion of the core TPB constructs follows, along with additional theories that have been empirically shown to improve the overall understanding of ISP behavioral compliance.

Decomposed Theory of Planned Behavior

Taylor and Todd (1995) introduced the concept of decomposing the theory of planned behavior in order to more deeply explore the dimensions of attitude, subjective norms, and perceived behavioral control by evaluating these variables as multi-dimensional constructs. There are two main advantages to this approach. First, it deals with the dilemma of monolithic belief structures being unable to represent the variety of dimensions existing in the main TPB antecedents (Bagozzi, 1981; Shimp and Kavas, 1984). For example, when exploring the construct of Perceived Behavioral Control (described in more detail below), addressing this variable as a monolithic structure may obscure or completely ignore employee beliefs about their ability to conduct a specific

behavior in light of some controlling or facilitating condition (Taylor and Todd, 1995). In the present study, the controlling condition being explored is whether employees feel capable of enforcing ISP actions on coworkers if witnessing a violation in progress.

The second benefit to decomposing the TPB variables is that by focusing on specific beliefs, the model becomes more practitioner friendly, highlighting specific factors that may influence employee behavioral intent (Taylor and Todd, 1995; Herath and Rao, 2009a). Such factors can be used to inform employer actions (training programs, technology implementation, process implementation or modifications, etc.) meant to strengthen employee intent to comply with the ISP.

Only one of the studies identified in Table 2 used to inform this study (Herath and Rao, 2009a) explicitly state the use of the decomposed TPB in developing their ISP compliance model. However, by effectively decomposing the attitudinal component represented in their ISP compliance models, all but two of the remaining studies (Al-Omari, El-Gayar & Deokar, 2012; Zhang et al. 2009) implicitly subscribe to the notion of antecedent decomposition expressed by Taylor and Todd (1995). Decomposing the associated variables with results of relevant recent research enriches the following description of the components of the TPB. The resulting composite theoretical framework and associated structural models that follow in Chapter 3 of this study is framed by the decomposed TPB, specifically focusing on decomposition of the Perceived Behavioral Control and Attitude variables.

Subjective Norms

According to the theory of planned behavior, subjective norms are beliefs about the normative expectations of other people that result in perceived social pressure (Ajzen, 2002). Employees' perceived social pressure to follow information security policies reflects their beliefs about how important referents (coworkers in general, peers, supervisors, subordinates, etc.) would like them to perform their security-related responsibilities (Ajzen, 2002; Zhang et al, 2009; Bulgurcu et al., 2011). If an employee believes that relevant others expect ISP compliance from them, they are more likely to undertake appropriate security actions.

Other names used from Table 2 studies for subjective norms (Al-Omari et al., 2012; Ifenido, 2012; Zhang et al., 2009) includes normative beliefs (Bulgurcu et al., 2010; Herath and Rao, 2009b; Pahnila, Siponen & Mahmood, 2007), social influence (Johnston and Warkentin, 2010), work group norm (Guo et al., 2011), and descriptive norms (Herath and Rao, 2009a). While the extant information technology and security literature has used a variety of labels for the subjective norms construct, each of the above contain the notion that an employee's behavioral intent is influenced by what relevant others expect to be done (Herath and Rao, 2009a). For sake of consistency with the TPB, the term Subjective Norms is used for the remainder of this paper.

Of the 12 empirical ISP behavioral compliance models examined in this study, all but three (D'Arcy et al., 2009; Ng et al., 2009; Workman et al., 2008) utilize the subjective norms construct. In each case of its use, the operationalization of the construct and measurement instruments for subjective norms were fairly consistent.

While the subjective norms construct is well represented in the ISP-compliance literature, there is at least one instance in which its explanatory power was not significant, in discordance with the TPB. In Zhang et al.'s (2009) study of the impact of perceived technical protection on security behaviors, the authors found no significant relationship between subjective norms and behavioral intent. An examination of the sample data by the authors provided a possible explanation for the incongruity with the TPB. Zhang et al (2009) noted that the majority of their respondents were employees with at least six years of experience at their organizations. This experience may indicate the presence of habits to comply or not comply with ISPs. As noted in other information system studies (Venkatesh and Davis, 2000), the effect of subjective norms can erode with increasing experience.

There is extensive literature on the impact of habit on TPB, including some that provide evidence of habits significantly adding to the prediction of intention over and above the effect of attitude and subjective norm and to the prediction of behavior from intention alone (Brinberg and Durand, 1983; Sparks et al., 1992). It has been posited that in the TPB model, habit may be best considered as a control variable (Perugini and Bagozzi, 2001). In the ISP-compliance literature, the only study that specifically addressed the impact of habits on behavioral intentions was Pahnila et al. (2007). Based upon the findings of Limayem and Hirt (2003), Pahnila et al. (2007) posited that habits (defined as unconscious or automatic behaviors) can trump subjective norms over time, directly influencing actual behavior and reducing the impact of behavioral intentions to comply with ISPs. Both habits and subjective norms were found to have a positive significant relationship with behavioral intent in the Pahnila et al. (2007) study. Although

habit may explain more variance when applied to the TPB model, it does not aid understanding of what underlies people's behavior (Mahon et al., 2006), thus it is not included in the composite ISP compliance model as a construct of interest.

Perceived Behavioral Control

The concept of perceived behavioral control (PBC) was introduced to the theory of planned behavior to address non-volitional aspects potentially inherent in all behaviors (Ajzen, 2002). In general terms, PBC refers to people's perceptions about the presence of factors that may facilitate or impede the performance of a behavior (Ajzen, 2002; Lee and Lee, 2002). Prior to PBC, similar ideas appeared in the health belief model (Kirscht, Haefner, Kegeles & Rosenstock, 1966), and Triandis' model of interpersonal behavior (Triandis, 1977). According to Ajzen (2002), the PBC construct owes its greatest debt to Bandura's work on self-efficacy.

A central tenet of social cognitive theory (Bandura, 1991), perceived ***self-efficacy*** was introduced to deal with coping behavior in the context of behavior modification (Bandura, 1977). Perceived self-efficacy refers to peoples' beliefs about their own capabilities to carry out a task (Bandura, 1991). The concepts of PBC and self-efficacy are quite similar as both are concerned with a person's perceived ability to perform a behavior (Ajzen, 2002). In the context of ISP behavior compliance, self-efficacy refers to an employee's self confidence in their skills or ability to comply with the actions called for in the ISP (Ng et al., 2009). People with a high level of self-efficacy have a stronger form of self-conviction about their ability to mobilize motivation and cognitive resources needed to successfully execute the guidance of the ISP (Rhee, Kim & Ryu, 2009).

A second component of PBC is known as ***perceived controllability***, a very similar concept to Rotter's (1966) locus of control with some nuanced differences. Perceived controllability considers the extent of which an employee's behavior is considered proactive or reactive (Ajzen, 2002). Locus of control is defined in a similar fashion, but is further described as having internal and external components (Workman et al., 2008). Internal locus of control is a belief that people control their own actions while external locus of control refers to the belief that forces (other people, fate, environmental factors, etc.) determine outcomes (Rotter, 1966). Perceived Controllability in PBC does not draw as clear a distinction between internal and external components; perceived control over an outcome is independent of the internal or external locus of factors responsible for it (Ajzen, 2002). Thus, while Perceived Controllability is focused on a person's belief of whether an event is controllable, self-efficacy focuses on a person's beliefs of their capabilities (skills and abilities) in performing a particular behavior.

The inclusion of the constructs Self-efficacy and Perceived Controllability into the singular concept of Perceived Behavioral Control has been contested inside and outside of the ISP behavioral compliance literature (Ajzen, 2002). Workman et al. (2008) argue that the combination of clearly different variables is problematic because the type of interventions organizations may target is different based upon whether the controllability is belief based (locus of control) or skills based (self-efficacy). This blending, Workman et al. (2008) challenge, can confuse organizations when trying to determine how to address the problem. Thus, Workman et al. (2008) include both self-efficacy and locus of control as separate constructs in their model of ISP behavioral compliance.

Ajzen (2002) acknowledges that there is considerable evidence of the distinctive nature of the variables self-efficacy and perceived controllability. Empirical research shows that items that load highly on self-efficacy deal with the ease or difficulty of performing a behavior; controllability involves beliefs of the whether the conduct of that behavior is up to the person (Ajzen, 2002). A meta-analysis of PBC items from various studies (cited in Ajzen, 2002) found that self-efficacy and perceived controllability taken together significantly improved prediction of behavioral intentions (more than either construct taken individually). Based upon the benefits of decomposing the components of the TPB (Taylor & Todd, 1995) and the arguments of Workman et al. (2008) and Ajzen (2002), this study will evaluate PBC with hierarchical variables of self-efficacy and Perceived Controllability. In particular, this study will explore Perceived Controllability with the controlling condition being whether employees feel capable of enforcing ISP actions on coworkers if witnessing a violation in progress.

Of the ISP behavioral compliance models examined in this study, seven (Al-Omari et al., 2012; Bulgurcu et al., 2010; Herath and Rao, 2009a; Johnston and Warkentin, 2010; Ng et al., 2009; Pahnila et al., 2007; Workman et al., 2008) use self-efficacy instead of PBC. For example, Bulgurcu et al. (2010) use self-efficacy as they state it measures the same latent construct as PBC (Fishbein, 2008) and is consistent with recent behavioral literature (Fishbein and Capella, 2006; Fishbein and Yzer, 2003; Giles, McClenehan, Cairns & Mallet, 2004; Yi and Hwang, 2003). Ajzen (2002) acknowledges that in some cases, only one of the PBC components (self-efficacy or perceived controllability) may be sufficient to calculate the effect of PBC depending on the behavior and context. Only Zhang et al. (2009) explicitly uses the PBC construct, with both of its component

variables. As discussed above, Workman et al. (2008) use both self-efficacy and locus of control constructs. Pahnila et al. (2007) uses both self-efficacy and facilitating conditions, a very similar construct to locus of control and perceived controllability originating with Triandis (1977). Finally, only three studies from Table 2 (D'Arcy et al., 2009; Guo et al., 2011; and Herath and Rao 2009b) ignore the concept of PBC altogether.

Of the nine ISP behavioral compliance models evaluated that used PBC/self-efficacy, only Pahnila et al. (2007) found self-efficacy to be an insignificant contributor to behavioral intent. However, in the Pahnila et al. (2007) study, self-efficacy was measured as one of three components of a higher-order construct called coping appraisal. A closer examination of how coping appraisal was measured would need to be conducted to determine if self-efficacy alone would have had a significant effect on behavioral intent in their study. However, the relative importance of any of the components of the TPB, including PBC, is expected to vary across behaviors and situations (Armitage and Conner, 2001), which also may address the results from the Pahnila et al. (2007) study.

Due to the similarity in construct definitions and measurement items described in Ajzen (2002) and Workman et al (2008), and in keeping with the basic framework of the TPB, the composite ISP behavioral compliance model presented in this paper uses the construct PBC with supporting variables of self-efficacy and perceived controllability. Additionally, discussion of comparisons between the health belief model (a precursor theory to PMT) and the TPB below support the use of TPB PBC constructs in the composite model.

Attitude Towards Compliance

The third main construct that guides an employee's behavioral intent to comply with ISPs is their attitude towards compliance. An employee's attitude toward compliance behavior is determined by their belief that performing (or not performing) the behavior will lead to certain consequences (Bulgurcu et al., 2010). In the context of this paper, satisfying of the attitude element means that the consequences of executing the ISP are believed to be desirable (Siponen, 2000). Numerous TPB-related studies (Beck, 1981; Mahon, Cowan & McCarthy, 2006; Nejad, Wertheim & Greenwood, 2005; Rutter, 1989) have shown that attitude can be the strongest predictor of behavioral intent, which makes research in this component of the TPB extremely valuable. In fact, the majority of literature in the information systems field on behavioral intent has focused most on investigating attitude and its antecedents (Bulgurcu et al., 2010). The ISP behavioral compliance literature presented in this paper has focused on three main themes in decomposing the attitudinal construct: sanction effects, threat assessment, and cost-benefit analysis.

Sanction Effects

Sanction effects are based upon general deterrence theory (GDT), which can be traced back to Italian jurist and philosopher Cesare Beccaria (1738-1794) (Siponen and Vance, 2010). The main hypothesis of the GDT is that people weigh costs and benefits when deciding whether to commit a crime (or in the context of this of this study, intend to violate some portion of the ISP). In essence, sanction effects are a negative version of rational choice theory (Simon, 1955), which is addressed in the Cost-Benefit Assessment section following. Specifically, the GDT focuses on sanctions against committing an

unwanted act and their effectiveness as a deterrent (Theoharidou, Kokolakis, Karyda & Kiountouzis, 2005). The effectiveness of sanctions is based upon the ***perceived severity of the sanction*** and the ***perceived probability of sanction imposition*** (Straub and Welke, 1998). The GDT is well established in the information security field (Straub and Nance, 1990; Straub and Straub, 1990; Straub and Welke, 1998) and explicitly represented in four of the ISP compliance models reviewed in this paper (D'Arcy et al., 2009; Herath and Rao, 2009a; Herath and Rao, 2009b; Pahnila et al., 2007). Additionally, both Bulgurcu et al. (2010) and Guo et al. (2010) implicitly use the GDT as they evaluate the effect of sanctions on behavioral intent.

The rationale for applying sanction effects to the attitudinal component of the TPB is that security mechanisms can be deployed by organizations to increase the perceptions of certainty and severity of punishment for ISP violations, thereby strengthening the behavioral intent to comply. Despite the theoretical base provided by the GDT, deterrence-based research in information security has been inconclusive (D'Arcy et al., 2009). Research on computer abuse behavior has focused on sanction effect mechanisms (policy, systems, and awareness programs) meant to increase the perceived cost of abusive behaviors (Lee and Lee, 2002). However, these mechanisms appear mostly ineffective in practice even though they are deployed in over 80 percent of U.S. organizations (Lee and Lee, 2002).

Of the six ISP behavioral compliance models that employed GDT examined in this paper, all but Pahnila et al. (2007) found sanction effects to be a significant contributor to behavioral intent. The two components of sanction effects are incorporated into the composite theoretical framework of ISP behavioral compliance as it addresses a

potentially important component of a person's attitude that is not specifically addressed in other supporting constructs.

Threat Assessment

The protection motivation theory (PMT) (Rogers, 1975; Rogers, 1983) is an extension of the health belief model (Kirscht et al., 1966) and elucidates the processes involved in coping with a threat (Johnson and Warkentin, 2010). The PMT consists of two main processes: threat assessment and coping appraisal. The appraisal of the threat and coping responses result in the intention to perform (or not perform) a particular action associated with a fear appeal related to that action. Coping appraisal is comprised of locus of control and self-efficacy (Workman et al., 2008), described above, and is normalized in this study under the label of perceived behavioral control.

Threat assessments, according to the PMT, are comprised of three variables: perceived severity, perceived vulnerability, and perceived response efficacy. The perception of threat is defined as the anticipation of a violation (physical, psychological, or social) to oneself or others (Workman et al., 2008). When a threat is perceived, behavior is adjusted to account for an acceptable amount of risk. ***Perceived severity*** of a threat will lead a person to behave more cautiously if their perception of the damage from the threat is greater. Thus, if a person feels that a specific security threat, such as the threat of spreading viruses from opening email attachments, is very high, they will tend to limit or eliminate that practice.

Perceived vulnerability, also called perceived susceptibility (Johnston and Warkentin, 2010; Ng et al., 2009), relates to how likely an employee feels that they will encounter a particular threat (Johnston and Warkentin, 2010; Workman et al., 2008). However,

individuals vary widely in their perceptions of vulnerability. Given the same information about the probability of an information security threat, one person may feel the likelihood of occurrence is very small and thus they are less vulnerable, while another feels quite opposite (Ng et al., 2009). Workman et al. (2008) refers to some people's "illusion of invulnerability" that allows them to ignore threats existing in the world so that they may continue to view the world as safe and orderly. Bad things happen to other people, not oneself. In the ISP compliance context, employees that operate with a sense of invulnerability are less likely to comply with the actions directed in the ISP. However, when an employee is given a reason to believe they are vulnerable to a specific threat, they will be more likely to comply with the ISP.

People often hold different views about the effectiveness of a directed behavior in the face of a threat (Workman et al., 2008). A person's belief about the availability and effectiveness of a threat mitigation action determines their behavior, not the objective facts about the recommended response (Ng et al., 2009). ***Response efficacy*** refers to an employee's perceived effectiveness of a recommended threat response (Rogers, 1975). According to the PMT, moderate to high levels of response efficacy are associated with positive beliefs about the threat mitigation of a particular recommended response (Johnston and Warkentin, 2010). The term *perceived benefits* (Ng et al., 2009) is also used in the ISP compliance literature but is defined synonymously with response efficacy. One significant difference between the PMT and the theory of planned behavior view of response efficacy is the protection motivation theory's conceptualization of the construct as a coping appraisal mechanism along with self-efficacy (Workman et al., 2008). In keeping with the TPB model, the composite framework presented in this paper

presents response efficacy as a component of attitudinal threat assessment in that it is specifically concerned with an individual's belief about the effectiveness of a particular action against a threat of some perceived severity and susceptibility.

As identified earlier, the PMT is an extension of the health belief model (HBM). The HBM suggests that an individual's behavior is determined by a threat assessment and beliefs about the efficacy of the behavior to resolve the threat (Ng et al., 2009). As the TPB extended the theory of reasoned action by including the perceived behavioral control construct, PMT extended the HBM by including self-efficacy and locus of control (see section 4 discussion above). Numerous empirical studies have been conducted comparing the HBM and the TPB (Beck, 1981; Nejad et al., 2005; Rutter, 1989), all of which conclude that the TPB is a better measure of behavioral intent and also reaffirm the importance of the attitudinal component of the TPB. The main contribution of the PMT to the composite model of ISP behavioral compliance is the addition of the threat assessment construct and associated variables.

Cost-Benefit Analysis

The TPB posits that behavior-related consequences manifest in one's attitude toward behavioral intent (Ajzen, 2001). In the context of obedience to ISPs, an employee's attitude is formed when the compliance-related consequences that will be personally experienced if they comply or do not comply are considered (Bulgurce et al., 2010). Thus, when an employee considers executing a behavior, they conduct a ***cost-benefit analysis***. An employee's cost-benefit analysis can be described as the affective and cognitive assessment of a behavior acquired through personal experience; the overall

assessment may be either favorable or unfavorable (Ajzen, 2003). The cost-benefit analysis construct is based upon rational choice theory (RCT) (Simon, 1955). The RCT, with roots in economic theory, argues that behavior is determined by balancing the costs and benefits of different options.

Three ISP compliance studies (Bulgurcu et al., 2010; Herath and Rao, 2009a; Workman et al., 2008) have explored, to some extent, the cost-benefit analysis component of the attitude construct; all found cost-benefit analysis to be a significant contributor to attitude. Herath and Rao's (2009a) evaluation of cost-benefit analysis is cursory. They use a variable, response cost, to estimate an employee's beliefs about how costly performing an ISP-related action will be.

Workman et al. (2008) proffer that an employee's intention to follow ISP-directed behaviors may be influenced by whether they perceive that the effort required to protect an information resource is worth the cost of the protection effort. It is noted, however, that cost-benefit attitudes vary among individuals when comparing such things as business value or threat severity to their own self-interests (Workman et al., 2008). Thus, if an ISP action is considered to address an extremely important resource, but it is very difficult or exceedingly time consuming to conduct, an employee may perceive the cost as outweighing the benefit (Thomas & Thomas, 2004). Conversely, if an ISP action provides only a minimal benefit, but the associated effort is also minimal, it may be adopted (Pechmann et al., 2003). Workman et al. (2008) measure cost-benefit analysis by assessing the inconvenience, cost, and impact to an employee's work from implementing the ISP.

Bulgurcu et al. (2010) took a more robust approach to exploring the antecedents of an employee's cost-benefit analysis through the application of rational choice theory. They posit that determinants of an employee's attitude originate in their beliefs about complying (or not complying) with the ISP and the consequences of their actions (Bulgurcu et al., 2010). Their cost-benefit analysis methodology posits two main constructs: beliefs about overall assessment of consequences and beliefs about outcomes.

Beliefs about overall assessment of consequences have three distinct beliefs: perceived benefit of compliance, perceived cost of compliance, and perceived cost of non-compliance (Bulgurcu et al., 2010). *Perceived benefit of compliance* is the overall expected favorable consequences to an employee for complying with the ISP. *Perceived cost of compliance* is the overall expected unfavorable consequences for complying with the ISP. *Perceived cost of non-compliance* is the overall expected unfavorable consequences for non-compliance.

Bulgurcu et al. (2010) further go on to define their second component of cost-benefit analysis, beliefs about outcomes. Beliefs about outcomes describes how an employee forms their beliefs about overall assessment of consequences. Addressing both intrinsic and extrinsic motivations, Bulgurcu et al. (2010) posit seven outcome beliefs that provide for the foundation for beliefs about consequences. The authors readily admit that they did not address all of the factors and outcome beliefs possible, such as those factors included in the sanction effects and threat assessment constructs. For sake of parsimony, the cost-benefit analysis construct measurements defined by Workman et al. (2008) are used in this study.

Organizational Commitment

Beyond the three main TPB constructs of subjective norms, PBC, and attitude, recent ISP compliance research identified another possible antecedent to behavioral intent – ***organizational commitment*** (Herath and Rao, 2009a). Herath and Rao (2009a) introduced the concept of organizational commitment to the context of ISP compliance research. Organizational commitment is defined as the overall strength of an individual's involvement and identification with their organization and captures the perceived relationship between the organization and the employee (Mowday, 1998). In the information security context, employees are less likely to enact poor security behaviors and put their organization at risk if their organizational commitment is high (Herath and Rao, 2009a).

While Herath and Rao explicitly identify organizational commitment as an antecedent, two other studies identify variables that have similar characteristics. D'arcy et al. (2009) decompose a similar concept that addresses user awareness of organizational security countermeasures. Their definition of security countermeasures consists of an organization's ISP, security monitoring technologies, and security education, training, and awareness programs. By implementing (or not implementing) such countermeasures, an organization helps define its commitment to security, but it is the employee's awareness and identification with such commitments that proffer to impact behavioral intent.

Bulgurcu et al. (2010) developed a comparable variable, called information security awareness, which has a direct effect on both behavioral intent and an indirect effect via an employee's cost-benefit analysis. Information security awareness is defined as an

employee's general knowledge about information security and specific knowledge of the ISP of their organization (Bulgurcu et al., 2010). In terms of organizational commitment, as with the D'Arcy et al. (2009) study discussed above, implementing (or not implementing) an organizational ISP, an organization helps define its commitment to security, but it is the employee's awareness of related information security threats and identification with the ISP that proffer to impact behavioral intent.

Including other variables, such as organizational commitment, with the TPB is considered an acceptable practice. While the TPB's *behavioral intent* construct has been consistently measured based upon subjective norms, attitude, and PBC, any number of factors may directly or indirectly influence behavioral intentions based upon the context applied to the behavior of interest (Ajzen and Albarracin, 2007; Conner and Armitage, 1998; Fishbein, 2008). The inclusion of organizational commitment to the composite ISP compliance model makes logical sense and has some measure of empirical validation (Bulgurcu et al., 2010; D'Arcy et al., 2009; Herath and Rao, 2009a). For sake of parsimony, the organizational security commitment construct measurements defined by Herath & Rao (2009a) are used in this study.

Exclusion of the Technology Acceptance Model (TAM)

Of the 12 papers that inform the composite model developed in this study, only Al-Omari et al. (2012) attempts to integrate TAM into an ISP behavioral compliance model. Indeed, the Al-Omari et al.(2012) paper is only included in literature review for this study specifically to address why TAM will not be used in the composite framework of ISP behavioral compliance presented in the next section.

Davis (1989) introduced TAM to address the issue of employee willingness (or unwillingness) to use new information technology in the workplace. To address limitations in the theory of reasoned action (also the foundation for the TPB), Davis introduced the concepts of perceived ease of use and perceived usefulness (Davis, 1989; Davis et al., 1989). Perceived ease of use equates to the extent to which users believes use of the technology will be effortless. Perceived usefulness addresses employee beliefs about how using the technology will enhance their work performance. Since its inception, TAM has been widely studied, resulting in numerous extensions including TAM2 (Venkatesh and Davis, 2000), TAM3 (Venkatesh and Bala, 2008), and the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003).

There are at least two distinct reasons for excluding TAM (and TAM extensions) from ISP behavioral compliance research models. First, ISP behavioral compliance is less about the use of a specific technology to accomplish a job task than it is about the application of numerous technologies and processes (and in some cases, just processes) meant to protect organizational information resources from a range of security threats. Additionally, while the TAM model has been empirically validated in its ability to predict employee behavioral intent to voluntarily use an information system (Huh, Kim & Law, 2009), it fails in environments of obligatory technology use (Dinev and Hu, 2007). For example, one of the information security threats explored in this study is the problem of inappropriate use of removable flash media on organizational information systems. The ISP described later in this chapter specifically calls for employees to refrain from using any removable flash media on U.S. Department of Defense computing resources. Thus, in order to comply with the ISP in this case, employees are not being requested to adopt the

use of any particular technology; instead, they are being directed to not use a threatening technology, primarily enforced through mandatory process compliance. The TAM model, in this case, is clearly not applicable.

Second, the majority of TAM models (Venkatesh and Davis, 1996; Venkatesh, 1999; Venkatesh, 2000; Venkatesh and Davis, 2000; Venkatesh et al., 2003; Venkatesh and Bala, 2008) eliminate attitude as an antecedent of employee intent towards IT usage (Dinev and Hu, 2007). Removing attitude as a mediator of behavioral intent contradicts the basic principles of the theory of reasoned action and the TPB. Eleven of the twelve studies that inform the composite model in this study (excluding Al-Omari et al., 2012) find attitude a strongly significant component of an employee's behavioral intent to comply with organizational ISPs. Inclusion of the TAM model (and its associated variables) would conflict empirically with all of the studies used to inform the composite ISP behavioral compliance framework and model presented in this study.

In a study addressing individual user adoption of anti-spyware software at home (in a non-work environment), Dinev and Hu (2007) evaluated both TAM and the TPB on behavioral intent. They found that neither perceived usefulness nor perceived ease of use significantly impacted behavioral intention to use technologies they defined as protective in nature. They posited that protective technologies were used more out of fear of the negative consequences of not using the technologies (Dinev and Hu, 2007). The TPB attitudinal component, as addressed above, incorporates a threat assessment component that addresses such beliefs.

ISP Behavioral Compliance Research Settings and Potential Issues

One of the potential weaknesses being explored in this study is the transportability of findings from related research to actual organizations. A summary of the research settings for the papers that inform this study are included in Table 2. Several important items can be discerned from this table. First, eight of the studies collected participant responses to survey questions based upon the general context of an overall information security policy. Essentially, all of the antecedents of behavioral intent in these papers' various models were measured based upon user feedback of the ISP as a whole. This measurement decision is potentially troublesome as ISPs typically address a range of information security threats and directed response mechanisms (Panko, 2009). As with the discussion on monolithic representation of TPB variables above, there is a danger that evaluating employee perceptions based on the monolithic concept of the overall meaning of an organization's ISP could result in inaccurate variable measurement or improper determination of significance in related structural models. Thus, an employee's perceived vulnerability of information resources from all security threats included in an ISP (for example = low) may be very different from the perceived vulnerability associated with very specific threats, such as phishing (for example = high) or tailgating (for example = very low).

Only four of the studies identified on Table 2 address specific information security threats. However, none of those studies compare employee behavioral intent for the specific threats identified with the notion of general ISP compliance, making comparison of results between the related studies more difficult. Additionally, of the four threat-specific studies, only one (Johnston and Warkentin, 2010) actually verified that the

specific threat being addressed by their model was even in the ISP of the organization. Thus, while all the specific threats in the four studies have solid face validity (they are widely accepted security threats that are ubiquitously present in any organization), there is no certainty that the respondents' answers about these threats pertain to actual ISP content or compliance intent. Unfortunately, even in the Johnston and Warkentin (2010) (2010), the ISP did not mandate action for the specific threat explored in the study. Obligatory compliance is a foundation of the effectiveness of an ISP (Panko, 2009).

On the matter of ISP existence comes another concern. Of the twelve studies shown in Table 2, only two of the studies (Workman et al., 2008; Johnston and Warkentin, 2010) explicitly state that the authors had access and knowledge of the subject organizations' ISPs. Six of the studies make no mention of whether their respondents' organizations even had ISPs. Three studies only accepted and evaluated responses from respondents that acknowledged presence of an ISP in their organization. Finally, one study (Ifenido, 2012) accepted responses from employees whether they acknowledged presence of an ISP or not.

The present study addresses the above weaknesses and omissions. Information security policy behavioral compliance intent is being studied within a single (large) organization with an established and available ISP. A composite theoretical framework will be modeled using structural equation methods to evaluate compliance intent from a general viewpoint as well as specific threats from the actual ISP as described in the next section. The following section describes several information security threats and the specific guidance in the organizational information security policy to address those threats.

Authors	ISP Context	Participants	Author Knowledge of Organizational ISP
Al-Omari, A., El-Gayar, O., & Deokar, A. (2012)	General ISP compliance (no scenarios)	Multiple organizations, anonymous	Only accepted responses from respondents that acknowledged the presence of an ISP at their organization. No discussion of content of any of the organization ISPs.
Bulgurcu, B., Cavusoglu, H., Benbasat, I. (2010)	General ISP compliance (no scenarios)	Multiple organizations, anonymous	Only accepted responses from respondents that acknowledged the presence of an ISP at their organization. No discussion of content of any of the organization ISPs.
D'Arcy, J., Hovav, A., & Galletta, D. (2009).	Four hypothetical scenarios: sending inappropriate email, use of pirated software, unauthorized access to computer resources, unauthorized modification of computerized data	Multiple organizations, anonymous	No discussion of presence of ISP at any organization or, if there was an ISP, whether any of the scenarios were included in the subject's ISP.
Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011)	Four hypothetical scenarios: writing down passwords, sensitive data on flash media, downloading software from Internet, use of insecure publi wifi	Multiple organizations, anonymous	No discussion of presence of ISP at any organization or, if there was an ISP, whether any of the scenarios were included in the subject's ISP.
Herath, T., & Rao, H. R. (2009a)	General ISP compliance (no scenarios)	Multiple organizations, anonymous	No discussion of presence or content of ISPs at any organization.
Herath, T., & Rao, H. R. (2009b)	General ISP compliance (no scenarios)	Multiple organizations, anonymous	No discussion of presence or content of ISPs at any organization.
Ifinedo, P. (2011)	General ISP compliance (no scenarios)	Multiple organizations, anonymous	Asked respondents for presence of ISP at their organization. Included responses for all (regardless of ISP presence) in analysis. No discussion of content of ISPs at any organization.
Johnston, A. C., & Warkentin, M. (2010)	Single scenario: use of anti-spyware software	Single University faculty/staff/students	University ISP recommends but does not mandate individuals' use of anti-spyware software.
Ng, B.-Y., Kankanhalli, A., & Xu, Y. (Calvin). (2009)	Single scenario: opening email with attachments	Part-time working students in two university classes, working in 3 IT-related organizations	No discussion of presence of ISP at any of the 3 organizations or, if there was an ISP, whether the respective ISPs addressed the specific information security threat.
Pahnila, S., Siponen, M., & Mahmood, A. (2007)	General ISP compliance (no scenarios)	Single organization	No discussion of presence or content of ISP at the organization.
Workman, M., Bommer, W. H., & Straub, D. (2008).	General ISP compliance (no scenarios)	Single organization	Authors had access and knowledge of organization's ISP.
Zhang, J., Reithel, B. J., & Li, H. (2009)	General ISP compliance (no scenarios)	Multiple organizations, anonymous	Only accepted responses from respondents that acknowledged the presence of an ISP at their organization. No discussion of content of any of the organization ISPs.

Table 2: ISP Behavioral Compliance Research Settings

Information Security Threats in Context

The present study explores ISP behavioral compliance in the context of the U.S. Department of Defense (DoD). The DoD is an interesting research population that consists of a mixture of military and civilian work force members. As of September 2010, the DoD employed 1,458,697 active duty service members (39.4%), 1,078,621 military ready reserve members (29.2%), and 919,254 (24.9%) (DoD, 2010). In addition to the approximately 3.5 million employees described above, there are also tens of thousands of private contractors that work with or for the DoD. All of these employees have at least one thing in common – they all fall under the same general ISP, known as DoD Information Awareness Assurance (IAA). Each and every DoD employee, regardless of rank, status or organization, falls under the IAA guidelines. Additional information security policy guidance may be provided by an individual's organization or for the DoD as a whole, such as for removable flash media usage (see below). The version of IAA guidance that was active for this study was version 10 which could be accessed freely (http://iase.disa.mil/eta/iaav10/index.htm) and provided guidance for 26 defined information security threats. All of the information security threats contained in IAA v10 are or can be applicable to any type of organization that operates information systems and that create or process any kind of sensitive information. Three of the threats from IAA v10 have been chosen below for examination in this study because of their currency and applicability in non-DoD organizations. Following is a description of the three threats and a brief description of their security impact on organizations (and specifically the DoD).

Phishing

As presented earlier, phishing is defined as an information security attack that uses authentic-looking email messages or websites to trick users into taking harmful actions or revealing personal or confidential information (Panko, 2009). In the IAA v10 guidelines and training, phishing is addressed more times (four) than any other security threat (DISA, 2012). Phishing is a dangerous threat where, rather than targeting a system people use, it targets the people using the system (Hong, 2012). While the IAA v10 primarily addresses phishing via email, the phenomenon has also spread to other mechanisms such as social networking sites (Arthur, 2009), online multiplayer games (Cavelli, 2009), and voice over IP (Internet Protocol), SMS (Short Message Service), and instant messaging (Verisign, 2009).

Phishing attacks against DoD personnel are common and can target employees' person and official DoD email addresses. In May 2010, the U.S. Strategic Command went to the great lengths to issue a press release for dissemination to all DoD personnel warning of phishing attacks aimed at customers of the United States Automobile Association (USAA) financial services and Navy Federal Credit Union (NFCU) (Daniel, 2010). The phishing e-mails appeared to originate from USAA and NFCU, ask the recipient to provide or verify a bevy of personal information such as name, account numbers, date of birth, mother's maiden name, and Social Security numbers. Similarly, University of Hawaii (UH) faculty, staff and students are regular targets of phishing attacks. For just the month of February 2012 alone, 16 unique phishing attempts against UH personnel were reported (see Security Alerts on http://www.hawaii.edu/its/ for current phishing alerts).

The primary defenses against phishing that most organizations can possibly implement are procedures (and training on the procedures) for employees to follow to negate the potential impact of phishing (Hong, 2012). As such, protecting against phishing is almost completely up to the user following practices defined in the ISP. Following are the IAA v10 guidelines for protecting against phishing, spear phishing (phishing aimed at a specific or group with tailored information meant to enhance tricking the recipients), and whaling (spear-phishing aimed at an organization's top executives).

Phishing:

- Do not access the web by selecting links in e-mails or pop-up messages
- Contact the organization using a telephone number
- Delete the e-mail
- View all e-mail in the plain text
- Type the web address or use bookmark
- Report e-mails requesting personal information to your POC
- Use caution when visiting sites with expired certificates
- Report trusted sites with expired certificates

Spear phishing:

- Assume all unsolicited information requests are phishing attempts
- Never reveal any personal information in an e-mail
- Look for digital signatures
- Never give out your password; IT will never ask for your password
- Never reveal any personal information in an e-mail

Whaling:

- Contact sender by other means before opening a doubtful attachment or clicking on a link
- Never give out organizational, personal, or financial information to anyone by e-mail
- Follow your organization's IT security policies and guidelines
- Contact your security POC regarding suspected whaling attempts

Additionally, DoD organizations have the authority to provide additional guidance and requirements on their users regarding phishing. For example, current Department of the Navy guidance requires employees to NOT select any web link or open an attachment that comes in an email unless the email is properly signed by the holder of a DoD public key infrastructure (PKI) digital signature. This requirement is aimed to help combat some, but clearly not all, forms of phishing.

Tailgating

Also known as piggybacking, tailgating is the act of gaining access to a secured area by following someone with legitimate access (Panko, 2009). As with phishing, tailgating is an information security problem that affects organizations beyond the DoD. Tailgating has been a physical access control challenge throughout history (Jensen, 2011). There are a plethora of technical solutions meant to obviate tailgating ranging from tailgate sensors to mantraps, biometrics devices and more. However, such technologies are expensive and sometimes physically difficult or impossible to implement at all organizations that have

information resources to protect. This reality applies to all organizations from elementary schools to major DoD offices.

Jenson (2011) describes a hypothetical building (organization type really doesn't matter) where employee entrances are protected by electronic card access. Employees carry an ID badge that also serves as a card access key. Tailgating into the facility can be as easy as pretending to have left your badge in the car, somewhere in your briefcase, or by pretending to be on a busy phone call but confidently acting like you belong inside the facility (Greenless, 2009). In the DoD context, where organizations regularly store and process sensitive or classified information, gaining unauthorized access can have disastrous consequences.

Homeland Security Presidential Directive 12 (HSPD-12) sets a clear goal to improve physical access control systems in federal agencies (including the DoD) through the use of government-wide standards. The National Institute of Standards and Technology (NIST) is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets (NIST, 2008). According to NIST Special Publication 800-116 (2008):

> *"The physical access control systems deployed in most Federal buildings are facility-centric and utilize proprietary architectures. Therefore, many issued identification cards operate only with the access control systems for which they were issued. The technologies used in these systems may offer little or no authentication assurance, because the issued ID cards are easily cloned or counterfeited."*

Following are the IAA v10 guidelines for protecting against tailgating.

- Use ONLY your own security badge or key code
- Never grant access for someone else
- Maintain possession of your security badge at all times (provides access to buildings and computer systems and contains information about you that is used to verify your identity)
- Challenge people without proper badges
- Be wary when people with visitor's badges ask about other people's office locations
- Report suspicious activity

As identified above, protecting against tailgating requires more than just the employees following proper access control procedures and supporting technologies; it is incumbent upon all DoD employees (that work in controlled access areas) to enforce the rules of the ISP on others.

Removable Flash Media

It currently costs less than $7 for an 8 gigabyte (GB) flash drive on Amazon.com. These cheap, convenient, small storage devices have been a security bane to organizations for years. In a 2009 survey of IT security professionals and executives worldwide, 57% of respondents reported that their top security concern was personal portable storage device misuse (Computer Economics, 2009). Removable flash media (and all other removable media) devices are considered a major potential source of

information leakage from organizations, yet approximately one-third of respondent organizations make no attempt to deter such device use.

Beyond information leakage, thumb drives also present a serious threat to the integrity of a computer system. In March 2013, Microsoft issued Microsoft Security Bulletin MS13-027, entitled "Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege (2807986)." The vulnerabilities identified in the bulletin affected all supported versions of the Windows operating system, including the newly released Windows 8, and allow attackers to gain full control of a targeted computer using USB-connected drives. The above vulnerability is truly significant; it can be triggered whether a target workstation is locked or when no user is logged in, allowing an attacker with only casual physical access to the machine to gain full system administrator privileges (Goodin, 2013).

The DoD has suffered numerous security incidents at the hands of removable flash media:

- In March 2006, the United States Marine Corps admitted that a flash drive was lost that contained personally identifiable information (PII) for enlisted Marines serving between 2001-2005. Information lost included name, marital status, and social security numbers. (MARADMIN 143/06, 2006)
- In 2007, the Department of the Navy reported over 100 incidents during an 18-month period involving the loss of PII. The loss impacted over 200,000 military and civilians employees, and their dependents. The most common causes of data loss was the loss or theft of laptop computers, thumb drives, and other portable removable media. (ALNAV, 057/07).

- In April 2006 in Bagram, Afghanistan (while the author of this study was serving at Bagram Airfield), western journalists identified flash/thumb drives identified for sale in local Afghani markets. Located on some of the flash media were classified documents, photos, and phone numbers of people described as Afghan spies working for the U.S. military, as well as PII for U.S. service members (Gall, 2006).

However, by far the most significant security incident involving removable media in the DoD occurred in 2008. In 2010, William Lynn, the U.S. Deputy Secretary of Defense at the time, admitted that the most significant breach of U.S. military computers in modern history was caused by a flash drive inserted into a U.S. military laptop from a remote base in the Middle East in 2008 (Lynn, 2010). Malicious code placed on the drive by a foreign intelligence agency uploaded itself onto a network run by the U.S. military's Central Command and infected tens of thousands of computers on both unclassified and classified systems. The incident led to a 2008 complete ban on the use of flash media on all DoD computer systems.

In 2011, the DoD ban on removable media (to include thumb/flash drives, CDs, DVDs, and external hard drives) was partially relaxed to allow use for command-directed and documented mission essential tasks (Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01F, 2011). However, if a subordinate DoD organization decides it does want to allow the use of removable media, it must meet the conditions identified by the Committee on National Security Systems Policy (CNSSP) No. 26 entitled “National Policy on Reducing the Risk of Removable Media.” The conditions of CNSSP 26 are extensive and include the following: If removable media are required, Departments and

Agencies should use the following mitigation techniques, at a minimum, to reduce risks to national security systems (NSS).

- Craft, promulgate, and implement risk management policies concerning the use of removable media.
- Restrict use to removable media that are USG-owned, and have been purchased or acquired from authorized and trusted sources.
- Encrypt data on removable media using, at a minimum, the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules.
- Verify that the media contain only the minimum files that are necessary, and that the files are authenticated and scanned so that they are free of malicious software. This should be completed prior to the media being inserted into NSS. Use a verification process authorized by the Department or Agency for Assured File Transfer. This verification process should be performed on a non-networked, stand-alone machine.
- Limit use of removable media to authorized personnel with appropriate training.
- Implement a program to track, account for, and safeguard all acquired removable media, as well as to track and audit all data transfers.
- Conduct both scheduled and random inspections to ensure compliance with Department/Agency promulgated guidance regarding the use of removable media.
- Implement system level software restriction rules in order to significantly reduce the potential for malicious code execution by removable media.

The specific actions called for in IAA v10, if an employee's agency does have a local policy for the use of removable media (in accordance with CNSSP 26 and CJSCI 6510.01F) include:

- Encrypt all data stored on removable media
- Encrypt in accordance with the data's classification or sensitivity level
- Label to reflect the sensitivity level
- Store in GSA approved storage containers at the appropriate level of classification
- Purge all removable media before discarding
- Follow your organization's policy for purging or discarding removable media
- Contact your security POC for more information

The ISP for this study imposes explicit actions on the individual employee when using (or considering using) removable media. However, from the author's personal experience and the DoD Information Assurance experts interviewed during this study, the prohibitions towards using removable media on DoD computer systems are among the most well-known and publicized of the ISP requirements for DoD employees. Unlike the aforementioned ISP rules for phishing (individual focus of effort), there is an implicit expectation in the DoD to question the use of removable media, especially flash media, by other employees.

CHAPTER 3. RESEARCH MODEL AND HYPOTHESES DEVELOPMENT

ISP Behavioral Compliance Composite Theoretical Framework

Based upon Taylor and Todd's (1995) decomposition of the theory of planned behavior and supporting studies that inform or expand the components of the TPB, a modified TPB theoretical framework for ISP behavioral compliance model is presented in Figure 3. As illustrated in Figure 3, subjective norms, attitude, perceived behavioral control, and organizational commitment are direct antecedents of behavioral intent.

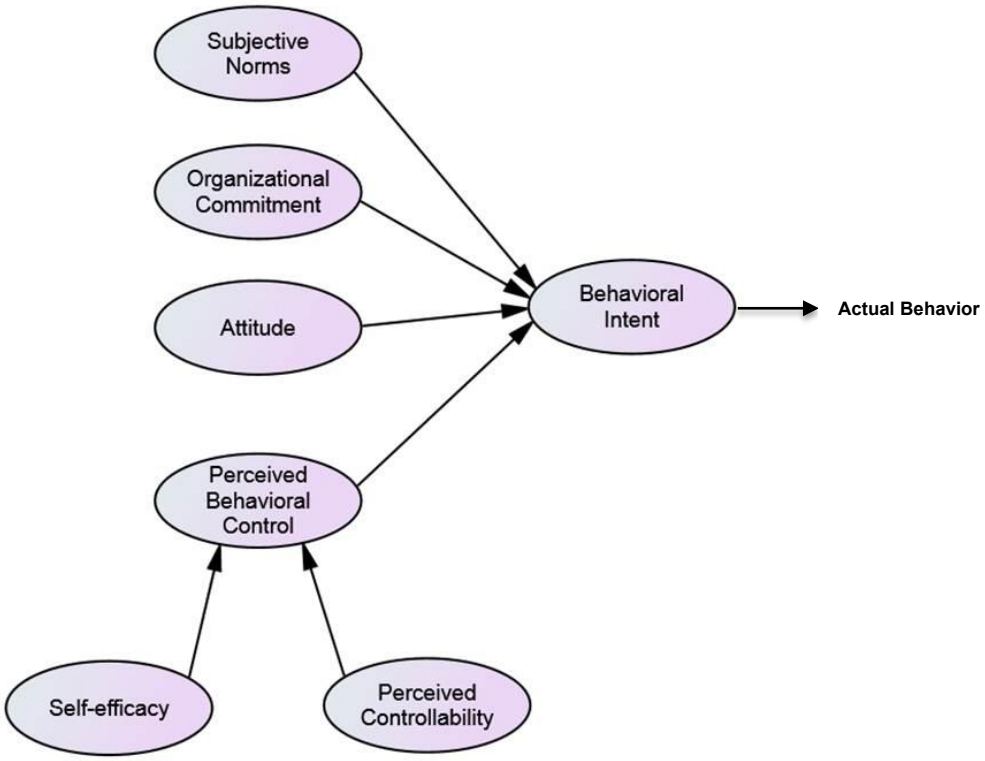

Figure 3: Modified TPB Model for ISP Behavioral Compliance

Perceived behavioral control is formed by an employee's perceived self-efficacy and perceived controllability towards an ISP-directed behavior. Subjective Norms is the

perceived pressure to comply with the ISP from referent groups. Organizational commitment measures the overall strength of an individual's involvement and identification with their organization and captures the perceived relationship between the organization and the employee. Attitude represents the degree to which an individual has a favorable or unfavorable appraisal of an ISP-directed security behavior.

As described in detail in the previous chapter, a significant portion of the ISP behavioral compliance research has focused on expanding and expounding upon the antecedents of attitude as shown in Figure 4.

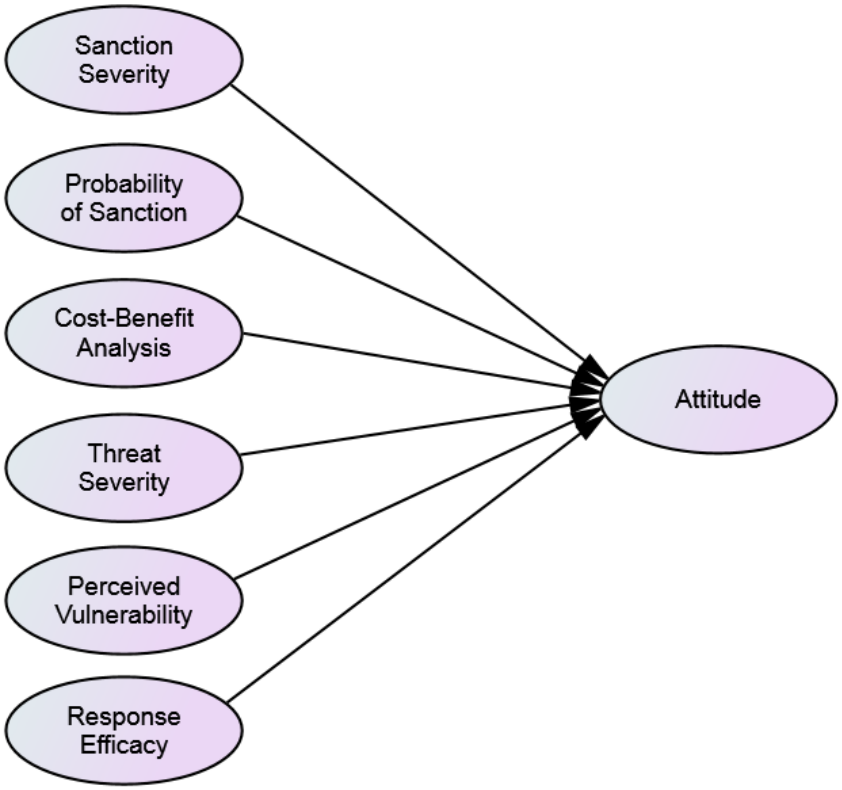

Figure 4: Decomposed Attitudinal Components of ISP Behavioral Compliance

The attitudinal component is formed by six direct antecedents based upon perceived sanction effects, perceived threat assessment, and cost-benefit analysis. Sanction effects are comprised of the perceived severity of a sanction (or set of sanctions) from the ISP and the perceived probability that a sanction will be imposed. Threat assessment is comprised of the perceived vulnerability from a security threat, the perceived severity of the threat, and the perceived response efficacy of the directed ISP behavior. Cost-benefit analysis is comprised of an employee's perceived benefit of ISP compliance, the perceived cost of compliance, and the perceived cost of non-compliances.

By combining the modified TPB framework for ISP behavioral compliance shown in Figure 3 with the attitudinal decomposition shown in Figure 4, a composite ISP behavioral compliance theoretical framework is formed and shown in Figure 5. Presented in Table 3 are normalized ISP behavioral compliance constructs, based upon the literature review presented in the previous chapter, represented in the composite framework. Following is a description of the constructs in the framework.

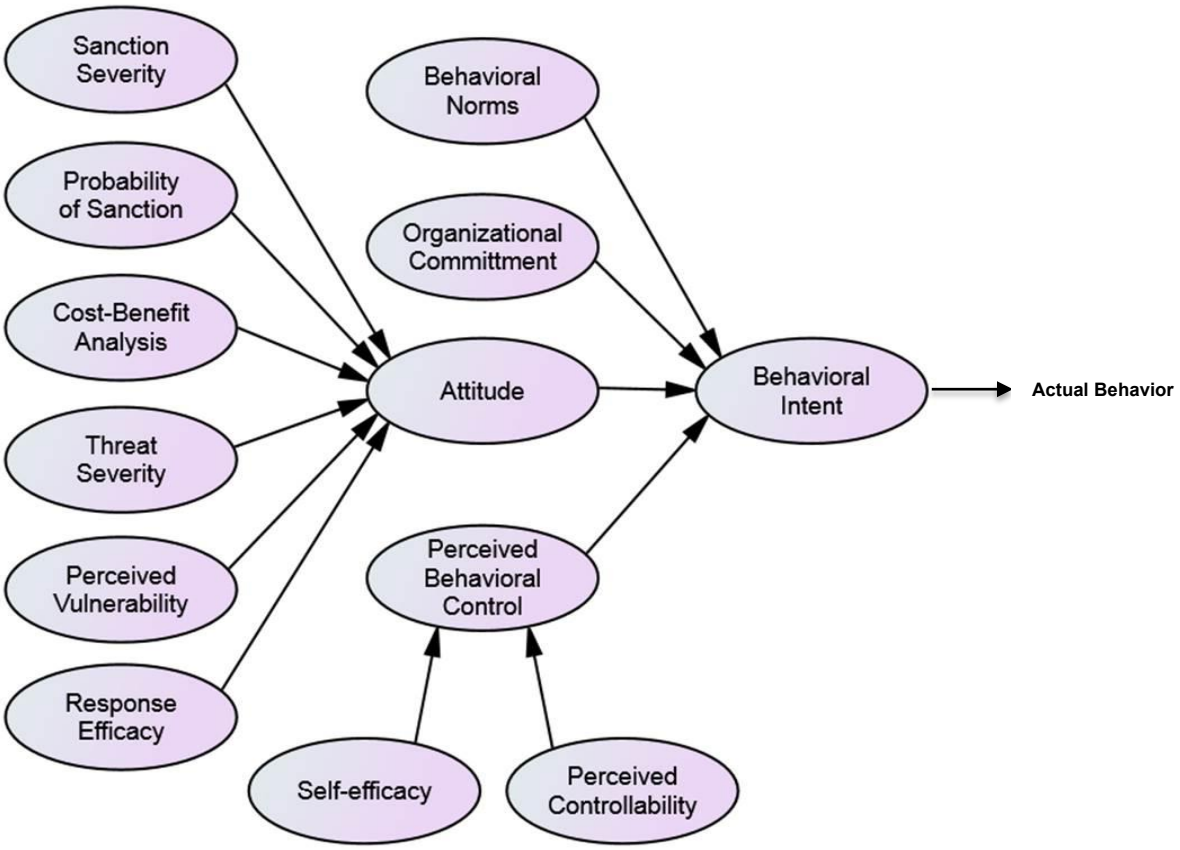

Figure 5: Composite ISP Behavioral Compliance Theoretical Framework

Construct	Definition	Supporting Theories
Behavioral intent (BINT)	An individual's intention to perform a particular ISP-related behavior	Theory of Planned Behavior
Subjective norms (NORM)	expectations of other people that result in perceived social pressure to comply with accepted security behaviors	Theory of Planned Behavior
Perceived behavioral controls (PBC)	An individual's perceptions about the presence of factors that may facilitate or impede the performance of an ISP-related behavior	Theory of Planned Behavior
Self-efficacy (SEFF)	An individual's beliefs about their own capabilities to carry out information security tasks	Social Cognitive Theory
Perceived controllability (CONT)	Considers an individual's sense of control over enforcing an ISP requirement	Theory of Planned Behavior
Attitude toward compliance (ATT)	favorable (or unfavorable) appraisal of that behavior	Theory of Planned Behavior
Perceived sanction severity (SSEV)	Perceived harshness of the penalty associated with a specific ISP disobediance	General Deterrence Theory
Perceived probability of sanction imposition (SPROB)	Perceived probability that an ISP disobediance will be punished if detected	General Deterrence Theory
Perceived vulnerability (PVUL)	Relates to how likely an individual feels that they will encounter a particular security threat	Protection Motivation Theory
Perceived threat severity (TSEV)	Perceived potential damage posed by a security threat	Protection Motivation Theory
Response efficacy (REFF)	Refers to an individual's perceived effectiveness of a particular recommended security threat response from the ISP	Protection Motivation Theory
Cost-benefit analysis (CBA)	The affective and cognitive assessment of a behavior acquired through personal experience based upon the overal expected favorable and unfavorable consequences to an individual for complying (or not complying) with the ISP	Rational Choice Theory
Organizational Commitment (ORCOM)	Overall strength of an individual's involvement and identification with their organization	Organizational Commitment

Table 3: Normalized ISP Behavioral Compliance Constructs

Research Phases and Models

Due to the complexity of the composite theoretical framework (consisting of 13 latent constructs), structural equation modeling analysis will be conducted in two phases. Phase One (ISP TPB Analysis) will evaluate the modified TPB model identified in Figure 3.

Phase Two (Attitudinal Decomposition) will evaluate the model identified in Figure 4. Both phases will be evaluated for the four conditions of General ISP compliance and compliance with specific ISP rules for phishing, removable flash media, and tailgating.

It is important to note that the composite theoretical framework presented in Figure 5 is a context-free theoretical model. In applying the organizational and threat contexts to the framework as identified earlier, as well as exploring possible alternative structural models based on supporting theory and related research, the structural models that follow resemble but do not always duplicate Figures 3 – 5. Explanation of the specific structural models evaluated in this study, along with tested hypotheses follows.

Phase One (ISP TPB Analysis) Model and Hypotheses

Evaluating the modified TPB theoretical model for ISP compliance requires an examination of the Perceived Behavioral Control (PBC) construct in context of the threat categories examined in this study. As discussed earlier, for situations where there is no controlling/facilitating factor being analyzed, it is acceptable practice to replace PBC with Self-efficacy (Ajzen, 2002). As discussed in Chapter 2, the threat conditions of Tailgating (explicitly) and Removable Flash Media (implicitly) require enforcement of ISP rules on coworkers and will be modeled with PBC as an antecedent to behavioral intent. Because the General ISP threat condition includes both Tailgating and Removable Flash Media threats, it too will be evaluated with PBC as an antecedent to behavioral intent. However, for the Phishing threat condition, the onus to follow the requirements of the ISP fall explicitly on the individual and there is no controllability aspect with respect to coworkers in this context. Thus, for Phishing, PBC will be replaced with the Self-

efficacy construct as an antecedent to behavioral intent. The structural model and hypotheses for General ISP, Removable Flash Media, and Tailgating contexts is shown in Figure 6. The structural model and hypotheses for the Phishing threat context is shown in Figure 7. As seen on Figures 6 & 7, Hypotheses 1, 2, and 3 are shared in all four threat contexts. Only Hypotheses 4, 5, 6, & 7 are different based upon the existence of controllability aspects of the threat.

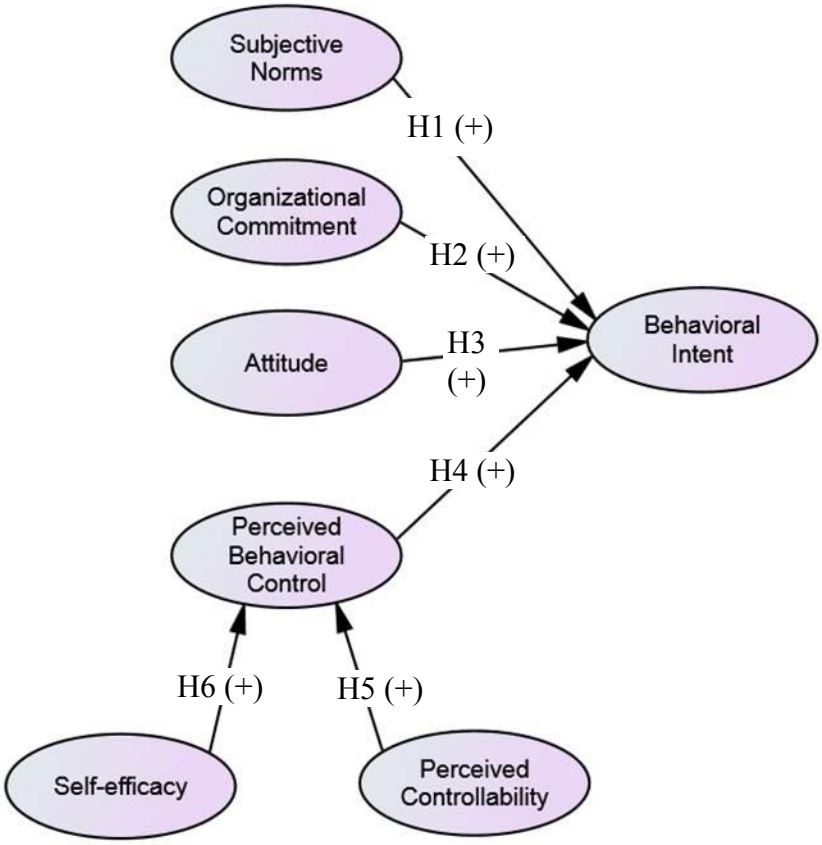

Figure 6: Phase One (ISP TPB Analysis) Model for the General ISP, Removable Flash Media and Tailgating Threat Contexts

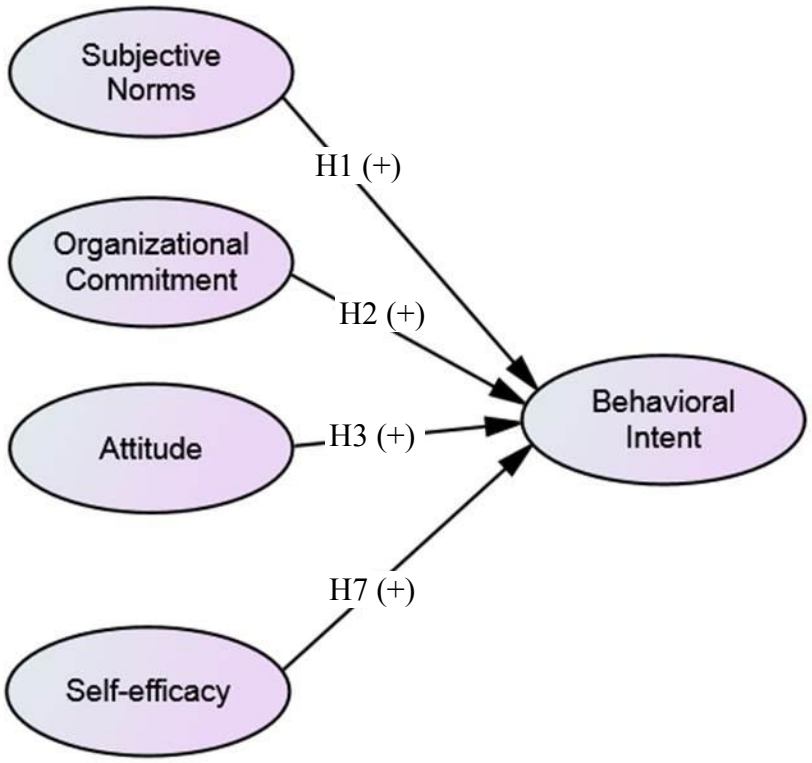

Figure 7: Phase One (ISP TPB Analysis) Model for the Phishing Threat Context

Subjective Norms

Subjective Norms addresses an individual's beliefs about the normative expectations of other people that result in perceived social pressure to comply with accepted security behaviors. Per the TPB, a positive relationship exists between subjective norms and behavioral intent. In the context of ISP compliance, if an employee believes that their relevant others (coworkers, managers, peers, subordinates, etc.) expect them to follow the guidelines of the ISP, the more likely they will be to comply (Bulgurcu et al., 2010). Therefore:

H1: Employees that perceive that relevant others positively expect them to comply with the ISP are more likely to have higher intentions to comply with the ISP.

Organizational Commitment

Organizational commitment is defined as the overall strength of an individual's involvement and identification with their organization and captures the perceived relationship between the organization and the employee (Mowday, 1999). In the information security context, employees are less likely to enact poor security behaviors and put their organization at risk if their organizational commitment is high (Herath and Rao, 2009a). Therefore:

H2: Higher levels of organizational commitment will result in an employee having higher intentions to comply with the ISP.

Attitude

In the context of obedience to ISPs, an employee's attitude forms when the compliance-related consequences that will be personally experienced if they comply or do not comply are considered (Bulgurcu et al., 2010). Attitudes toward a particular behavior refer to the degree to which a person has a favorable (or unfavorable) appraisal of that behavior (Ajzen, 1991). Regarding ISP compliance, users who have a more favorable attitude towards following the ISP will have a higher intention to comply with the ISP.

H3: Employees with a positive attitude towards ISP behaviors are more likely to have higher intentions to comply with the ISP.

Perceived Behavioral Control

Under the original TPB presentation by Ajzen (1991), PBC was presented as a unitary construct. After significant research and discussion, Ajzen (2002) enunciated that PBC has two distinct dimensions of self-efficacy and controllability. Taylor & Todd (1995), Pavlou & Fyngenson (2006), Dinev & Hu (2007) address PBC as a construct that is formed by the dimensions of self-efficacy and controllability, and that is how it is modeled in the present study. Perceived behavioral control refers to employees' perceptions about the presence of factors that may facilitate or impede the performance of an ISP-related behavior. In the context of ISP compliance, a greater perceived ease of performing the respective ISP behavior will result in a higher intention to comply with the ISP. As discussed above, PBC is being explored in the General ISP, Removable Flash Media, and Tailgating threat conditions. Therefore:

H4: Employees with higher perceived behavioral control are more likely to have higher intentions to comply with the ISP.

Perceived Controllability

Perceived controllability, per Ajzen (2002), is the personal sense of control over performing a behavior. The specific controllability context that this study is exploring is an employee's sense of control over enforcing an ISP requirement on the three important referent groups (peers, subordinates, superiors) in the organization. As discussed above, Perceived Controllability is being explored in the General ISP, Removable Flash Media, and Tailgating threat conditions. Therefore:

H5: Employees that perceive a higher personal sense of control over performing ISP behaviors are more likely to have higher levels of perceived behavioral control towards the ISP.

Self-efficacy

Self-efficacy refers to an employee's beliefs about his or her own capabilities to carry out a task (Bandura, 1977). Thus, an employee who believes that they have a stronger ability to act in accordance with the ISP will feel there is a greater presence of factors that facilitate the performance of an ISP-related. As discussed above, Self-efficacy is being explored in the all threat conditions examined in this study. However, for the Phishing threat, Self-efficacy is treated as a direct antecedent of Behavioral Intent while in the other threat conditions, Self-efficacy is treated as a direct antecedent to PCB. Therefore:

H6: Employees with higher self-efficacy (with regard to the General ISP, Removable Flash Media, and Tailgating threats) are more likely to have higher levels of perceived behavioral control towards the ISP.

H7: Employees with higher self-efficacy (with regard to the Phishing threat) are more likely to have higher intentions to comply with the ISP.

Phase Two (Attitudinal Decomposition) Model and Hypotheses

As discussed in Chapter 2, numerous TPB-related studies have shown that attitude can be a very important predictor of behavioral intent. This second phase of evaluating

the composite theoretical framework benefits from the focus of the majority of the literature in the information systems field on behavioral intent which has investigated attitude and its contributing factors. Unlike Phase One (ISP TPB Analysis) of this study, which focuses on the core TPB modified for the ISP compliance context, this study's focus on Attitudinal decomposition is unique in comparison to the studies identified in Table 1 in that it specifically explores the direct and indirect effects of theoretically postulated and empirically validated antecedents of Attitude. The structural model and hypotheses for Attitudinal decomposition is shown in Figure 8.

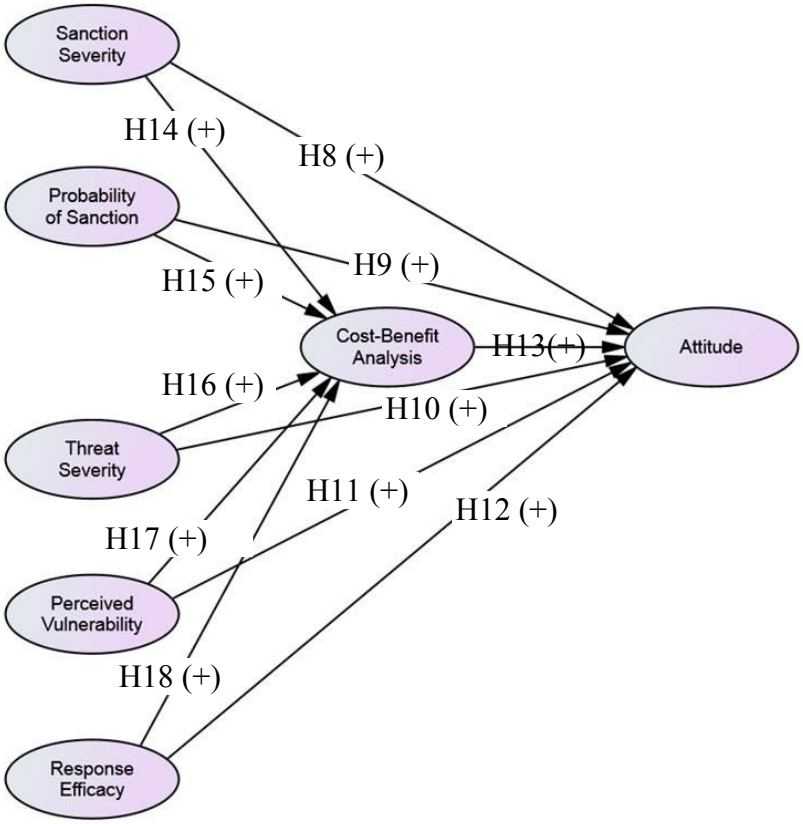

Figure 8: Phase Two (Attitudinal Decomposition) Model and Hypotheses

As described in the previous chapter, research in ISP behavioral compliance has focused on six main antecedents of attitude related to individual perceptions about sanction effects, threat assessment, and cost-benefit analysis.

Perceived Sanction Severity

Following the general deterrence theory, the greater the perceived severity of sanctions for a specific behavior, the more likely individuals are to avoid that behavior. Sanctions address negative outcomes that employees may try to avoid. Thus, the higher the perceived sanction severity for violating actions directed by the ISP, the more favorable the employee's attitude will be towards fulfilling the ISP behavior.

> ***H8: The more severe the perceived sanction for non-compliance with actions directed by the ISP, the more likely an employee will have a favorable feeling about fulfilling the ISP behavior.***

Perceived Probability of Sanction Imposition

Numerous criminology studies have shown that the perceived probability of sanction imposition has as strong, if not a stronger, deterrent effect than sanction severity (von Hirsch, Bottoms, Burney & Wikstrom, 1999). The higher the perceived probability of being punished for a behavior, the more favorable an individual's attitude will be to avoid that behavior and its associated punishment. In the context of ISP compliance, the more likely an employee is to be punished for failing to follow an ISP-directed behavior, the more likely the employee will be to follow the procedures. Therefore,

H9: The more certain an employee feels that they will be punished for non-compliance with actions directed by the ISP, the more likely an employee will have a favorable feeling about properly fulfilling the ISP behavior.

Perceived Threat Severity

According to the Protection Motivation Theory, the perceived severity of a threat will lead a person to behave more cautiously if their perception of the damage from the threat is great. Thus, if a person feels that a specific security threat called out in the ISP, such as the threat of spreading malicious software from opening unsafe email attachments, is very high, they will tend to have a more positive towards attitude towards following the ISP-directed behavior for that threat. Therefore:

H10: The more severe the perceived potential damage from an information security threat, the more likely an employee will have a favorable feeling about properly fulfilling the ISP behavior for that threat.

Perceived Threat Vulnerability

According to the Protection Motivation Theory, perceived vulnerability relates to how likely an employee feels that they will encounter a particular threat. Threats that are considered more likely will have a positive effect on how the employee feels about conducting the ISP-directed behavior for that threat. Therefore:

H11: The more vulnerable an employee feels towards a specific information security threat addressed by the ISP, the more likely an employee will have a favorable feeling about properly fulfilling the ISP behavior for that threat.

Perceived Response Efficacy

A person's belief about the availability and effectiveness of a threat mitigation action determines their behavior. Thus, an employee's perceived effectiveness of a recommended threat response behavior as called out in the ISP will have a direct impact on their attitude about performing that behavior. Therefore:

> ***H12: The more effective an employee feels the ISP response to a specific information security threat is, the more likely an employee will have a favorable feeling about properly fulfilling the ISP behavior for that threat.***

Cost-Benefit Analysis

According to classical Rational Choice Theory (Simon, 1955), when an employee considers executing a behavior, they conduct a cost-benefit analysis. The more beneficial an ISP-directed action when compared to its associated costs, the more positive an employee's attitude will be towards the ISP behavior. Therefore:

> ***H13: The more favorable the cost-benefit analysis for an ISP-directed action, the more positive an employee's attitude will be towards the ISP behavior.***

Cost-Benefit Analysis as a Mediator of Attitude

As discussed in Chapter 2, an employee's intention to follow ISP-directed behaviors may be influenced by whether they perceive that the effort required to protect an

information resource is worth the cost of the protection effort. It is noted, however, that cost-benefit attitudes vary among individuals when comparing such things as threat severity to their own self-interests (Workman et al., 2008). Thus, if an ISP action is considered to address an extremely important resource, but it is very difficult or exceedingly time consuming to conduct, an employee may perceive the cost as outweighing the benefit (Thomas & Thomas, 2004). Conversely, if an ISP action provides only a minimal benefit, but the associated effort is also minimal, it may be adopted (Pechmann et al., 2003). Workman et al. (2008) measure cost-benefit analysis by assessing the inconvenience, cost, and impact to an employee's work from implementing the ISP.

Similarly, Bulgurcu et al. (2010) posit that determinants of an employee's attitude originate in their beliefs about complying (or not complying) with the ISP and the consequences of their actions (Bulgurcu et al., 2010). Accordingly, employees' beliefs about overall assessment of consequences have three distinct components: perceived benefit of compliance, perceived cost of compliance, and perceived cost of non-compliance (Bulgurcu et al., 2010). *Perceived benefit of compliance* is the overall expected favorable consequences to an employee for complying with the ISP. *Perceived cost of compliance* is the overall expected unfavorable consequences for complying with the ISP. *Perceived cost of non-compliance* is the overall expected unfavorable consequences for non-compliance. Thus, Bulgurcu et al. (2010) postulate and empirically examine that an employee's attitude towards an ISP behavior is fully mediated through a cost-benefit analysis.

Based upon the above discussion, as well as the empirical evidence from the Bulgurcu et al. (2010) study, it is plausible that an employee's Cost-Benefit Analysis mediates the relationship between Attitude and the components of Sanction Effects (Perceived Sanction Severity and Perceived Probability of Sanction Imposition) and Threat Assessment (Perceived Threat Severity, Perceived Threat Vulnerability, and Response Efficacy). In addition to the evaluating the direct effects of the attitudinal decomposition elements, this study explores the direct effects of Sanction Effects and Threat Assessment on Cost-Benefit Analysis in order to explore possible mediation. Therefore:

H14: The more severe the perceived sanction for non-compliance with actions directed by the ISP, the more likely an employee will have a favorable analysis of the costs and benefits of following the ISP behavior.

H15: The more certain an employee feels that they will be punished for non-compliance with actions directed by the ISP, the more likely an employee will have a favorable analysis of the costs and benefits of following the ISP behavior.

H16: The more severe the perceived potential damage from an information security threat, the more likely an employee will have a favorable analysis of the costs and benefits of following the ISP behavior.

H17: The more vulnerable an employee feels towards a specific information security threat addressed by the ISP, the more likely an employee will have a favorable analysis of the costs and benefits of following the ISP behavior.

H18: The more effective an employee feels the ISP response to a specific information security threat is, the more likely an employee will have a favorable analysis of the costs and benefits of following the ISP behavior.

Mediation refers to a third variable that provides a clearer interpretation of the relationship between two examined variables by elucidating the causal process among the three variables (Baron & Kenny, 1986). Inferences concerning mediational relationships hinge on the validity of the assertion that the relationships depicted unfold in that sequence (Stone-Romero & Rosopa, 2004). In the present study, the mediating variable being examined is Cost-Benefit Analysis with the examined variables being the components of Sanction Effects and Threat Assessment, as seen in Figure 2.

H19: Cost-Benefit Analysis positively mediates the relationship between Perceived Sanction Severity and Attitude, such that a more severe perceived sanction severity for not following an ISP-directed behavior is likely to be associated with a more favorable Cost-Benefit Analysis, and a more favorable Cost-Benefit Analysis is likely to be associated with a more favorable feeling about properly fulfilling the ISP behavior for that threat.

H20: Cost-Benefit Analysis positively mediates the relationship between Perceived Probability of Sanction Imposition and Attitude, such that a higher perceived probability of sanction imposition for not following an ISP-directed behavior is likely to be associated with a more favorable Cost-Benefit Analysis, and a more favorable Cost-Benefit Analysis is likely to be associated with a more favorable feeling about properly fulfilling the ISP behavior for that threat.

H21: Cost-Benefit Analysis positively mediates the relationship between Perceived Threat Severity and Attitude, such that the more severe the perceived potential damage from an information security threat addressed in the ISP, the more likely it is to be associated with a more favorable Cost-Benefit Analysis, and a more favorable Cost-Benefit Analysis is likely to be associated with a more favorable feeling about properly fulfilling the ISP behavior for that threat.

H22: Cost-Benefit Analysis positively mediates the relationship between Perceived Threat Vulnerability and Attitude, such that the more vulnerable an employee feels towards a specific information security threat addressed by the ISP the more likely it is to be associated with a more favorable Cost-Benefit Analysis, and a more favorable Cost-Benefit Analysis is likely to be associated with a more favorable feeling about properly fulfilling the ISP behavior for that threat.

H23: Cost-Benefit Analysis positively mediates the relationship between Perceived Response Efficacy and Attitude, such that the more effective an employee feels the ISP response to a specific information security threat is, the more likely it is to be associated with a more favorable Cost-Benefit Analysis, and a more favorable Cost-Benefit Analysis is likely to be associated with a more favorable feeling about properly fulfilling the ISP behavior for that threat.

CHAPTER 4. METHOD

Sample and Procedures

Data were collected using a questionnaire (see Appendix) administered to DoD employees at multiple organizations, all of whom fell under the same information security policy guidance (IAA v10) at the time of survey data collection. Primary survey collection was via an online survey tool using www.surveymonkey.com. However, as a condition of the DoD Institutional Review Board (IRB) that approved this study, a paper version of the questionnaire (identical to the online version) was made available to potential respondents. The DoD IRB's primary concern was the possible reluctance of some survey respondents to participate in an online survey using a government owned computer because all electronic communication on a DoD-owned computers are subject to government monitoring. Fifty paper surveys were completed; however, the reason for paper survey use was for convenience (surveys were provided at a gathering of employees) versus concern over DoD monitoring.

Survey email invitations and reminders were sent to organization leadership and digitally signed using the author's DoD Public Key Infrastructure (PKI) private cryptographic key to authenticate the sender. Digitally signing the survey invitation, which included a hyperlink to the online survey, was required by the ISP. Based upon feedback from the organizations that authorized surveying their personnel, 1380 DoD employees were provided the opportunity to participate in the survey. Individual survey responses were anonymous for both the organization and individual. In accordance with federal and DoD regulations, survey participation was voluntary.

A total of 317 survey responses were collected, 50 of which were paper surveys and the rest were online surveys, for a total response rate of 23%. Of the 267 online survey responses, 189 were usable; all 50 of the paper surveys were complete and usable. The 78 unusable surveys were categorized as such because the survey participants did not complete a significant portion of the survey as explained below. Therefore, the total useful sample was two hundred and thirty nine (239), and the useful survey response rate was 17.3%.

The survey consisted of a total of 49 questions divided into eight sections. The strategy of breaking up the survey into sections and showing current complete percentage is one of the recommendations from Dillman, Smyth & Christian (2008) for long surveys. The first section of the online survey consisted of the mandatory privacy act statement for surveys of DoD personnel. Respondents must select an option on the survey that indicates they understand the statement before they could continue to the survey. It was only after this section was successfully completed that any survey responses were recorded. The second section of the online survey consisted of the Informed Consent Affirmation which also must be agreed with prior to accessing the survey questions. Sections 3 – 6 of the survey consisted of the main survey questions (8-11 questions per section) used to evaluate the models identified earlier. Section 7 consisted of the demographics section which was placed at the end of the main survey questions in accordance with guidance from Dillman et al. (2008). Section 8 collected addition survey item questions not evaluated in this study. Based upon pilot studies, including a trial by a member of the DoD IRB, the survey took approximately 30 minutes to complete all 49 questions.

The 78 unusable online surveys were due to response mortality during the long survey. Of the 267 participants that completed Section 1, 239 agreed to the informed consent in Section 2 resulting in a 10.5% mortality rate from Section1. 218 respondents completed Section 3 (9% mortality rate from Section 2); 209 respondents completed Section 4 (4% mortality rate from Section 3); 195 respondents completed Section 5 (6.7% mortality rate from Section 4); 189 respondents completed all of Sections 1-7 (3% mortality rate from Section 5). In order to check possible response bias of respondents that did not finish all seven sections of the main survey, a series of ANOVAs were run between groups that finished all sections and those that completed up to sections 3 – 5 of the survey. Results of the ANOVA analysis showed no statistically significant difference in responses for measured variables.

Measures

Using validated and tested questions improves the reliability of survey research (Straub, 1989). The survey instrument for this study was derived from the previous literature review and validated quantitative scales specifically from the ISP behavioral compliance studies used to inform the composite model (see Table 1). While using empirically validated constructs adopted from previous studies may be sound and acceptable practice, additional content validation in the context of the study is recommended (Herath & Rao, 2009a). A three-step process was taken in this study. The survey instrument used in this study was first pre-tested by three DoD Information Assurance experts through interviews, focusing on the context of the established ISP and seeking to reduce ambiguity. These experts provided extensive item-level feedback

regarding content validity, item wording clarity, and opinion on possible respondent sensitivity of certain questions. The instrument was examined several times by this panel as changes were made to question clarity and content. Following the expert review, a pretest of 10 DoD users using the online survey tool (www.surveymonkey.com) was conducted. The participants were requested to provide feedback on any item that they did not understand, confusing wording, general mechanics of taking the survey online, the instructions provided, completion time, and any questions they felt uncomfortable answering. Several questions outside of the primary construct items were identified as uncomfortable, such as "Have you ever knowingly violated the ISP?" These questions were either reworded or removed from the survey.

A final pilot study was conducted with 20 DoD users (including the same 10 participants from the first pilot). The participants were requested to provide feedback on any item that they did not understand, confusing wording, general mechanics of taking the survey online, the instructions provided, completion time, and any questions they felt uncomfortable answering. Additionally, each of the 20 participants was given two versions of the survey in order to assess how to best collect survey response for the four threat categories (General ISP, Phishing, Tailgating, and Removable Flash Media). Two methods were being explored. The first method addressed the different threats for each distinct survey question in parallel. The second method was more scenario-based, asking each survey question for each threat context sequentially as a unit. All 20 respondents unanimously chose the first method as the preferred delivery of questions in context. The reason given was that having the same question asked four different times for the four threats felt overly redundant and frustrating to the participants when compared to the

single question – four threats per question – approach in method one. Thus, method one was chosen for the final survey instrument.

All of the following latent construct measurement items were measured using a 7-point Likert ordinal scale as described below. Although it is ideal to use interval scales in evaluating structural equation modeling (SEM) factor analysis (Heck, 1998) and path models, ordinal scales are often used in behavioral research. Five-point scales are considered acceptable for SEM analysis using the Maximum Likelihood (ML) estimation method (Boomsma, 1987), with a greater number of points on the scale better representing ordinal data as interval data (Heck, 1998). Seven-point Likert scales were the standard in the studies identified in Table 1. All scales and associated items are shown in the Appendix. The following constructs were measured for all four threat contexts (General ISP, Phishing, Tailgating, and Removable Flash Media) unless otherwise stated.

Behavioral Intent. The twelve studies shown in Table 1 are fairly consistent in their measurement of behavioral intent (BINT). All the studies referenced Ajzen's (1991) guidance on creating measures for the latent construct. Three items taken from Bulgurcu et al. (2010) were used to assess Behavioral Intent using a 7-point Likert scale ranging from (1) Strongly Disagree to (7) Strongly Agree.

Subjective Norms. Following from Taylor & Todd's (1995) decomposed TPB and specifically regarding the referent groups of subordinates, peers, and superiors, the Subjective Norm measures from Herath & Rao (2009a) and Karahanna et al. (1999) were used in the instrument. Three items were used to assess Subjective Norms using a 7-point Likert scale ranging from (1) Strongly Disagree to (7) Strongly Agree.

Attitude. The Attitude construct captures users' general feelings towards ISP-directed behaviors and used the measures from Herath & Rao (2009), which were derived from Peace et al. (2003) and Riemenschneider et al. (2003). Three items were used to assess Attitude using a 7-point Likert scale ranging from (1) Strongly Disagree to (7) Strongly Agree.

Organizational Commitment. As discussed in the earlier literature review, Ajzen (2002) states that the theory of planned behavior is expected to consist of additional constructs that capture the context of the evaluated behavior. In this case, Organizational Commitment becomes a core TPB construct in the ISP compliance context. Organizational Commitment items were taken from Herath & Rao (2009a), which were adopted from Mowday's (1998) organizational commitment questionnaire. Three items were used to assess Organizational Commitment using a 7-point Likert scale ranging from (1) Strongly Disagree to (7) Strongly Agree.

Perceived Behavioral Control. PBC measures were taken from Taylor & Todd's (1995) decomposed TPB and modified for the ISP behavioral compliance context. Three items were used to assess PBC using a 7-point Likert scale ranging from (1) Strongly Agree to (7) Strongly Disagree. Perceived Behavioral Control was measured for only three of the four threat contexts (General ISP, Tailgating, and Removable Flash Media). It was not measured for the Phishing threat context as the requirements of the ISP are directed solely upon the individual to follow the procedures on their own; there is no explicit or implicit requirement to enforce Phishing policies on others, which is the controlling factor being analyzed in this study.

Self-efficacy. The Self-efficacy construct is widely used in the ISP behavioral compliance literature and, based upon Bandura (1997), is fairly consistent in its measurement. Specific Self-efficacy measures were used from Herath & Rao (2009a), derived from Peace et al. (2003), and consisted of three items using a 7-point Likert scale ranging from (1) Strongly Disagree to (7) Strongly Agree.

Perceived Controllability. One distinction with Perceived Controllability is that it is being modeled as a formative construct while the other 12 variables in this study are measured as reflective constructs (taken from previously empirically validated as reflective in related research). Reflective constructs consist of measurement items that are interchangeable and a change in the overall construct implies a change in the same direction for all associated measures (Jarvis, MacKenzie & Podsakoff, 2003). In contrast, changes in the measures of formative constructs are hypothesized to cause changes in the underlying construct (Bollen & Lennox, 1991; Fornell & Bookstein, 1982). While reflective indicators are invoked in an attempt to account for observed variances or covariances, formative indicators, in contrast, are not designed to account for observed variables.

The rationale for modeling a construct as formative is based on the notion that dynamic concepts (such as Perceived Controllability) are likely to be manipulated differently by other factors (Trafimow et al., 2002); the factors in this case are the expectations of distinct referent groups that may not have any or equal influence on each other. Hence, Perceived Controllability cannot equally cause the beliefs of three distinct referent groups (peers, subordinates, and managers), thus rendering a reflective construct model unlikely. The beliefs about controllability of these three referent groups "makes"

the construct Perceived Controllability. Removing one of these elements (peers, for example) fundamentally changes the construct because not all referent group elements are represented Moreover, since a change in one of the lower-order factors (referent groups) does not necessarily imply an equal change in the other, a formative model is deemed more likely (Pavlou & Fygenson, 2006).

Per the guidance of Podsakoff et al. (2003), Perceived Controllability is included as a multiple indicators and multiple causes (MIMIC) (Joreskog & Goldberger, 1975; Diamantopoulos & Winklhofer, 2001) modeled construct with three formative items that follow Taylor & Todd's (1995) guidance for self and referent group measurement; the items measure the perceived controllability of an individual to follow the ISP if required to interact with referent groups (including peers, subordinates, and executives). The three measurement items are: I am confident that I can follow the overall (general information security / removable flash media / tailgating) guidance and actions directed by the ISP if I witnessed a violation in progress by one of my (executives / peers / subordinates (or those of lower rank/status)). The two reflective items, taken from Sparks et al. (1997) following Ajzen's (2002) guidelines for Perceived Controllability measurement, are: (1) Enforcing specific guidance and actions directed in the ISP on your coworkers is within your control and (2) It's mostly up to me to follow the guidance and actions directed in the ISP when I am required to enforce specific ISP policies on my coworkers. The five questions are assessed using a 7-point Likert scale ranging from (1) Strongly Disagree to (7) Strongly Agree. Perceived Controllability was measured for only three of the four threat contexts (General ISP, Tailgating, and Removable Flash Media). Perceived Controllability was not measured for the Phishing threat context as the requirements of

the ISP are directed solely upon the individual to follow the procedures on their own; there is no explicit or implicit requirement to enforce Phishing policies on others.

Perceived Sanction Severity. The measures for Perceived Sanction Severity were taken from Herath & Rao (2009a), which were derived from Peace et al. (2003) and Knapp et al. (2005). Perceived Sanction Severity consists of three items all using a 7-point Likert scale ranging from (1) Strongly Disagree to (7) Strongly.

Perceived Probability of Sanction Imposition. The measures for Perceived Probability of Sanction Imposition were taken from Herath & Rao (2009a), which were derived from Peace et al. (2003) and Knapp et al. (2005). Perceived Probability of Sanction Imposition consists of two items using 7-point Likert scales ranging from (1) Strongly Disagree to (7) Strongly Agree and (1) Very Low to (7) Very High.

Perceived Vulnerability. The measures for Perceived Vulnerability were taken from Ng et al. (2009), which were derived from Champion's (1984) instrument development guidelines for the health belief model. Perceived Vulnerability consists of three questions, all using 7-point Likert scales ranging from (1) Strongly Disagree to (7) Strongly Agree and (1) Very Low to (7) Very High.

Perceived Threat Severity. The measures for Perceived Threat Severity were taken from Ng et al. (2009), which were derived from Woon et al.'s (2005) application of the protection motivation theory. Perceived Threat Severity consists of four questions using a 7-point Likert scale ranging from (1) Very Harmless to (7) Very Harmful.

Response Efficacy. The measures for Response Efficacy were taken from Workman et al. (2008), which were adapted from Rippetoe & Rogers (1987) and modified according to Milne et al.'s (2000) recommendations. Response Efficacy consists of three

questions using a 7-point Likert scale ranging from (1) Very Ineffective to (7) Very Effective.

Cost-Benefit Analysis. Cost-Benefit Analysis measures were taken from Workman et al. (2008), which were adapted from Rippetoe & Rogers (1987) and modified according to Milne et al.'s (2000) recommendations. Cost-Benefit Analysis consists of three questions using a 7-point Likert scale ranging from (1) Strongly Disagree to (7) Strongly.

Control Variables

This study controlled for gender, job type / community, and whether the online survey was completed on a DoD or personal computer. As discussed earlier, the DoD IRB that approved this study identified a concern with possible response bias from the online survey being taken over a DoD-owned and monitored computer. The concern was that, knowing all DoD computers are subject to monitoring, respondents might answer the survey questions in a way that was more favorable or that they felt was expected of them.

Eight of the supporting studies shown in Table 1 controlled for gender (D'Arcy et al., 2009; Herath & Rao, 2009a; Herath & Rao 2009b; Guo et al., 2011; Johnston & Warkentin, 2010; Ng et al., 2009; Pahnila et al., 2007; Zhang et al, 2009); all of the studies found no significant impact of gender on Behavioral Intent with the exception of Herath & Rao (2009a) & Herath & Rao (2009b). It should be noted that both Herath & Rao studies used the same data. In the Herath & Rao (2009a, 2009b) studies, females

were shown to have a statistically significant higher reported Behavioral Intent score. Gender has been reported as a significant control variable in studies related to IS misuse intention (Leonard & Cronan, 2001; Leonard, Cronan & Kreie, 2004) where females showed a lower propensity towards intent to misuse information technology.

The control variable of job type / community was evaluated in four related studies (Bulgurcu et al., 2010; Herath & Rao, 2009a; Herath & Rao, 2009b; Johnston & Warkentin, 2010) and was included in this study, although this variable was not found to be a significant contributor to Behavioral Intent. The measurement items for job type / community were chosen to reflect the standard organizational departments in DoD organizations (Administration, Intelligence, Operations, Logistics and/or Maintenance, Command/Control/Communications/Computers, Command Staff Element, and Other). Only three respondents selected the "Other" choice; the specified communities provided were evaluated by the author and two senior DoD personnel to determine if there was a distinct "Other" category. Two of the respondents were reclassified as Operations and the last as Logistics and/or Maintenance.

Model Evaluation and Data Analysis

The ISP behavioral compliance intention models identified earlier were tested using covariance-based structural equation modeling (SEM) procedures using SPSS AMOS version 21 software. AMOS is an acronym that stands for Analysis of Moment Structures. Structural equation modeling techniques are considered an appropriate analysis method when testing or disconfirming explanatory relationships between latent constructs of a theoretically derived, *a priori* model (Raykov & Marcoulides, 2006).

Effectively, SEM techniques integrate construct measurements and the hypothesized causal paths into a simultaneous assessment that can analyze many stages of independent and dependent variables, including the error terms associated with item measurement, into one unified model (Gefen, Rigdon & Straub, 2011). Prior to conducting SEM analyses, the data were screened for issues that may jeopardize the results, such as outliers, multicollinearity, non-normality, and missing data (Kline, 2011; Byrne, 2001; Gefen et al., 2000). Measurement item convergent and discriminant validity were addressed during the confirmatory factor analysis (CFA) stage. Common method bias was addressed using the methods described in Podsakoff, MacKenzie & Lee (2003) per the guidance in Gefen et al. (2011).

Covariance-based SEM analysis consists of two parts: a confirmatory factor analysis stage and the structural model analysis (also known as path analysis) stage (Joreskog & Sorbom, 1989; Heck, 1998). The CFA stage assessed the quality / validity of the construct measures. Confirmatory techniques work best when you have measures that have been carefully developed and have been subjected to (and survived) prior exploratory and confirmatory analyses (Raykov & Marcoulides, 2006), as is the case in this study where all measurement items have been empirically evaluated and validated from previous, contextually-related studies. The CFA stage is performed on the entire set of measurement items for all latent constructs simultaneously, with each observed variable restricted to load on its *a priori* factor (Dinev & Hu 2007).

Following establishment of the measurement model in the CFA stage, the data were fitted to the hypothesized models and assessed for goodness-of-fit. The assessment of model fit was based on multiple criteria, as recommended by numerous sources (Raykov

& Marcoulides, 2006; Kline, 2011; Hu & Bentler, 1999; Heck, 1998). First, the Normed Chi-Square, which is the model chi-square coefficient divided by the overall degrees of freedom (X^2/df), is reported for which values ranging from less than 2.0 (good fit) to 5.0 (acceptable fit) (Kline, 2011) are used to assess evaluation. However, reliance upon X^2/df alone for model fit determination is cautioned. X^2/df is sensitive to sample size; larger samples tend to result in spuriously larger values of X^2/df (and the opposite is true for smaller samples) (Raykov & Marcoulides, 2006). Kline (2011) recommends, in addition to X^2/df, reporting one goodness-of-fit and one badness-of-fit metric when assessing overall model fit.

The comparative fit index (CFI) is the goodness-of-fit metric reported and measures model fit relative to a null or baseline model and relative noncentrality index; CFI is one of the most widely used goodness-of-fit indices in information systems SEM-based research (Gefen et al., 2011). Values for CFI above .90 (Marsh, Hau & Wen, 2004) or .95 are recommended (Russell, 2002; Hu & Bentler, 1998). The badness-of-fit metric reported is the standardized root mean square residual (SRMR). The root mean square (RMR) residual is the positive root of the unweighted average of the squared fitted residuals (Jöreskog & Sörbom, 2001) and represents the difference between the observed correlation and the predicted correlation. This measure tends to be smaller as sample size increases and as the number of parameters in the model increases (Hu & Bentler, 1999). Because the scale of RMR varies with the scale of the observed measurement items, the standardized RMR (SRMR) is typically reported. A high value of SRMR indicates that residuals (unexplained variance) are large on average, relative to what one might expect from a well-fitting model. A value of .08 or lower is generally considered a good fit (Hu

& Bentler, 1999). It is important to note that it is acceptable that not all fit indexes be simultaneously within the above threshold rules of thumb (Gefen et al., 2011).

The structural analysis stage specifies direct and indirect causal relationships among the constructs and the amount of unexplained variance (Anderson & Gerbing 1988). Path analyses were used to test hypotheses 1 through 18. The bias-corrected bootstrap estimation procedure in AMOS with 95% bootstrapping confidence intervals (Cheung & Lau, 2008) was performed to test the significance of the mediated effects in hypotheses 19 through 23. The bias-corrected bootstrap estimation procedure in SEM is a non-parametric approach involving multiple samples being drawn with replacement from the original data set and the model being re-estimated on each sample, allowing estimation of confidence intervals providing a range of plausible population values for the mediation effects. This bootstrapping approach is recommended for examining the mediation effects with latent variables to control for the effects of the measurement errors and the possible non-normal sampling distribution of the indirect effect.

Data Screening

Prior to conducting structural equation modeling, the data were screened for missing data (as discussed above), multicollinearity, multivariate normality, sample size, and outliers, Multicollinearity may occur when one or more predictor variables exhibit very strong correlations with one another, misleadingly inflating standard errors and can cause multiple SEM model fit issues (such as standardized regression weights >1 and negative variance estimates) (Grewal, Cote & Baumgartner, 2004). Per Grewal et al. (2004), high multicollinearity, in combination with low measure reliability, small sample size, and low explained variance in endogenous constructs, may result in numerous issues that

negatively impact SEM model analyses. First, if high multicollinearity exists, the SEM model may not terminate in a proper solution. Particularly in models with very high levels of collinearity (correlations among the exogenous variables greater than 0.9) and low measure reliability (composite reliability smaller than 0.7), improper solutions can be common. However, even when a proper solution can be obtained, multicollinearity can lead to inaccurate parameter estimates and a high incidence of Type II errors (failure to reject a null hypothesis), particularly when reliability is weak, sample size is small, and explained variance is low. In the present study, all SEM models properly terminated, and none of the facilitating conditions of very high correlations among exogenous variables and low measure reliability exist (as discussed below).

The variance inflation factor (VIF) statistic may be used to test for multicollinearity. According to Kline (2011), VIF greater than 10 signifies that the variable may be redundant. Using an iterative process, VIFs were evaluated using SPSS. First, the items scores for all the latent constructs were averaged to obtain a single indicator to be used in the regression analysis along with single indicators representing control variables. Using the VIF function of SPSS, each composite variable indicator takes a turn as the Dependent Variable (DV) and all other composite indicators are treated as Independent Variables (IVs). The process involves regressing all the IVs on the DV, record/examine the VIFs, and then switching the DV with one of the IVs and repeating until all indicators take a turn as the DV. The results indicated that none of variables exceeded a maximum VIF of 3. Thus, multicollinearity does not appear to be to be a problem in this dataset.

The assumption of multivariate normality was assessed using the test for normality option in AMOS 21 which provides a measure of the Mardia's coefficient of multivariate kurtosis as well as univariate normality statistics such as skewness and kurtosis for each variable. Kline

(2011) stated that the Mardia's test is limited by the fact that trivial departures from normality may be statistically significant in larger samples (>200 data points) and suggests that multivariate nonnormality is detectable through a careful evaluation of univariate distributions. According to Kline (2011) standardized skew index values between -3.0 and +3.0 and standardized kurtosis index of -10.0 to +10.0 may be considered roughly normal for SEM analysis using Maximum Likelihood (ML) estimation. The results demonstrated that none of the variables indicated the existence of skewness and kurtosis in the data close to the limits stated above; the data in this study is considered roughly normal and adequate for testing using the ML estimation method. However, to account for the potential impact of even mild deviations from perfectly normal data distributions on the X^2 model fit, Bollen-Stine bootstrapping (Bollen & Stine, 1992) is conducted.

Minimum sample size for SEM analyses depends on many factors such as data normality, size of the model, distribution of the variables, amount of missing data, reliability of the variables, estimation method used, and strength of the relationships among the variables (Marcoulides & Chin, 2012; Muthen & Muthen, 2002; Heck, 1998). Although SEM methods have existed and have been robustly examined for almost 40 years, there is no universal agreement on minimum sample size required for SEM analyses. However, many minimum sample size rules of thumb exist to help researchers: 10 times the number of item indicators in the model; 50 + 8 times the number of item indicators in the model; >200 observations (Gefen et al., 2011). The Phase 1 (ISP TPB Analysis) model has 7 variables with 23 measurement items and the Phase 2 (Attitudinal Decomposition) analysis model has 7 variables with 21 measurement items.. Sample size in the current study is 239 usable observations satisfies the above rules of thumb (>200

observations; 10 times the number of items = 230; 50 + 8 times the number of indicators = 234). Thus, sample size is considered adequate for this study.

Outliers are cases whose scores are substantially different from the rest in a dataset. Multivariate outliers have extreme scores on two or more variables or the pattern of the scores appears atypical in the sample. A common method for detecting multivariate outliers, which is also available as an option in AMOS 21, is based on the calculation of the Mahalanobis distance (D^2) statistic for each case. The outlying cases will have D^2 statistics that are distinctively different from all the other cases and have a low p-value leading to a rejection of the null hypothesis that these cases come from the same population (a recommended conservative level is $p < 0.001$) (Kline, 2011). The examination of the Mahalanobis D^2 and associated p-values in AMOS indicated that there were six - ten cases (depending on threat context) that have D^2 values that stand distinctively apart and have p-values lower than 0.001. However, when these values were deleted from the dataset, the results remained practically unchanged from the results reported below. The scores were examined in detail and for the most part were found plausible in the context of the survey. Thus, the scores were retained in the dataset.

Measurement Model Reliability, Validity, Common Method Variance

The overall recursive model (including all 13 latent constructs) was estimated using AMOS 21. Testing an SEM model typically consists of two parts. First, the Confirmatory Factor Analysis (CFA) stage (examination of the measurement model) is conducted followed by the structural model stage (testing of the hypotheses / model paths) (Raykov & Marcoulides, 2006; Kline, 2011). The CFA stage was performed on the entire set of

items simultaneously, with each observed variable restricted to load on its *a priori* factor. The necessary steps in validation of the measurement model and reliability assessment following the widely used validation heuristics recommended for SEM by Byrne (2001) and Gefen et al. (2000) follows. CFA evaluation was conducted for all four information security threats examined in this study.

First, to ensure the individual item reliability and convergent validity of constructs, factor loadings of individual measures on their respective underlying constructs, as well as the average variance extracted (AVE), was examined. Measurement item loadings for each threat context are shown in Table 4. Measurement item loadings on respective constructs for the large majority were above the recommended minimum value of 0.707, indicating, that at least 50 percent of the variance was shared with the construct; however, item values between .40 and .70 are acceptable for inclusion as long as composite reliabilities are above .70 (which they are in all cases) (Chin, 1998). The AVE values for all reflective constructs were greater than the minimum recommended value of 0.50 (Tables 5-8), indicating that the items satisfied the convergent validity requirements.

To ensure the discriminant validity of constructs in the research model, AVE, Maximum Shared Squared Variance (MSV), and Average Shared Squared Variance (ASV) were examined. The MSV is the square of the highest covariance between a specific factor and all other latent factors. The ASV is the average of the square of each covariance between a specific factor and all other latent factors. To show adequate discriminant validity, MSV and ASV should both be less than AVE, thus showing that the construct items load more on their respective latent variables than other constructs

(Hair, Black, Babin & Anderson, 2010). As shown in Tables 5-8, discriminant validity checks are considered satisfactory for this study.

To confirm the scale reliability and internal consistency of the constructs in the research model, the composite reliability (Fornell and Larcker 1981) and Cronbach's alpha scores were calculated. Composite reliability and Cronbach's alpha values of 0.7 or greater is considered acceptable (Gefen et al. 2000). Composite reliability scores are calculated by squaring the sum of the standardized loadings for a construct and dividing by the square sum of the standardized loadings for a construct plus the sum of the indicator measurement error. Cronbach's alpha was determined using SPSS 20. As shown in Tables 5-8, the composite reliability and alpha values for all of the constructs in the research model were greater than 0.70, demonstrating that all constructs had adequate reliability assessment scores.

Latent Construct	Item	Standardized Item Loadings by Threat Context			
		General ISP	Removable Flash Media	Tailgating	Phishing
Behavioral Intent	BINT3	0.991	0.973	0.866	0.953
	BINT2	0.972	0.981	0.944	0.984
	BINT1	0.945	0.969	0.948	0.919
Perceived Subjective Norms	SNORM3	0.668	0.845	0.842	0.758
	SNORM2	0.885	0.614	0.654	0.700
	SNORM1	0.718	0.937	0.915	0.907
Organizational Commitment	ORCOM3	0.536	0.563	0.556	0.550
	ORCOM2	0.816	0.791	0.821	0.782
	ORCOM1	0.800	0.813	0.780	0.831
Attitude	ATT3	0.891	0.913	0.802	0.863
	ATT2	0.944	0.934	0.913	0.972
	ATT1	0.942	0.961	0.803	0.897
Perceived Behavioral Control	PBC3	0.850	0.813	0.812	
	PBC2	0.858	0.732	0.801	
	PBC1	0.807	0.892	0.856	
Self-efficacy	SE3	0.946	0.968	0.968	0.963
	SE2	0.948	0.949	0.951	0.975
	SE1	0.936	0.961	0.926	0.960
Perceived Controllability	CONT2	0.840	0.830	0.864	
	CONT1	0.951	0.962	0.924	
Perceived Sanction Severity	SSEV3	0.728	0.788	0.826	0.792
	SSEV2	0.736	0.626	0.756	0.750
	SSEV1	0.724	0.762	0.815	0.778
Percevied Sanction Probability	SPROB2	0.849	0.831	0.872	0.892
	SPROB1	0.714	0.619	0.786	0.714
Cost-Benefit Analysis	CBA3	0.795	0.854	0.825	0.821
	CBA2	0.818	0.832	0.822	0.739
	CBA1	0.788	0.800	0.762	0.865
Perceived Vulnerability	VUL3	0.930	0.936	0.899	0.902
	VUL2	0.971	0.973	0.972	0.955
	VUL1	0.820	0.699	0.807	0.812
Perceived Threat Severity	TSEV4	0.889	0.924	0.925	0.909
	TSEV3	0.901	0.905	0.919	0.896
	TSEV2	0.952	0.916	0.915	0.949
	TSEV1	0.665	0.655	0.657	0.590
Perceived Response Efficacy	REFF3	0.854	0.762	0.821	0.849
	REFF2	0.923	0.958	0.949	0.932
	REFF1	0.829	0.864	0.930	0.826

Note 1: N = 239. All items significant at least at p< .0001
Note 2: Perceived Behavioral Control and Perceived Controllability not measured for the Phishing threat context.

Table 4: Confirmatory Factor Analysis Standardized Item Loadings

Finally, the threat of common method bias (Podsakoff et al., 2003; Straub et al., 2004) was addressed. By ensuring anonymity to the respondents, assuring participants that there were no right or wrong answers, requesting that each question be answered as honestly as possible, and providing no incentive for participating in the study, the

likelihood of bias caused by social desirability or respondent acquiescence is expected to be reduced (Podsakoff et al., 2003). Also, following Podsakoff et al. (2003), common method variance was empirically evaluated using Harman's single-factor test in two ways. First, all items in factor analysis were simultaneously loaded using Varimax rotation on a single item in SPSS (Dinev & Hu, 2007). No single factor accounted for a majority of the variance. Second, a Harman Single Factor CFA test was used which involved loading all item indicators for the thirteen latent constructs in the study on a single latent factor. The results showed poor data fit ($X^2/df > 8.5$, CFI < .35, SRMR > 0.14) for all threat contexts, suggesting that a single common method factor does not account for the majority of the covariance among the measures. Lastly, a marker variable, which is expected to be theoretically unrelated to all constructs in the study, was added to the structural model for all four threat contexts. A variable assessing an individual's self-assessment of their general computer knowledge measured on a 7-point Likert scale (1 = very low and 7 = very high), was included in the model. This marker variable was shown in previous ISP behavioral compliance studies to be unrelated to evaluated constructs. The marker variable was not found to be significantly related to any of the other variables, while the fit of the model and the significance and the estimates associated with the structural paths remained practically unchanged, providing further support for the lack of common method variance.

	CR	α	AVE	MSV	ASV	ORCOM	TSEV	REFF	CONT	SEFF	NORM	BINT	PVUL	SSEV	SPROB	CBA	PBC	ATT
ORCOM	0.771	0.705	0.531	0.518	0.210	0.729												
TSEV	0.916	0.904	0.738	0.213	0.098	0.326	0.859											
REFF	0.898	0.888	0.756	0.358	0.168	0.480	0.383	0.870										
CONT	0.893	0.888	0.805	0.303	0.165	0.457	0.461	0.550	0.897									
SEFF	0.972	0.972	0.890	0.624	0.180	0.352	0.281	0.317	0.520	0.943								
NORM	0.848	0.824	0.582	0.462	0.185	0.680	0.246	0.421	0.315	0.408	0.763							
BINT	0.983	0.982	0.940	0.518	0.211	0.720	0.399	0.362	0.504	0.476	0.656	0.970						
PVUL	0.908	0.897	0.827	0.110	0.015	0.046	0.332	0.004	0.063	0.077	0.012	0.120	0.909					
SSEV	0.771	0.769	0.532	0.423	0.124	0.355	0.326	0.581	0.237	0.211	0.394	0.287	0.051	0.729				
SPROB	0.704	0.675	0.615	0.423	0.109	0.363	0.250	0.598	0.171	0.131	0.343	0.308	0.025	0.650	0.784			
CBA	0.868	0.866	0.641	0.088	0.040	0.296	0.018	0.201	0.284	0.202	0.225	0.149	-0.170	-0.123	-0.014	0.800		
PBC	0.855	0.857	0.703	0.624	0.184	0.437	0.231	0.286	0.505	0.790	0.433	0.473	0.107	0.302	0.163	0.276	0.839	
ATT	0.955	0.955	0.857	0.456	0.199	0.571	0.272	0.324	0.461	0.675	0.562	0.614	0.054	0.214	0.225	0.188	0.619	0.926

CR = Composite Reliability	ORCOM = Organizational Commitment	PVUL = Perceived Vulnerability
α = Cronbach's alpha	TSEV = Perceived Threat Severity	SSEV = Perceived Sanction Severity
AVE = Average Variance Extracted	REFF = Perceived Response Efficacy	SPROB = Perceived Probability of Sanction Imposition
MSV = Maximum Shared Squared Variance	CONT = Perceived Controllability	CBA = Cost-Benefit Analysis
ASV = Average Shared Squared Variance	SEFF = Self-efficacy	PBC = Perceived Behavioral Control
BINT = Behavioral Intent	NORM = Perceived Subjective Norms	ATT = Attitude

Table 5: Validity Table with Factor Correlation Matrix for the General ISP Compliance Context

	CR	α	AVE	MSV	ASV	ORCOM	TSEV	REFF	CONT	SEFF	NORM	BINT	PVUL	SSEV	SPROB	CBA	PBC	ATT
ORCOM	0.767	0.705	0.535	0.316	0.152	0.731												
TSEV	0.917	0.907	0.735	0.142	0.072	0.245	0.857											
REFF	0.903	0.897	0.748	0.225	0.113	0.474	0.289	0.865										
CONT	0.892	0.888	0.807	0.317	0.122	0.452	0.377	0.429	0.898									
SEFF	0.960	0.960	0.920	0.870	0.176	0.338	0.229	0.298	0.465	0.959								
NORM	0.804	0.780	0.656	0.429	0.132	0.505	0.135	0.342	0.138	0.316	0.810							
BINT	0.979	0.979	0.949	0.429	0.161	0.495	0.312	0.204	0.294	0.537	0.655	0.974						
PVUL	0.934	0.931	0.770	0.058	0.014	0.055	0.241	-0.003	0.025	0.046	0.042	0.164	0.878					
SSEV	0.773	0.773	0.531	0.368	0.107	0.322	0.301	0.472	0.255	0.248	0.350	0.271	-0.030	0.729				
SPROB	0.760	0.751	0.537	0.368	0.075	0.155	0.247	0.399	0.214	0.262	0.140	0.203	0.020	0.607	0.733			
CBA	0.842	0.842	0.687	0.077	0.039	0.234	0.014	0.193	0.207	0.162	0.274	0.187	-0.213	-0.113	-0.053	0.829		
PBC	0.877	0.818	0.664	0.770	0.200	0.470	0.275	0.321	0.563	0.933	0.311	0.485	0.089	0.260	0.258	0.237	0.815	
ATT	0.947	0.947	0.876	0.336	0.173	0.562	0.345	0.314	0.371	0.472	0.573	0.580	0.124	0.309	0.213	0.278	0.529	0.936

CR = Composite Reliability	ORCOM = Organizational Commitment	PVUL = Perceived Vulnerability
α = Cronbach's alpha	TSEV = Perceived Threat Severity	SSEV = Perceived Sanction Severity
AVE = Average Variance Extracted	REFF = Perceived Response Efficacy	SPROB = Perceived Probability of Sanction Imposition
MSV = Maximum Shared Squared Variance	CONT = Perceived Controllability	CBA = Cost-Benefit Analysis
ASV = Average Shared Squared Variance	SEFF = Self-efficacy	PBC = Perceived Behavioral Control
BINT = Behavioral Intent	NORM = Perceived Subjective Norms	ATT = Attitude

Table 6: Validity Table with Factor Correlation Matrix for the Removable Flash Media Threat Context

	CR	α	AVE	MSV	ASV	ORCOM	TSEV	REFF	CONT	SEFF	NORM	BINT	PVUL	SSEV	SPROB	CBA	PBC	ATT
ORCOM	0.768	0.705	0.531	0.321	0.139	0.728												
TSEV	0.919	0.911	0.742	0.135	0.055	0.261	0.862											
REFF	0.929	0.926	0.813	0.531	0.131	0.346	0.225	0.902										
CONT	0.889	0.888	0.800	0.272	0.107	0.458	0.367	0.260	0.895									
SEFF	0.964	0.963	0.900	0.704	0.146	0.280	0.164	0.137	0.435	0.948								
NORM	0.850	0.826	0.658	0.551	0.146	0.500	0.099	0.455	0.193	0.342	0.811							
BINT	0.943	0.939	0.847	0.551	0.165	0.567	0.213	0.328	0.337	0.502	0.742	0.920						
PVUL	0.923	0.920	0.801	0.117	0.017	0.033	0.342	-0.115	0.087	0.086	-0.069	0.064	0.895					
SSEV	0.842	0.842	0.639	0.561	0.149	0.291	0.286	0.729	0.171	0.132	0.451	0.378	-0.068	0.800				
SPROB	0.816	0.813	0.689	0.561	0.120	0.299	0.165	0.614	0.099	0.101	0.358	0.359	-0.036	0.749	0.830			
CBA	0.845	0.842	0.646	0.104	0.038	0.163	-0.018	0.082	0.285	0.288	0.190	0.157	-0.077	-0.122	-0.179	0.804		
PBC	0.863	0.859	0.678	0.704	0.162	0.380	0.184	0.165	0.522	0.839	0.299	0.384	0.174	0.194	0.156	0.323	0.823	
ATT	0.878	0.874	0.707	0.324	0.126	0.519	0.254	0.222	0.361	0.492	0.339	0.378	0.036	0.291	0.216	0.197	0.569	0.841

CR = Composite Reliability	ORCOM = Organizational Commitment	PVUL = Perceived Vulnerability
α = Cronbach's alpha	TSEV = Perceived Threat Severity	SSEV = Perceived Sanction Severity
AVE = Average Variance Extracted	REFF = Perceived Response Efficacy	SPROB = Perceived Probability of Sanction Imposition
MSV = Maximum Shared Squared Variance	CONT = Perceived Controllability	CBA = Cost-Benefit Analysis
ASV = Average Shared Squared Variance	SEFF = Self-efficacy	PBC = Perceived Behavioral Control
BINT = Behavioral Intent	NORM = Perceived Subjective Norms	ATT = Attitude

Table 7: Validity Table with Factor Correlation Matrix for the Tailgating Threat Context

	CR	α	AVE	MSV	ASV	ORCOM	TSEV	REFF	SEFF	NORM	BINT	PVUL	SSEV	SPROB	CBA	ATT
ORCOM	0.770	0.705	0.535	0.295	0.124	0.731										
TSEV	0.909	0.892	0.719	0.171	0.079	0.313	0.848									
REFF	0.903	0.899	0.757	0.335	0.123	0.358	0.265	0.870								
SEFF	0.977	0.977	0.933	0.356	0.105	0.227	0.184	0.259	0.966							
NORM	0.834	0.804	0.629	0.437	0.154	0.543	0.273	0.327	0.421	0.793						
BINT	0.967	0.965	0.907	0.437	0.170	0.517	0.413	0.318	0.449	0.661	0.952					
PVUL	0.921	0.918	0.795	0.110	0.020	0.022	0.331	-0.210	0.098	0.077	0.157	0.892				
SSEV	0.817	0.816	0.598	0.408	0.119	0.284	0.268	0.579	0.180	0.303	0.194	-0.093	0.774			
SPROB	0.788	0.775	0.653	0.408	0.098	0.280	0.210	0.455	0.153	0.220	0.230	-0.013	0.639	0.808		
CBA	0.851	0.849	0.656	0.094	0.031	0.110	0.050	0.091	0.306	0.234	0.207	0.013	-0.181	-0.131	0.810	
ATT	0.937	0.932	0.831	0.367	0.171	0.477	0.343	0.397	0.597	0.498	0.606	-0.010	0.299	0.313	0.223	0.912

CR = Composite Reliability	ORCOM = Organizational Commitment	PVUL = Perceived Vulnerability
α = Cronbach's alpha	TSEV = Perceived Threat Severity	SSEV = Perceived Sanction Severity
AVE = Average Variance Extracted	REFF = Perceived Response Efficacy	CBA = Cost-Benefit Analysis
MSV = Maximum Shared Squared Variance	ATT = Attitude	NORM = Perceived Subjective Norms
ASV = Average Shared Squared Variance	SEFF = Self-efficacy	
BINT = Behavioral Intent	SPROB = Perceived Probability of Sanction Imposition	

Table 8: Validity Table with Factor Correlation Matrix for the Phishing Threat Context

CHAPTER 5. RESULTS, DISCUSSION, CONCLUSION

Results of SEM Analysis and Hypotheses Testing

Phase One (ISP TPB Analysis) Model

.

The structural model consisted of seven latent constructs and three single indicator control variables as described previously in the measurement model section for the General information security policy compliance, Tailgating, and Removable Flash Media threat contexts. The structural model consisted of five latent constructs for the Phishing threat context. Following the basic confirmatory factor analysis assumptions (Brown, 2006), all indicators were loaded only on one latent construct, all error terms associated with the latent constructs' indicators were uncorrelated, and every latent construct was scaled by fixing the direct effect of one of the three indicators to 1.0 and by setting the unstandardized residual coefficient for all indicators associated with latent constructs to 1.0.

The hypothesized structural model, as represented in Figures 6 and 7, provided good fit to the data as shown in Table 9. Overall, it is estimated that all predictors of Behavioral Intent explain 63% percent of its variance for General ISP compliance, 57% of its variance for Removable Flash Media, 65% of its variance for Tailgating, and 57% for the Phishing threat context.

Model	X^2/df	Bollen-Stine p	CFI	SRMR	Behavioral Intent Variance Explained
GIS	1.617	0.26	0.967	0.0501	0.63
Flash Media	2.241	0.06	0.943	0.0566	0.57
Tailgating	2.201	0.131	0.929	0.062	0.65
Phishing	2.755	0.029	0.947	0.0511	0.57

Table 9: Phase 1 (ISP TPB Analysis) Structural Model Fit Values

Figure 9 presents the results of the path analysis with standardized parameter estimates. Table 10 summarizes the direct effects of the antecedents on Behavioral Intent. Table 11 summarizes the hypotheses results for all four information security threat contexts.

Control variables.

Being female was associated with a significantly higher level of Behavioral Intent to comply with the ISP (standardized effect estimate = - 0.11, $p < 0.05$) while none of the other control variables had a significant effect on the model. It is important to note that females accounted for only 9 % of the sample population (21 out of 239). With females accounting for such a small portion of the overall sample population, caution should be taken in interpreting this result; ideally, a larger sample of female respondents should be analyzed to determine if gender does have a significant impact on Behavioral Intent in this specific organizational context.

Hypotheses testing.

This section summarizes the results of the Phase 1 path analyses for the four threat contexts. A detailed discussion of the results is presented in the discussion section. For

the General ISP Compliance context, Subjective Norms was positively related to Behavioral Intent (standardized effect estimate = .23, $p < .05$), providing support for hypothesis 1. Organizational Commitment was positively related to Behavioral Intent (standardized effect estimate = .46, $p < .0001$), providing support for hypothesis 2. Attitude was positively related to Behavioral Intent (standardized effect estimate = .16, $p < .05$), providing support for hypothesis 3. Perceived Behavioral Control was positively related to Behavioral Intent (standardized effect estimate = .12, $p < .05$), providing support for hypothesis 4. Self-efficacy was positively related to Perceived Behavioral Control (standardized effect estimate = .79, $p < .0001$), providing support for hypothesis 6. Finally, Perceived Controllability was not associated with Perceived Behavioral Control (hypothesis 5 is not supported).

For the Removable Flash Media threat context, Subjective Norms was positively related to Behavioral Intent (standardized effect estimate = .44, $p < .0001$), providing support for hypothesis 1. Organizational Commitment was positively related to Behavioral Intent (standardized effect estimate = .46, $p = .084$), providing support for hypothesis 2. Attitude was positively related to Behavioral Intent (standardized effect estimate = .14, $p < .05$), providing support for hypothesis 3. Perceived Behavioral Control was positively related to Behavioral Intent (standardized effect estimate = .28, $p < .0001$), providing support for hypothesis 4. Self-efficacy was positively related to Perceived Behavioral Control (standardized effect estimate = .94, $p < .0001$), providing support for hypothesis 6. Finally, Perceived Controllability was not associated with Perceived Behavioral Control (hypothesis 5 is not supported).

For the Tailgating threat context, Subjective Norms was positively related to Behavioral Intent (standardized effect estimate = .60, $p < .0001$), providing support for hypothesis 1. Organizational Commitment was positively related to Behavioral Intent (standardized effect estimate = .24, $p < .001$), providing support for hypothesis 2. However, Attitude was not associated with Behavioral Intent (hypothesis 3 is not supported). Perceived Behavioral Control was positively related to Behavioral Intent (standardized effect estimate = .19, $p < .0001$), providing support for hypothesis 4. Self-efficacy was positively related to Perceived Behavioral Control (standardized effect estimate = .85, $p < .0001$), providing support for hypothesis 6. Finally, Perceived Controllability was not associated with Perceived Behavioral Control (hypothesis 5 is not supported).

Finally, for the Phishing threat context, Subjective Norms was positively related to Behavioral Intent (standardized effect estimate = .39, $p < .0001$), providing support for hypothesis 1. Organizational Commitment was positively related to Behavioral Intent (standardized effect estimate = .18, $p < .05$), providing support for hypothesis 2. Attitude was positively related to Behavioral Intent (standardized effect estimate = .27, $p < .0001$), providing support for hypothesis 3. However, Self-efficacy was not associated with Behavioral Intent (hypothesis 7 is not supported).

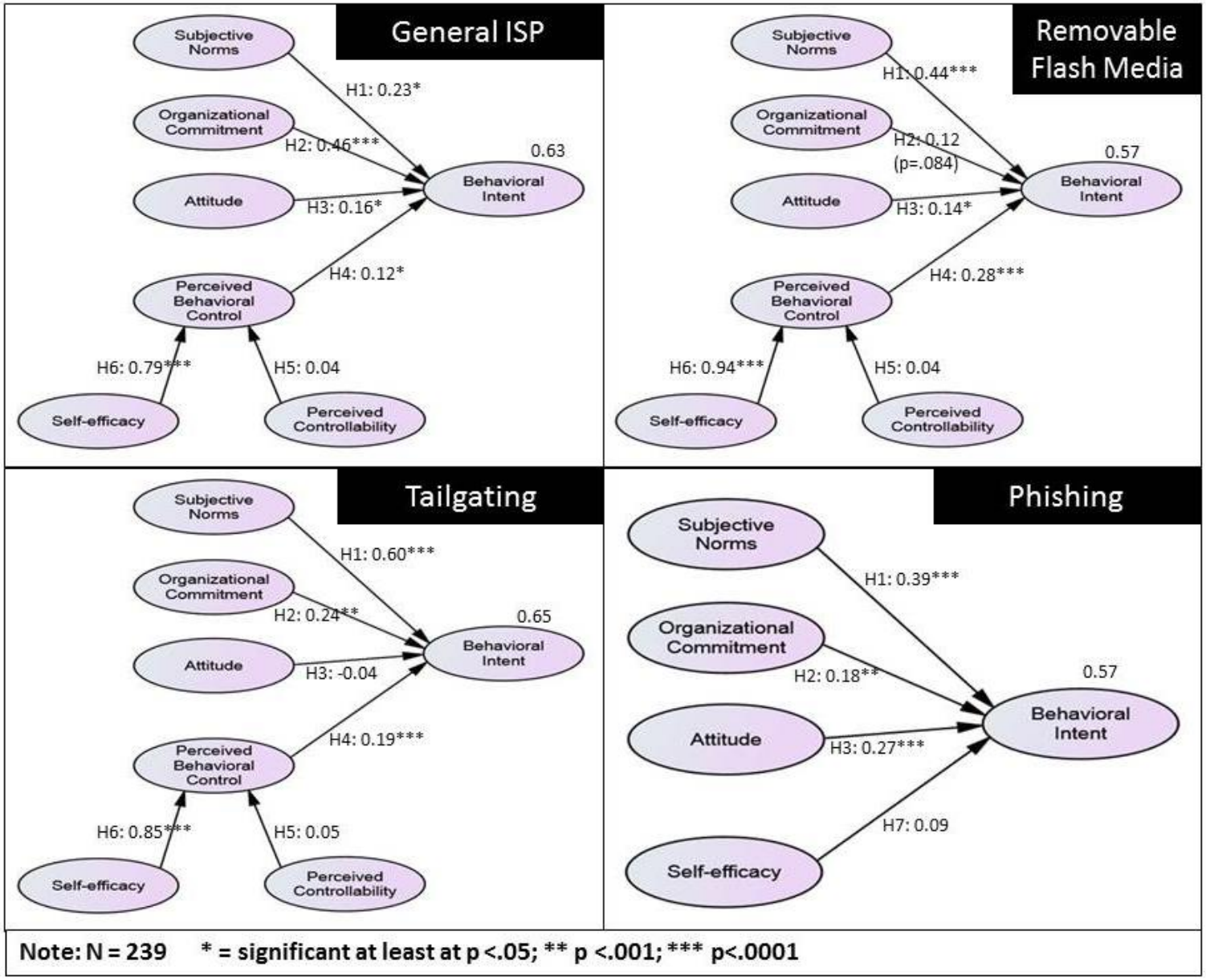

Figure 9: Results of the Phase 1 (ISP TPB Analysis) Structural Equation Modeling Analysis with Standardized Parameter Estimates

		General ISP			Removal Flash Media			Tailgating			Phishing		
Model Paths	**Hypoth #**	**Std. Est.**	**UnStd. Est.**	**Std Error**	**Std. Est.**	**UnStd. Est.**	**Std Error**	**Std. Est.**	**UnStd. Est.**	**Std Error**	**Std. Est.**	**UnStd. Est.**	**Std Error**
Subjective Norms → Behavioral Intent	H1	0.23*	0.18*	0.04	0.44***	0.30***	0.04	0.60***	0.42***	0.05	0.39***	0.26***	0.05
Organizational Committment → Behavioral Intent	H2	0.46***	0.34***	0.07	0.12 (p=.084)	0.09 (p=.084)	0.05	0.24**	0.21**	0.06	0.18*	0.11*	0.05
Attitude → Behavioral Intent	H3	0.16*	0.17*	0.07	0.14*	0.12*	0.06	-0.04	-0.04	0.07	0.27***	0.21***	0.05
Perceived Behavioral Control → Behavioral Intent	H4	0.12*	0.09*	0.04	0.28***	0.26***	0.05	0.19***	0.17***	0.05			
Perceived Controllability → Perceived Behavioral Control	H5	0.04	0.04	0.05	0.05	0.04	0.04	0.05	0.05	0.05			
Self-efficacy → Perceived Behavioral Control	H6	0.79***	0.91***	0.07	0.94***	1.03	0.06	0.09***	0.98***	0.07			
Self-efficacy → Behavioral Intent	H7										0.10	0.06	0.04
Gender → Behavioral Intent		-0.11*	-0.17*	0.07	-0.11*	-0.22*	0.09	-0.08*	-0.18*	0.10	-0.10*	-0.18*	0.07
Note 1: N = 239 * = significant at least at p <.05; ** p <.001; *** p<.0001													
Note 2: Only statistically significant control variables and paths shown above													
Note 3: H4 - H6 are not tested for the Phishing threat context and H7 is only tested in the Phishing threat context due to the ISP's actions requiring personal action from employees only (ISP-related Phishing requirements do not require employees to enforce actions on others).													

Table 10: Phase 1 (ISP TPB Analysis) Standardized Direct Effects, Standard Errors, and p-values.

		Hypothesis Suppored?			
Model Paths	**Hypothesis #**	**General ISP**	**Removable Flash Media**	**Tailgating**	**Phishing**
Subjective Norms → Behavioral Intent	H1	YES	YES	YES	YES
Organizational Committment → Behavioral Intent	H2	YES	YES	YES	YES
Attitude → Behavioral Intent	H3	YES	YES	**NO**	YES
Perceived Behavioral Control → Behavioral Intent	H4	YES	YES	YES	
Perceived Controllability → Perceived Behavioral Control	H5	**NO**	**NO**	**NO**	
Self-efficacy → Perceived Behavioral Control	H6	YES	YES	YES	
Self-efficacy → Behavioral Intent	H7				**NO**
Note: H4 - H6 are not tested for the Phishing threat context and H7 is only tested in the Phishing threat context due to the ISP's actions requiring personal action from employees only (ISP-related Phishing requirements do not require employees to enforce actions on others).					

Table 11:Phase 1 (ISP TPB Analysis) Hypotheses Testing Result Summary

Phase Two (Attitudinal Decomposition) Model

.

The structural model consisted of seven latent constructs and three single indicator control variables as described previously in the measurement model section for the General ISP, Tailgating, and Removable Flash Media threat contexts. Following the basic CFA assumptions (Brown, 2006), all indicators were loaded only on one latent construct, all error terms associated with the latent constructs' indicators were uncorrelated, and every latent construct was scaled by fixing the direct effect of one of the three indicators to 1.0 and by setting the unstandardized residual coefficient for all indicators associated with latent constructs to 1.0.

The hypothesized structural model, as represented in Figure 8, provided good fit to the data as shown in Table 12. Overall, it is estimated that all predictors of Attitude explain 15% percent of its variance for General ISP compliance, 29% of its variance for Removable Flash Media, 17% of its variance for Tailgating, and 28% for the Phishing threat context.

Model	X^2/df	Bollen-Stine p	CFI	SRMR	Attitude Variance Explained
GIS	1.571	0.045	0.966	0.0457	0.154
Flash Media	1.688	0.029	0.959	0.0474	0.286
Tail-gating	1.731	0.01	0.957	0.0475	0.174
Phishing	1.522	0.057	0.967	0.0462	0.276

Table 12:Phase 2 (Attitudinal Decomposition) Structural Model Fit Values

Figure 10 presents the results of the path analysis with standardized parameter estimates. Table 13 summarizes the direct and indirect effects. Table 14 summarizes the hypotheses results for all four information security threat contexts.

Control variables.

The three control variables (gender, whether the online survey respondents used a DoD PC, and job type / community) were applied to the two endogenous variables in the model, Attitude and Cost-Benefit Analysis. None of the control variables had a significant effect on the model.

Hypotheses testing.

This section summarizes the results of the Phase 2 path analyses for the four threat contexts. A detailed discussion of the results is presented in the discussion section. For the General ISP Compliance context, neither Sanction Severity nor Probability of Sanction Imposition was associated with Attitude (hypotheses 8 and 9 were not supported). Threat Severity was positively related to Attitude (standardized effect estimate = .19, $p < .05$), providing support for hypothesis 10. Neither Perceived Vulnerability nor Response Efficacy (see below discussion on mediation) was associated with Attitude (hypotheses 11 and 12 were not supported). Cost-Benefit Analysis was positively related to Attitude (standardized effect estimate = .16, $p < .05$), providing support for hypothesis 13. Sanction Severity was positively related to Cost-Benefit Analysis (standardized effect estimate = .33, $p < .05$), providing support for hypothesis 14. Neither Probability of Sanction nor Threat Severity was associated with Cost-Benefit Analysis (hypotheses 15 and 16 were not supported). Perceived Vulnerability was positively associated with Cost-Benefit Analysis (standardized effect estimate = .15, $p < .05$), providing support for hypothesis 17. Response efficacy was positively related to

Cost-Benefit Analysis (standardized effect estimate = .38, $p < .0001$), providing support for hypothesis 18; see below section on mediation effects for more.

For the Removable Flash Media threat context, Sanction Severity was positively related to Attitude (standardized effect estimate = .25, $p < .05$), providing support for hypothesis 8. Probability of Sanction Imposition was not associated with Attitude (hypothesis 9 was not supported). Threat Severity was positively related to Attitude (standardized effect estimate = .21, $p < .05$), providing support for hypothesis 10. Perceived Vulnerability was positively related to Attitude (standardized effect estimate = .15, $p < .05$), providing support for hypothesis 11. Response Efficacy was not associated with Attitude (hypotheses 12 was not supported; see mediation discussion below). Cost-Benefit Analysis was positively related to Attitude (standardized effect estimate = .31, $p < .0001$), providing support for hypothesis 13. Sanction Severity was positively related to Cost-Benefit Analysis (standardized effect estimate = .29, $p < .05$), providing support for hypothesis 14. Probability of Sanction and Threat Severity were not associated with Cost-Benefit Analysis (hypotheses 15 and 16 were not supported). Perceived Vulnerability was positively related to Cost-Benefit Analysis (standardized effect estimate = .20, $p < .05$), providing support for hypothesis 17. Response Efficacy was positively related to Cost-Benefit Analysis (standardized effect estimate = .28, $p < .0001$), providing support for hypothesis 18.

For the Tailgating threat context, Sanction Severity was positively related to Attitude (standardized effect estimate = .27, $p = .088$), providing support for hypothesis 8. Probability of Sanction Imposition was not associated with Attitude (hypothesis 9 was not supported). Threat Severity was positively related to Attitude (standardized effect

estimate = .19, $p < .05$), providing support for hypothesis 10. Neither Perceived Vulnerability nor Response Efficacy was associated with Attitude (hypotheses 11 and 12 were not supported). Cost-Benefit Analysis was positively related to Attitude (standardized effect estimate = .25, $p < .05$), providing support for hypothesis 13. Sanction Severity, Probability of Sanction, Threat Severity, and Perceived Vulnerability were not associated with Cost-Benefit Analysis (hypotheses 14, 15, 16, and 17 were not supported). Response Efficacy was positively related to Cost-Benefit Analysis (standardized effect estimate = .38, $p < .0001$), providing support for hypothesis 18.

Finally, for the Phishing threat context, neither Sanction Severity nor Probability of Sanction Imposition was associated with Attitude (hypotheses 8 and 9 were not supported). Threat Severity was positively related to Attitude (standardized effect estimate = .23, $p < .05$), providing support for hypothesis 10. Perceived Vulnerability was not associated with Attitude (hypotheses 11 was not supported). Response Efficacy was positively related to Attitude (standardized effect estimate = .19, $p < .05$), providing support for hypothesis 18. Sanction Severity was positively related to Cost-Benefit Analysis (standardized effect estimate = .31, $p < .05$), providing support for hypothesis 14. Probability of Sanction, Threat Severity, and Perceived Vulnerability were not associated with Cost-Benefit Analysis (hypotheses 15, 16, and 17 were not supported). Response Efficacy was positively related to Cost-Benefit Analysis (standardized effect estimate = .19, $p < .05$), providing support for hypothesis 18.

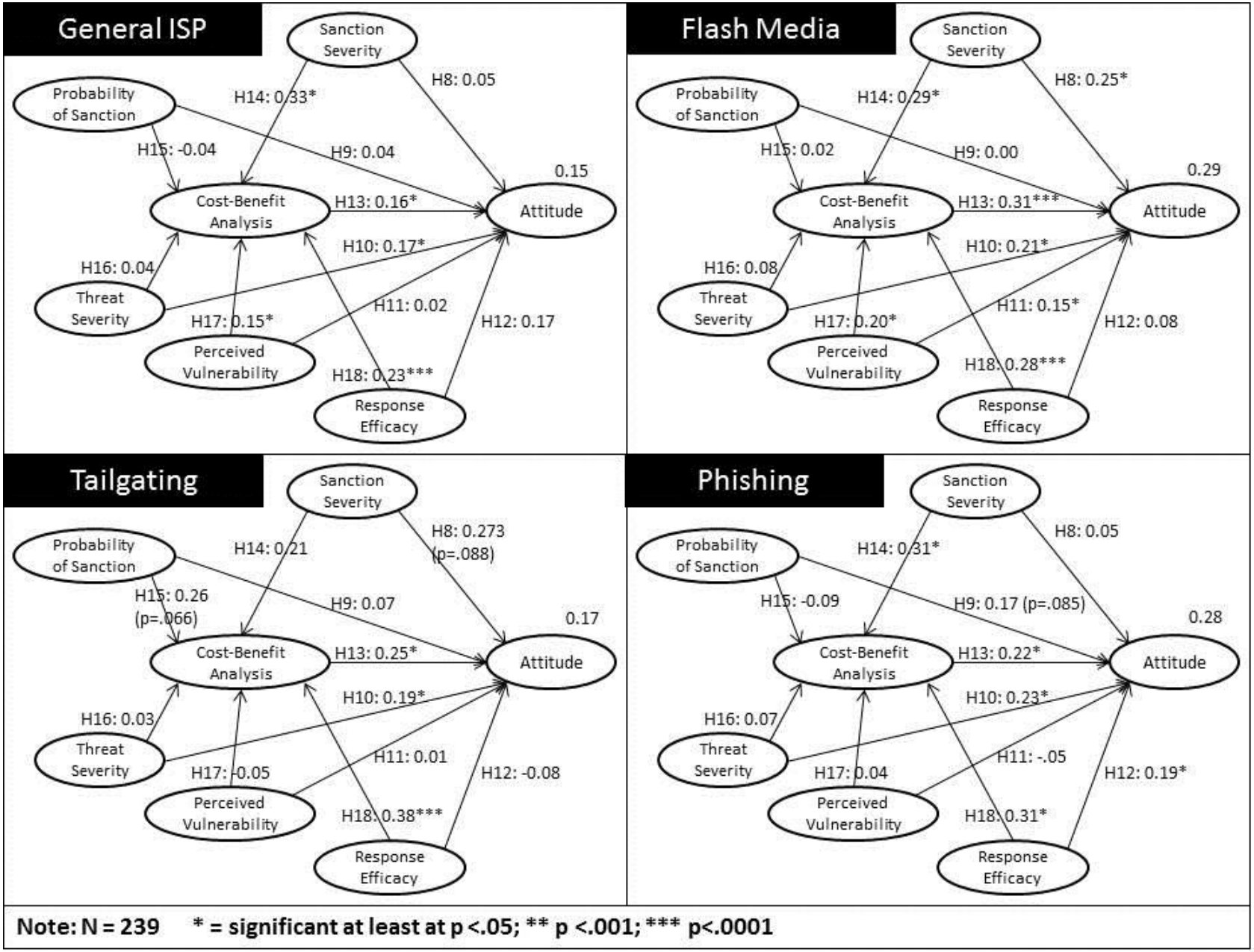

Figure 10: Results of the Phase 2 (Attitudinal Decomposition) Structural Equation Modeling Analysis with Standardized Parameter Estimates

Model Paths	Hypoth #	General ISP			Removal Flash Media			Tailgating			Phishing		
		Std. Est.	UnStd. Est.	Std Error	Std. Est.	UnStd. Est.	Std Error	Std. Est.	UnStd. Est.	Std Error	Std. Est.	UnStd. Est.	Std Error
Direct Paths													
Perceived Sanction Severity → Attitude	H8	0.05	0.02	0.05	0.25*	0.14*	0.06	0.27 (p=.088)	0.11 (p=.088)	0.07	0.05	0.02	0.04
Perceived Probability of Sanction Imposition → Attitude	H9	0.04	0.01	0.04	0.00	0.00	0.06	0.07	0.03	0.05	0.17 (p=.085)	0.07 (p=.085)	0.04
Cost-Benefit Analysis → Attitude	H10	0.16*	0.05*	0.02	0.31***	0.12***	0.03	0.25*	0.1*	0.03	0.22**	0.08**	0.02
Perceived Threat Severity → Attitude	H11	0.17*	0.08*	0.04	0.21*	0.14*	0.04	0.19*	0.09*	0.04	0.25***	0.14***	0.04
Perceived Vulnerability → Attitude	H12	0.02	0.01	0.02	0.15*	0.07*	0.03	0.01	0.00	0.03	0.05	0.02	0.02
Perceived Response Efficacy → Attitude	H13	0.17	0.11	0.07	0.08	0.08	0.08	0.08	0.05	0.06	0.19*	0.12*	0.06
Perceived Sanction Severity → Cost-Benefit Analysis	H14	0.33*	0.45*	0.17	0.29*	0.45*	0.02	0.22	0.23	0.18	0.31*	0.36*	0.15
Perceived Probability of Sanction Imposition → Cost-Benefit Analysis	H15	0.04	0.05	0.15	0.02	0.03	0.18	0.26 (p=.066)	0.27 (p=.066)	0.15	0.09	0.10	0.13
Perceived Threat Severity → Cost-Benefit Analysis	H16	0.04	0.06	0.13	0.08	0.14	0.13	0.03	0.04	0.10	0.07	0.12	0.14
Perceived Vulnerability → Cost-Benefit Analysis	H17	0.15*	0.14*	0.07	0.20*	0.23*	0.08	0.05	0.05	0.07	0.04	0.04	0.08
Perceived Response Efficacy → Cost-Benefit Analysis	H18	0.4***	0.83***	0.23	0.28***	0.77***	0.23	0.38*	0.56*	0.17	0.31*	0.57*	0.18
Indirect Paths													
Perceived Sanction Severity → Cost-Benefit Analysis → Attitude	H19	0.05	0.02	0.02	0.09	0.05	0.03	0.05	0.02	0.03	0.07	0.03	0.02
Perceived Probability of Sanction Imposition → Cost-Benefit Analysis → Attitude	H20	-0.01	-0.01	0.01	0.01	0.01	0.03	0.06	0.03	0.02	0.02	0.01	0.01
Perceived Threat Severity → Cost-Benefit Analysis → Attitude	H21	0.01	0.00	0.01	0.02	0.02	0.02	0.01	0.01	0.01	0.02	0.01	0.01
Perceived Vulnerability → Cost-Benefit Analysis → Attitude	H22	0.02	0.01	0.01	0.06	0.03	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Perceived Response Efficacy → Cost-Benefit Analysis → Attitude	H23	0.06*	0.04*	0.03	0.09*	0.09*	0.04	0.10	0.05	0.03	0.07	0.04	0.02

Note 1: N = 239 * = significant at least at p <.05; ** p <.001; *** p<.0001

Table 13: Phase 2 (Attitudinal Decomposition) Standardized Direct and Indirect Effects, Standard Errors, and p-values.

Model Paths	Hypoth	Hypothesis Suppored?			
		General ISP	Removable Flash Media	Tailgating	Phishing
Direct Paths					
Perceived Sanction Severity → Attitude	H8	**NO**	YES	YES	**NO**
Perceived Probability of Sanction Imposition → Attitude	H9	**NO**	**NO**	**NO**	YES
Cost-Benefit Analysis → Attitude	H10	YES	YES	YES	YES
Perceived Threat Severity → Attitude	H11	YES	YES	YES	YES
Perceived Vulnerability → Attitude	H12	**NO**	YES	**NO**	**NO**
Perceived Response Efficacy → Attitude	H13	**MEDIATED**	**MEDIATED**	**NO**	YES
Perceived Sanction Severity → Cost-Benefit Analysis	H14	YES	YES	**NO**	YES
Perceived Probability of Sanction Imposition → Cost-Benefit Analysis	H15	**NO**	**NO**	YES	**NO**
Perceived Threat Severity → Cost-Benefit Analysis	H16	**NO**	**NO**	**NO**	**NO**
Perceived Vulnerability → Cost-Benefit Analysis	H17	**NO**	**NO**	**NO**	**NO**
Perceived Response Efficacy → Cost-Benefit Analysis	H18	YES	YES	YES	YES
Indirect Paths					
Perceived Sanction Severity → Cost-Benefit Analysis → Attitude	H19	**NO**	**NO**	**NO**	**NO**
Perceived Probability of Sanction Imposition → Cost-Benefit Analysis → Attitude	H20	**NO**	**NO**	**NO**	**NO**
Perceived Threat Severity → Cost-Benefit Analysis → Attitude	H21	**NO**	**NO**	**NO**	**NO**
Perceived Vulnerability → Cost-Benefit Analysis → Attitude	H22	**NO**	**NO**	**NO**	**NO**
Perceived Response Efficacy → Cost-Benefit Analysis → Attitude	H23	**FULL MEDIATION**	**FULL MEDIATION**	**NO**	**NO**

Table 14: Phase 2 (Attitudinal Decomposition) Hypotheses Testing Result Summary

The results of the mediation analysis indicate that the effect of Response Efficacy on Attitude is fully mediated by Cost-Benefit Analysis for the General ISP Compliance (standardized indirect effect estimate = 0.06, $p < 0.0001$) and the Removable Flash Media (standardized indirect effect estimate = 0.09, $p < 0.0001$) threat contexts, supporting hypothesis 23 for these threat contexts. However, there was no mediation effects present for any of the other variables in the model (hypotheses 19-22 for all threat contexts and hypothesis 23 for the Tailgating and Phishing threat contexts are not supported).

Discussion

In a perfect world, there would be no need for organizational information security policies, as there would be no threats to the information resources of an organization. Unfortunately, information security threats do exist and pose a tangible and significant challenge to modern organizations of all types. It is important to understand the behavioral factors that affect an employee's intent to comply with the (hopefully) well-thought procedural protections offered in the ISP. A comprehensive reading of the literature on recent research in the area of ISP behavioral compliance has identified a number of theoretically grounded and empirically validated factors expected to influence behavioral intent to comply with ISPs. The major goal of this research study was to explore the relative importance of specific behavioral antecedents, identified in the composite theoretical framework, of an employee's stated behavioral intent to comply with organizational information security policies for a specific organization (the DoD) with an established and robust ISP (Research Question #1). Additionally, this study aimed to explore how behavioral intent to comply with the ISP varies for employees when presented with the overall guidance of the ISP and specific guidance for several

threats that exist across organizations (phishing, tailgating, and the use of removable flash media) (Research Question #2). Lastly, this study explored the impact of an employee's perceived ability to follow the ISP when they are required to enforce (via monitoring and/or interaction) ISP requirements on other employees (Research Question #3).

The results of this study's structural equation modeling analysis indicate strong support for the composite ISP behavioral compliance theoretical framework in the organizational context explored. However, the results indicated that not all of the relationships predicted by the composite framework (and associated structural models) exist under the different threat conditions. Findings of insignificant relationships by threat context (for the same sample population), however, can provide significant insights for future theoretical exploration and, most clearly, in practical application of the results. Lastly, the results of the study showed that an employee's perceived ability to enforce specific ISP requirements on coworkers did not have a significant relationship to their intent to follow through on required ISP actions. This last result offers interesting questions and opportunities for both practice and future research. Each of the antecedents and their relationships, for both phases of the composite framework evaluation, is discussed below.

Phase One (ISP TPB Analysis)

According to the extent literature on information security polciy compliance, an employee's intent to follow the guidance of the ISP depends on a number of important factors. The expectation is, in line with the theory of planned behavior, a strong intent to comply with the ISP will generally result in actual compliance. Theoretically, an employee would feel a very strong intent to follow through on the required ISP actions

(to protect organizational information resources) if they felt their referent coworker groups expected them to follow the ISP requirements, if they were strongly committed to their organization, had favorable attitudes towards all the actions called for in the ISP, and felt capable of performing the ISP actions in the light of their personal confidence in following the rules and any facilitating or limiting factors associated with those ISP actions.

The findings of this study (as depicted in Figure 7 and Table 11) suggest that the DoD employees surveyed generally have a very strong intent to comply with the information security policy (ISP) guidelines evaluated (General ISP, Tailgating, Phishing, and Removable Flash Media). In all threat contexts, the perceived expectations of referent coworker groups had a strong impact on intent to comply with the ISP. Likewise, participants' strong organizational commitment to the DoD strengthed their intent to comply with the ISP. In all cases except for the Tailgating threat, employee favorable attitudes towards taking directed ISP actions was related to a greater intent to comply with the ISP. And, with the exception of the Phishing threat context, DoD employee perceptions of their abilities to comply with the ISP were positively related to greater intention to comply with ISP actions. However, in all threat contexts explored, reported employee confidence in their ability to enfore ISP actions on coworkers was not significantly related to an employee's intent to comply with the ISP.

Subjective Norms. As predicted, Subjective Norms had a positive relationship to Behavioral Intent. In fact, it had the strongest relationship with Behavioral Intent for all of the specific threat contexts than all other antecedents. The DoD employees participating in this study are clearly and strongly affected by their expectations of what

referent coworker groups expect them to do with regards to ISP compliance. While in this case subjective norms have a strong and positive influence on ISP behavioral intent, it should be cautioned that such a strong reliance upon Subjective Norms could have deleterious effects in different circumstances. For example, this study showed a significant impact of Subjective Norms on employee intent to comply with Tailgating requirements; employees stated that they strongly believed that their coworkers expected them to follow the guidance on Tailgating, and this was shown to be statistically related to a positive intent to follow the rules. If this relationship holds true under certain circumstances where employee's believe that coworkers really don't expect them to follow the Tailgating rules, behavioral intent to comply with the ISP would suffer.

Organizational Commitment. This study provides credence to the Herath & Rao (2009a) and Guo et al. (2009) findings that Organizational Commitment is a significant contributer to employee Behavioral Intent to comply with ISPs. In the present study, Organizational Commitment was positively associated with Behavioral Intent in all four threat contexts explored. Organizational Commitment was the only construct in the Phase 1 (ISP TPB Analysis) model that was only measured once and applied consistently to all threat contexts. Effectively acting as an anchor construct in the model analysis, the fact that Organizational Commitment varied in importance for different threats is notable. For example, in the General ISP compliance context, Organizational Commitment was the dominant factor affecting Behavioral Intent. However, in the light of the high-profile Removable Flash Media threat context, Organizational Commitment was reduced to the least powerful of the relevant factors affecting Behavioral Intent.

Attitude. Attitude, an important antecedent of Behavioral Intent identified in related ISP compliance research, had a positive relationship to Behavioral Intent for all threat conditions except Tailgating. There are several possible explanations for why Attitude fails to positively impact Behavioral Intent in the face of the Tailgating threat. First, as posited by Herath & Rao (2009a), it is possible that Attitude may be desensitized when other important variables come into play (norms, efficacy, commitment). In the Tailgating threat context, Subjective Norms has a very strong positive impact on Behavioral Intent. It is possible that, in the case of Tailgating, an employee may perceive such significant pressure from their coworkers to follow the ISP rules that their attitudes are not as relevant in determining their intent to comply. Another possible explanation is that employee attitudes towards Tailgating are significantly impacted by the organizational sub-context in which they work, something that was not measured for this study. While all participants in this study were DoD employees, there are many (hundreds if not thousands) of sub-organizational contexts in the DoD. While Tailgating is considered an important security threat to all DoD organizations (hence its inclusion in the ISP), it may be considered more or less important depending on the specific sub-organizational context. For example, in a DoD workplace with limited access to classified information and perhaps a small numbers of employees, prevention of Tailgating may result in a considerbly less favorable attitude towards ISP-directed actions than in an organization that relies upon considerable access to classified information and technical systems. Additionally, it is altogether possible that the respondents in this survey have a generally less favorable attitude about following the Tailgating requirements. A paired-sample t-test comparison of Attitude for the General ISP and Tailgating threats shows

that participant attitudes towards taking Tailgating-related ISP actions (M= 6.52, SD= 0.61) is statistically signficantly lower than for General ISP compliances (M= 6.61, SD= 0.48), t(238)= 2.477, p = 0.01. If this is the case, it indicates that there is an opportunity for the DoD to strengthen their employee's attitude towards following the Tailgating ISP actions through attention to this matter via communication, education, inspections, etc.

Perceived Behavioral Control and Self-efficacy. For the three threat contexts where PBC and Self-efficacy were both measured (General ISP, Tailgating, Removable Flash Media), there was a positive relationship with intent to comply with the ISP. DoD respondents felt they were capable enough to follow the ISP for these threat contexts, which coincides with the results of related ISP compliance studies in other organizational contexts (Bulgurcu et al., 2010; Johnston & Warkentin, 2010; Workman et al., 2008; Ng et al., 2009). It should be noted, however, that PBC had a smaller effect on Behavioral Intent in the General ISP threat context. It is possible that the General ISP compliance threat is too general – it may be more difficult for respondents to ascertain their ability to fulfill ISP actions without having specifics on which actions to fulfill.

Self-efficacy. As discussed earlier, neither PBC nor Perceived Controllability were measured for the Phishing threat context because the ISP-directed actions for Phishing are focused directly on an employee's own actions; there is no implicit or explicit expectation that employees will enforce Phishing actions on other employees. As shown in Figure 9, the results of this study show that employee Self-efficacy was not directly related to employee intent to comply with the ISP for the Phishing context. A close look at the survey data showed that survey participants responded to Phishing with the highest Behavioral Intent scores of all threat categories (M = 6.73, SD= .46, n= 239) but lowest

overall Self-efficacy grades of all the threat categories (M= 6.49, SD= .66, n= 239). Unfortunately, this study did not collect any data to explore in more depth why employee Self-efficacy in the Phishing context was not a significant contributor to Behavioral Intent. However, a discussion of these results with one of the DoD Information Assurance (IA) experts that participated in the earlier survey instrument review identified a possible explanation. In the opinion of the IA expert, the the actions for Phishing called for in the ISP are not as clear and decisive as they are for Tailgating and Removable Flash Media. The ISP Phishing actions require users to make judgement calls on emails and web links or pages that they may or may not feel comfortable making; the indicators of a good Phishing attempt are, by design, hard to identify. Indeed, following the ISP guidance for Phishing actually may extremely difficult for some DoD users. For example, the Navy guidance for prevention of Phishing requires users to ignore attachments and web links from emails that were not digitally signed. However, there are many DoD organizations that do not require their employees to digitally sign emais, and there are many challenges in educating and training personnel (DoD or not) how to properly digitally sign email. In either case, the failure of Self-efficacy to positively and significantly influence Behavioral Intent in the Phishing context identifies a potential area for further exploration and possible remedial action.

Perceived Controllability. As stated by Ajzen (2002), the construct of perceived behavioral control (PBC) was added to the theory of planned behavior in an attempt to deal with situations in which people may lack complete volitional control over the behavior of interest. The present study was the first one of its kind in the ISP Compliance literature to explore the potential impact of an employee's feelings of their ability to

enforce ISP actions on coworkers in the form Perceived Controllability. The results of this study show that in no threat context examined was Perceived Controllability significantly related to Perceived Behavioral Control, and through it Behavioral Intent. It should be noted that structural models were tested to evaluate the impact of Percevied Controllability directly to Behavioral Intent with similar results – no significant relationship existed.

There are few conclusions one can draw from this study alone with regards to why Perceived Controllability is not a significant contributor to PBC. A close look at the item scores for Perceived Controllability show that the mean values of each are far lower than for PBC and Behavioral Intent (as shown in Table 15) and the standard deviations for all of the Perceived Controllability items are much larger than for PBC and Behavioral Intent. Interestingly, the mean score for all referent groups (executives, peers, and subordinates) are higher for Removable Flash Media than for General ISP compliance and Tailgating. This indicates that survey participants felt a greater perceived controllability while enforcing the Removable Flash Media rules over the other threat contexts. Additionally, it comes as no surprise that in every threat context, participants felt they had more control over enforcing the ISP actions as they moved down the rank/status heirarchy from executives to subordinates.

It is possible that Perceived Controllability's lack of a significant relationship to PBC in this study signals a failure in the ability of theory of planned behavior (and thus the composite theoretical framework) to account for the potential impact of enforcing ISP requirements on coworkers. The results of this study highlight a potential area for future research and practical inspection in the DoD context.

Construct	General ISP Compliance		Removable Flash Media		Tailgating	
	Mean	Std Dev	Mean	Std Dev	Mean	Std Dev
Perceived Controllability						
Executives	6.038	0.997	6.167	0.897	5.766	1.268
Peers	6.201	0.805	6.293	0.793	5.971	1.094
Subordinates	6.264	0.790	6.335	0.776	6.059	0.910
Coworkers 1	6.188	0.806	6.188	0.806	6.188	0.806
Coworkers 2	6.251	0.791	6.251	0.791	6.251	0.791
Perceived Behavioral Control	6.370	0.652	6.478	0.657	6.423	0.725
Behavioral Intent	6.660	0.474	6.678	0.561	6.579	0.620

Table 15: Means and Standard Deviations for Perceived Controllability

Phase Two (Attitudinal Decomposition)

One of the purposes of the composite theoretical framework for ISP behavioral compliance was to capture the various factors of Attitude from previous research and apply them simultaneously and in context. Shown in Table 14, the findings of this phase of the study suggest that, for the DoD employees surveyed, Attitude towards an ISP behavior is affected by a range of factors depending on threat context. This threat-dependency may be an explanation for the much lower variances (as shown in Figure 10) explained for Attitude when compared to Behavioral Intent in Phase One of this study. For all threat contexts, an employee's positive Cost-Benefit Analysis of an ISP behavior was associated with a more favorable Attitude towards that behavior. Likewise, employees that assessed a higher Threat Severity for a specific threat context had a more favorable opinion of the ISP action associated with that threat. However, the remaining antecedents posited in the composite framework had relationships with Attitude and Cost-Benefit Analysis that were much more varied with threat (as shown in Table 14).

Sanction Severity and Perceived Probability of Sanction Imposition. Sanction Severity was found to have a significant impact on Attitude in the Removable Flash Media and Tailgating contexts; in these cases, the more severe the perceived sanction severity, the more favorable the employee's attitude toward complying wih that behavior. However, it was shown that while Sanction Severity did not have a significant impact on Attitude for General ISP compliance and Phishing threats, it did have a significant effect on Cost-Benefit Analysis for these threats. Thus, in each threat context examined, Sanction Severity did play some role in the development of an employee's Attitude towards an ISP behavior. In comparison, the perceived probability of sanction imposition only had a direct effect on Attitude in the Phishing threat context. It is possible that respondents, knowing that all DoD computers are subject to monitoring, felt that a failure to follow Phishing requirements of the ISP would result in eventual detection and punishment. The only case in which sanction probability had a possible significant effect on Cost-Benefit Analysis is the case of Tailgating (where $p = 0.066$); it appears that respondents included the possiblity of getting caught in their Cost-Benefit Analysis calculations even though this same probability had no direct effect on Attitude. The overall results for Sanction Severity and Probability of Sanction Imposition are in line with the results of the D'Arcy et al. (2008) study, which found that Sanction Severity had a much greater impact on behavioral intent while sanction probability did not. However, D'Arcy et al. (2008) did not examine the impact of sanction effects over the same threat contexts or in the case of General ISP compliance. These results are interesting because the DoD, as with many organizations studied in related research, appear to rely upon sanction effects as an effective tool to ensure employee compliance with the ISP. Given

the varied impacts of Sanction Severity and Probabiliy of Sanction in this study, a closer examination of the expected effectiveness of sanction effects is warranted.

Threat Severity. As predicted, Perceived Threat Severity had a positive relationship on an employee's Attitude about an ISP action for all threat conditions; the more severe the perceived threat, the more favorable an employee's attidue towards complying with the related ISP behavior. Similar results were seen, albeit under different organizational and threat contexts, in the Johnston & Warkentin (2010), Guo et al. (2011), and Workman et al. (2008) studies. However, Threat Severity did not have a significant impact on Cost-Benefit Analysis. One may conclude that the DoD's efforts to educate employees on the potential harm from the threat contexts examined has been effective and has contributed to a stronger intent to comply with ISP requirements.

Cost-Benefit Analysis and Perceived Response Efficacy. As predicted in the Workman et al. (2008), Bugurcu et al. (2010) studies, the rational choice-based Cost-Benefit Analysis had a positive relationship to Attitude. In this study, it was shown to have a signficant effect in all threat contexts; the more positive the analysis (the benefits of the action exceeded the costs), the more favorable the Attitude towards the respective ISP behavior. Additionally, it was shown that Cost-Benefit Analysis fully mediated the effects of Perceived Response Efficacy on Attitude in the General ISP and Removable Flash Media threat contexts. This means that the entire impact of an employee's assessment of the effectiveness of an ISP behavior was felt on Attitude through the Cost-Benefit Analysis variable. Meanwhile, Perceived Response Efficacy had no direct or indirect impact on Attitude for the Tailgating and Phishing contexts, but did have a direct and significant impact on the Cost-Benefit Analysis calculus for those threats. This last

set of relationships essentially states that, while employees generally believed that the ISP-directed actions for Tailgating and Phishing were indeed effective methods to combat the threat, how they viewed the behavior was part of an overall calculus of weighing costs and benefits versus a direct contributer of their attitude about the behavior.

Perceived Vulnerability. The only context in which Perceived Vulnerability was considered a significant contributor to Attitude was for the Removable Flash Media threat. As see in Figure 11, the highest variance explained for Attitude is for this threat context and it has the largest number of significant attitudinal antecedents of any other threat category. This phenomenon may be a result of the extreme nature of the DoD ban on removable flash media in 2008 and the significant reporting and discussion of the threats in the open media as well as within the DoD ISP training curriculums. Additionally, the only threat context in which Perceived Vulnerabilty was a significant contributor to Cost-Benefit Analysis is for the General ISP compliance category. An analysis of the data shows that in all threat contexts, there was a wide range of responses for Perceived Vulnerability (standard deviation for all threat contexts was > 1.50 on a 7 point scale); employees do not appear to have a consistent and strong feeling that they are vulnerable to the threats examined in this study. This identifies a possible area for improvement in ISP education for the DoD.

Theoretical Contributions

This study contributed to the emerging body of knowledge about the important domain of employee information security policy behavioral compliance. The composite theoretical framework captures theory-based and empirically validated factors of

behavioral intent from a diverse research base in a relatively parsimonious manner. Using the theory of planned behavior as the theoretical foundation for the framework, this study proposed and explored the impact of the various antecedents of behavioral intent in both threat and organizational context. Additionally, this study provided a robust evaluation of the decomposition of an employee's attitude towards specific ISP-related behaviors, identifying factors that vary considerably with threat context.

The majority of the ISP behavioral compliance literature that informed the composite theoretical framework was designed to maximize potential generalizability of results by exploring ISP compliance over multiple organizations simultaneously. These studies were not constructed to allow cross-organizational compliance analyses; responses were aggregated in a single structural model for evaluation. As with most behavioral research, there are numerous organizational contexts that can effect the antecedents of intent and actual ISP compliance behavior. By aggregating employee responses across organizations without a deep understanding of the relative importance of information security requirements facing the respondents, it is possible these studies sacrificed important insights into the organizational contexts that can effect the understanding of behavioral intent. Additionally, few of the related studies declared an awareness of the actual content of the respondents' overarching information security policies, or even if there were any ISPs in effect. Fundamental to ISP behavioral compliance research should be an understanding of the information security threats present and the actions required to designed to protect agains the threats. The present study focused on employees of an organization (the DoD) known for its appreciation of information security, a history of employee ISP compliance issues, an established record of expending significant

resources to attain acceptable levels of compliance, and a well-defined ISP. It is believed that the results of this study will provide a tangible organizational and ISP anchor point for comparison with future studies of both similar and dissimilar organizations.

Another similarity with much of the ISP compliance related research is the evalation of general compliance with information security actions. By evaluating "general" compliance, these studies tend to treat all security threats in the same manner with the same basic variables affecting intent to comply with the ISP. As shown in the description of the ISP for this study, the threat from and the actions required for the specific security threats are very different. The results of this study highlight, in this particular organization, that the antecedents of an employee's attitude about a behavior and their intent comply with the behavior can vary greatly depending on the threat context. Based upon the results of this study, one can question the validity of examining "general ISP compliance" in this or any other organization. Examination of ISP behavorial compliance should be focused on specific threat, not on the notion of a general set of threats that cover a possible myriad of information security risks that can and will vary depending on many factors related to the organization.

Finally, this study explored, for the first time in the ISP behavioral compliance literature, the potential impact of how an employee's perception of their ability to enforce required ISP actions on coworkers impacts their overall intent to comply with a specific ISP action. While this study did not show a significant effect for the Perceived Controllability construct as modeled, it highlighted the potential inability of the composite theoretical framework, built upon the theory of planned behavior, to address this real phenomena of interest. Additional research into ISP behavioral compliance is

needed to determine how, if it is possible, to incorporate such controllability aspects into a theoretical framework for understanding employee intent to comply with information security policies.

Implications for Practice.

This results of this study offer important practical implications for information security practitioners in the DoD and other organizations. First, it is necessary to explore employee intent to comply with specific ISP actions without assuming that the same factors exist and act the same way in all threat contexts. As shown in this study, the threat context has a significant impact on the strength and significance of specific behavioral antecedents. It is not only important to evaluate whether antecedent factors of intent to comply and attitude are significant as expected, but also when they are not significant. A lack of a significant relationship between an antecedent and attitude, for example, can identify a possible weakness in the organization's information security education and awareness platforms and a disconnect between the information security expectations of the organization and its employees.

This study identified that an employee's perception of their coworkers' expectation of them with regards to a specific ISP action as a strong factor affecting their intent to comply with the ISP. While this is a good finding in this study, the same relationship can have serious negative consequences if an employee feels that their coworkers don't really care if they follow the procedures. For example, in a hypothetical organization, if an employee feels that his or her coworkers don't care if they follow Tailgating procedures as long as violations don't impact their own work area, the employee may be less likely to follow the overall guidance of the ISP in this particular context. Care should be taken

to listen to employees to ascertain their thoughts on the organization's security subjective norms, vice what the ISP states the norms should reflect.

Results of this study showed that while employees intend to follow the ISP for Phishing threats, their feelings about their capability to properly perform the required actions are not related to that intent. Additional training or education on the ISP Phishing actions required may improve users's confidence in their ability to make judgement calls on emails and web links or pages that they encounter.

The analyses of the factors affecting an employee's attitude towards an ISP behavior identified several potentially problematic areas that organizations may want to investigate and address in future information security training and awareness programs. In particular, the relative insignificance of employee perceptions of the probability of sanction imposition for failing to comply with the ISP indicates that, in almost all cases examined, a violation would not result in punishment. This lack of fear of being punished clearly does not enhance an employee's intention to comply with the procedure. Also, respondents' perceived vulnerability for the ISP threats were weak all around (with the exception of the removable flash media threat); the current DoD information security awareness campaign, despite the significant resources applied to it, does not seem to be influencing employees in this area to the extent expected.

Finally, this research shows that, depending on the threat context, respondents' calculus of the consequences of conducting the ISP-directed security behavior is a significant factor in their attitude towards that action. Organizations should review the factors that do and do not affect this cost-benefit analysis to identify areas where

resources can be most effectively applied to raise the perceived overall benefit, reduce the cost, and thereby improve an employee's attitude towards the ISP behavior.

Limitations and Future Research Directions

There are several limitations of this study, as described in this section. The foremost limitation that is shared by this research and all of the empirical studies that inform this study is the measurement of behavioral intent versus actual behavioral compliance. While there is significant support in the literature for using intention as a predictor of actual behavior, there is no guarantee that an individual will behave as indicated. There are many more potential factors that are not modeled by the theory of planned behavior that may interfere with an individual's intention translating to actual behavior. For instance, the theoretical framework proposed in this study does not account for technical or environmental factors at a specific organization that can impede intention leading to action. A multitude of time and situational conditions such as high levels of ambient noise, poor door placement, being in a rush to leave work, individual's color blindness, ambiguous technology feedback, or having a good or bad day may intervene between a person's intent to enforce Tailgating requirements and actually recognizing or following through on preventing a violation. Unfortunately, this study did not gain the access to observe actual behavioral compliance after measuring intent in this organizational context. Future research should focus on measuring both intention and observing actual ISP compliance behavior to not only validate which factors were important in actual compliance, but also which factors failed or new factors came into play that caused a disconnect between intent and actual behavior.

Another considerable limitation of this study relates to the selection of participants. The participants in this study are not claimed to be a representative sample of all DoD employees; findings of this study should not generalized as applicable to the greater DoD employee base without significant caution. Requirements for surveying DoD personnel require researchers to gain approval of individual organizational commanders (the highest level of leaders in an organization) in order to gain access to their personnel. There are thousands of individual organizations in greater DoD enterprise. Even after permission is obtained, survey participation is mandatorily both anonymous and voluntary. Additionally, there are many different organizational sub-contexts in the DoD that may have significant impacts on the factors affecting an employee's behavioral intent. It was not feasible for this study to obtain a sample population that represented a random selection of participants from the greater DoD and address all possible organizational sub-contexts. However, all of the participants that did participate in this study did identify themselves as DoD employees who all fall under the guidance of the ISP described earlier. Future studies should look at exploring behavioral intent and actual compliance in a broader population of the DoD, with a greater attention taken to exploring different organizational sub-contexts within the DoD.

As with all other survey-based cross-sectional studies, the causal relationships implied in the proposed composite framework and models are inferred from underlying theories, not by the design of the study and correlations observed (or not observed). Future longitudinal research with multiple sources of measurement of intent and observed behavior should be used to further validate or refute the relationships identified in this study.

Additionally, this study applied Taylor & Todd's (1995) concept of decomposing the components of the theory of planned behavior only to Attitude and Perceived Behavioral Control (PBC). In the case of PBC, the results of this study failed to make a connection between an employee's perceived controllability of enforcing ISP requirements on coworkers and PBC. Future research is needed to determine how, if at all, the composite framework proposed in this study can be improved to account for the very real phenomenon of mandatory ISP enforcement on coworkers. And, while the decomposition of Attitude under various threat conditions identified numerous relationships between the variables, this study was not designed to determine why certain factors failed in one threat context but were significant in others. Lastly, there is an ample base of research on organizational commitment, subjective norms, and self-efficacy that can be drawn upon in future studies to explain in greater detail the factors affecting behavioral intent to comply with ISPs.

Conclusion

As the reliance of the world economy on information and information systems has increased, so too has the potential cost and impact of information security threats increased. Despite powerful and rapidly evolving technical security mechanisms designed to mitigate information security risks, it is often incumbent upon users to utilize the technologies and/or associated procedures faithfully and properly for them to be effective. In a modern organization, information security depends on the effective behavior of humans. Unfortunately, we humans are not doing a consistently good job at following the information security policies designed to help keep our information resources safe.

Building upon recent empirical research in information security policy behavioral compliance, this study provides a composite theoretical framework that captures key factors shown to impact an employee's behavioral intent to comply with related policies. The theoretical framework is tested and validated in a real organizational context employing a robust and well-defined set of information security policies, a first in this burgeoning line of research. Also a first, this study evaluates how behavioral intent to follow security policies, and its measured antecedents, vary for employees for both the general specter of information security policy compliance and specific guidance for three common security threats (phishing, tailgating, and the use of removable flash media). Lastly, the study explored how the impact of mandatory information security policy enforcement on coworkers affected overall intent to comply with information security policies.

This study found that, as predicted, the primary factors affecting behavioral intent (subjective norms, organizational commitment, attitude, perceived behavioral control, and self-efficacy) had strong, positive relationships with intent to comply with information security policies when examined at a high level of general compliance. However, when evaluated for specific information security threat contexts, individual factor importance and significance varied greatly. In the Removable Flash Media threat context, an employee's measured organizational commitment decreased from the most powerful influencer on behavioral intent to comply with the information security policy to the least impactful. Attitude, a relevant antecedent of behavioral intent in the General ISP compliance context, did not have a significant contributing relationship to behavioral intent in the Tailgating threat context. Additionally, employee Self-efficacy was strongly

related to behavioral intent in all threat contexts except Phishing. This variation in the significance and potency of behavioral intent antecedents would not be evident if different and relevant threat contexts were not evaluated. Focusing on the results of just the General ISP compliance context in this study would not have predicted the pattern of factor significance in any of the other threat contexts.

Evaluation of the factors affecting an employee's attitude towards a directed information security behavior showed similar variability between threat contexts. These results indicate that there is limited value in future research on "general" information security threat compliance without accounting for the differences in individual threat contexts. Additionally, evaluating the composite theoretical framework proposed in this study under different threat contexts highlights strengths and weaknesses under different conditions. There may be more value to researchers and practitioners alike in exploring when and why the theorized behavioral compliance factors fail than in confirming the presence and impact of variables that should be impactful.

Finally, while this study failed to establish a correlation between behavioral compliance intent and an employee's perception of their ability to enforce of mandatory information security policy requirements on coworkers, it did highlight a potential gap in the composite theoretical framework for this important phenomenon that should be addressed in future research.

APPENDIX. SURVEY ITEMS AND INSTRUMENT

Table 16: Survey Constructs, Questions, Item Number, and Source

Variable	Survey Question/Item	Survey item#	Source
Organizational Commitment	I am willing to put in a great deal of effort beyond that normally expected in order to help my organization be successful.	4	Mowday (1998), Herath & Rao (2009a)
	I really care about the fate of this organization.	5	
	For me, this is the best of all possible organizations for which to work.	6	
Behavioral Intent	I intend to comply with the _____ requirements of the ISP of my organization in the future.	7	Ajzen (1991), Bulgurcu et al. (2010)
	I intend to protect information and technology resources according to the _____ requirements of the ISP of my organzation in the future.	8	
	I intend to carry out my _____ responsibilities prescribed in the ISP of my organization when I use information and technology in the future.	9	
Perceived Subjective Norms	My peers/colleagues think that I should comply with the _____ requirements of the ISP.	10	Taylor & Todd (1995), Karahanna et al. (1999), Herath & Rao (2009a)
	My executives think that I should comply with the _____ requirements of the ISP.	11	
	My subordinates (or those junior to me) think that I should comply with the _____ requirements of the ISP.	12	
Self-efficacy	I have the necessary skills to fulfill the _____ requirements of the ISP.	13	Bandura (1997), Herath & Rao (2009a), Peace et al. (2003)
	I have the necessary knowledge to fulfill the _____ requirements of the ISP.	14	
	I have the necessary competencies to fulfill the _____ requirements of the ISP.	15	

Perceived Behavioral Control	I would be able to follow the ISP for _____ threats.	16	Taylor & Todd (1995)
	Following the ISP for _____ threats is entirely within my control.	17	
	I have the resources and knowledge and ability to follow the ISP for _____ threats.	18	
Attitude	Adopting ISP-related security technologies and practices is important for protecting against _____ threats.	19	Herath & Rao (2009a), Peace et al. (2003), Riemenschneider et al. (2003)
	Adopting ISP-related security technologies and practices is beneficial for protecting against _____ threats.	20	
	Adopting ISP-related security technologies and practices is helpful for protecting against _____ threats.	21	
Cost-Benefit Analysis	Implementing ISP-directed _____-related security practices is inconvenient.	22	Rippetoe & Rogers (1987), Milne et al. (2000), Workman et al. (2008)
	Implementing ISP-directed _____-related security practices is costly.	23	
	Implementing ISP-directed _____-related security practices negatively impacts my work.	24	
Perceived Sanction Severity	My organization disciplines employees who fail to follow the _____ requirements of ISP.	25	Herath & Rao (2009a), Peace et al. (2003), Knapp et al. (2005)
	My organization terminates employees who repeatedly fail to follow the _____ requirements of the ISP.	26	
	If I were caught violating the _____ requirements of the ISP, I would be severely punished.	27	
	Have you or someone you know ever been punished for failing to follow the _____ requirements of the ISP?	28	

Perceived Probability of Sanction Imposition	Employees that fail to follow the _____ requirements of the ISP would be caught, eventually.	29	Herath & Rao (2009a), Peace et al. (2003), Knapp et al. (2005)
	The likelihood the organization would discover that an employee failed to follow the _____ requirements of the ISP is:	30	
Perceived Vulnerability	The chances of experiencing a/an _____ threat at work is:	31	Champion (1984), Ng et al. (2009)
	There is a good possibility that I will encounter a/an _____ threat to my organization:	32	
	I am likely to encounter a/an _____ threat to my organization:	33	
Perceived Threat Severity	_____ threats to the security of my organization's information resources are:	34	Woon et al. (2005), Ng et al. (2009)
	Having my organization's information resources accessed by unauthorized parties because of _____ threats is:	35	
	Having someone successfully attack and damage my organization's information resources because of a/an _____ threat is:	36	
	Attacks on my organization's information resources due to _____ violations of the ISP are:	37	
Perceived Response Efficacy	Efforts to keep my organization's information resources safe from _____ threats are:	38	Rippetoe & Rogers (1987), Milne et al. (2000), Workman et al. (2008)
	The effectiveness of available measures to protect my organization's information resources from _____ threats is:	39	
	The preventative measures available to me to comply with the _____ requirements of the ISP are:	40	

Perceived Controllability	I am confident that I can follow the overall general information security guidance and actions directed by the ISP if I witnessed a violation in progress by one of my _____.	41	Taylor & Todd (1995), Ajzen (2002)
	I am confident that I can follow the overall guidance and actions regarding tailgating directed by the ISP if I witnessed a violation in progress by one of my _____.	42	
	I am confident that I can follow the overall guidance and actions regarding the use of removable flash media directed by the ISP if I witnessed a violation in progress by one of my _____.	43	
	Enforcing specific guidance and actions directed in the ISP on your coworkers is within your control.	44	Sparks et al. (1997), Ajzen (2002)
	Its mostly up to me to follow the guidance and actions directed in the ISP when I am required to enforce specific ISP policies on my coworkers.	45	

Table 17: Construct Means and Standard Deviations

Construct	General ISP		Removable Flash		Tailgating	
	Mean	Std Deviation	Mean	Std Deviation	Mean	Std Deviation
Behavioral Intent	6.660	0.474	6.678	0.561	6.579	0.620
Subjective Norms	6.455	0.593	6.406	0.728	6.357	0.746
Attitude	6.607	0.476	6.499	0.676	6.526	0.608
Organizational Commitment	6.060	0.769	6.060	0.769	6.060	0.769
Perceived Behavioral Control	6.370	0.652	6.478	0.657	6.423	0.725
Self-efficacy	6.503	0.559	6.583	0.562	6.538	0.611
Perceived Controllability						
Executives	6.038	0.997	6.167	0.897	5.766	1.268
Peers	6.201	0.805	6.293	0.793	5.971	1.094
Subordinates	6.264	0.790	6.335	0.776	6.059	0.910
Coworkers 1	6.188	0.806	6.188	0.806	6.188	0.806
Coworkers 2	6.251	0.791	6.251	0.791	6.251	0.791
Cost-Benefit Analysis	4.298	1.620	3.944	1.757	4.646	1.597
Perceived Sanction Severity	4.962	1.193	5.100	1.175	4.692	1.386
Perceived Probability of Sanction	5.174	1.161	5.487	1.115	4.877	1.364
Perceived Vulnerability	4.541	1.516	4.778	1.508	4.205	1.545
Perceived Threat Severity	5.892	0.957	5.837	1.048	5.690	1.071
Perceived Response Efficacy	5.817	0.766	5.909	0.829	5.488	1.139

Information Security Policy Compliance Survey

1. Privacy Act Statement

*1. PRIVACY ACT STATEMENT

Authority: SECNAVINST 5211.5E, Department of the Navy Privacy Act (PA) Program, 10(a) Page 12, 10(d) Page 13 of 28 December 2005

Purpose: Human performance data and other research information will be collected in an experimental project entitled "Exploring the Factors that Affect Employee Intention to Comply with Information Security Policies."

Routine Uses: The Departments of the Navy and Defense, and other U.S. Government agencies will use the resulting research data for analyses and reports. Use of the information obtained may be granted to non-Government agencies following the provisions of the Freedom of Information Act or contracts and agreements. I voluntarily agree to its disclosure to agencies or individuals identified above and I have been informed that failure to agree to this disclosure may make the research less useful. The "Blanket Routine Uses" that appear at the beginning of the Department of the Navy's compilation of data bases also apply to this system.

Voluntary Disclosure: Participation in this study and provision of information is voluntary. However, failure to provide requested information may invalidate test data and/or test procedures and could therefore result in removal from the project. Dismissal from the research project will involve no reproach, prejudice or jeopardy to my job or status.

I Understand - Continue

Information Security Policy Compliance Survey

2. Informed Consent Affirmation

INTRODUCTION

You are invited to participate in this study because you are at least 18 years old and are a military or civilian DoD employee. Your participation in this study is voluntary. You should read the information below and ask questions about anything you do not understand before deciding whether to participate.

PURPOSE OF RESEARCH

The present survey is part of an investigation that evaluates some of the factors that are believed to influence employee intention to follow information security policies. Specifically, we are interested in your personal opinions regarding general threats as well as three well-publicized information security threats to the Department of Defense (DoD): phishing, improper use of removable flash media, and access control. Please read each question carefully and answer it to the best of your ability. There are no correct or incorrect responses; we are merely interested in your personal point of view. Participation in this study will involve the completion of an on-line (Internet) survey or paper survey. The survey website, www.surveymonkey.com, is password protected and only the primary investigator will have access to the password.

DURATION OF STUDY INVOLVEMENT

Completion of the survey is expected to take less than one hour.

PROCEDURES

You are being asked to complete an online survey. Every effort has been made to guarantee your responses are anonymous. You are strongly encouraged to use a private computer. If you choose to use a private computer, your anonymity is protected by commercial state-of-the-art security software. **If you choose to use a Department of Defense (DoD) information system, you are reminded that DoD computers are not private and are subject to monitoring by the DoD.** If you choose to not complete the survey online, a hard copy of the survey will be made available to you along with a stamped envelope addressed to the principal investigator or the location of a secure survey collection box.

Prior to the survey, you are asked to read this informed consent form to understand your rights. In order to preserve your anonymity, participation in the online or hard copy survey will be counted as your consent. You will be asked complete a short background questionnaire including information about your rank, gender, and experience at the end of the survey. Each of the questions in this survey are voluntary. If you feel uncomfortable answering any particular question, you may skip that question and move on with the survey.

RISKS AND DISCOMFORTS

This research is considered to be minimal risk. Minimal risk means that the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests. **However, you are again reminded that DoD computers are not private and are subject to monitoring by the DoD.**

POTENTIAL BENEFITS

There is no direct benefit to you from participating in this study. The information derived from this study will ultimately provide organizational leadership with a better understanding of factors that affect an employee's intent to comply with information security policies, potentially leading to improvements in the overall information security posture of the DoD.

ALTERNATIVES TO PARTICIPATION

An alternative to participation in this study is to not participate in the study.

Information Security Policy Compliance Survey

VOLUNTARY PARTICIPATION AND WITHDRAWAL

Participation in the study is voluntary. Refusal to participate involves no penalty or loss of benefits, and you may discontinue participation at any time without. You are free to participate in this research or withdraw at any time. There will be no penalty or loss of benefits if you stop taking part in this study.

By volunteering for this study you have agreed to provide honest and ethical responses to the best of your ability throughout the study. Failure to follow directions and procedures may result in invalid test data that can negatively impact the research project. Participation or non-participation in this research project will involve no reproach, prejudice, or jeopardy to your job or status.

CONFIDENTIALITY AND PRIVACY

This survey is to be completed and data collected anonymously. Personal information regarding your participation as well as that of other subjects will not be collected. Only summarized and averaged information will be presented in technical reports and scientific presentations. Published information will not contain any identifiers associated with you or any other study volunteer. Specific survey response data will only be available to the principle investigators.

Participants that use DoD computers to take this survey online should be aware that while your use of any government information system, such as a PC to take this survey, is subject to monitoring by the DoD, the researchers conducting this study are not privy to any monitoring information or logs that can be used to associate you with a specific survey response. Those concerned with possible monitoring of their survey responses by the DoD are encouraged to use a personal (non-DoD) computer or request a hard-copy survey by emailing salvatore.aurigemma@navy.mil.

CONTACT INFORMATION

You are free at any time to make inquiries concerning the procedures employed in this study and that the investigators will respond freely to those inquiries. For inquiries during and after the study has been completed you may also contact the principal investigator, Sal Aurigemma, SSC Pacific H531, salvatore.aurigemma@navy.mil, 808.352.0307. You may also contact the University of Hawaii Committee on Human Studies at 808.956.5007 or uhirb@hawaii.edu or my faculty advisory, Dr. Raymond Panko, at panko@hawaii.edu.

Please print this form for your records.

This is revision # 1 of 1. Approved 30 JUL 2012. This document may NOT be used after 30 JUL 2013.

***2. I understand the informed consent information above and agree to take the survey.**

- Yes
- No

Information Security Policy Compliance Survey

3. Main Survey Questions

Please answer all the following questions.

3. Are you taking this survey online using a personal or DoD computer?

Please note: if you are uncomfortable taking this online survey on a DoD computer, you are encouraged to use a personal computer or request a hard-copy of the survey from salvatore.aurigemma@navy.mil.

- Personal Computer
- DoD Computer

Background and Definitions: The following is provided to assist in understanding and answering the survey questions.

ISP: An Information Security Policy (ISP) describes employee roles and responsibilities, addressing specific security issues, in protecting the information resources of an organization. Many Department of Defense (DoD) organizations have their own mission-specific ISP. However, all DoD employees fall under the umbrella information security policy guidance provided in the mandatory annual training called Information Assurance Awareness (IAA) posted at http://iase.disa.mil/eta/index.html. When answering questions below, consider the current IAA online training matter as your organization's ISP.

Phishing: Phishing is a way of attempting to acquire information such as usernames, passwords, and banking/credit card details by masquerading as a trustworthy entity in an electronic communication. In many cases, victims of phishing may inadvertantly threaten their organization's information systems by injecting malware (malicious software) into the computer network. The best defense against phishing is employee awareness and proper action.

Removable Flash Media: The Defense Department banned the use of removable flash media and storage devices from all government computers in 2008. In 2010, the ban was rescinded in special cases where removable media use will be limited to mission-essential operations, and only after strict compliance requirements are met. Most DoD organizations currently enforce the ban on flash drives.

Tailgating: Physical tailgating (also known as piggybacking) is a method for gaining entry to controlled access areas (where control is accomplished by electronically or mechanically locked doors) by following closely behind another person without applying your own proper credentials. DoD policy on tailgating applies to an employee's own actions to not tailgate, but also to ensure that others do not tailgate when using your credentials to enter or exit a controlled access area.

---

4. I am willing to put in a great deal of effort beyond that normally expected in order to help my organization be successful.

	Strongly Disgree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
Please choose one:							

5. I really care about the fate of this organization.

	Strongly Disgree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
Please choose one:							

6. For me, this is the best of all possible organizations for which to work.

	Strongly Disgree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
Please choose one:							

7. I intend to comply with the _____requirements of the ISP of my organization in the future.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

8. I intend to protect information and technology resources according to the _____requirements of the ISP of my organzation in the future.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

9. I intend to carry out my _____responsibilities prescribed in the ISP of my organization when I use information and technology in the future.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

10. My peers think that I should comply with the _____requirements of the ISP.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

Information Security Policy Compliance Survey

11. My executives think that I should comply with the _____requirements of the ISP.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

12. My subordinates (or those junior to me) think that I should comply with the _____requirements of the ISP.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

Information Security Policy Compliance Survey

4. Main Survey (cont.)

13. I have the necessary skills to fulfill the _____requirements of the ISP.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

14. I have the necessary knowledge to fulfill the _____requirements of the ISP.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

15. I have the necessary competencies to fulfill the _____requirements of the ISP.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

16. I would be able to follow the ISP for _____threats.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

17. Following the ISP for _____threats is entirely within my control.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

18. I have the resources and knowledge and ability to follow the ISP for _____ threats.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

19. Adopting ISP-directed security technologies and practices is important for protecting against _____threats.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

20. Adopting ISP-directed security technologies and practices is beneficial for protecting against _____threats.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

21. Adopting ISP-directed security technologies and practices is helpful for protecting against _____threats.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

22. Implementing ISP-directed _____-related security practices is inconvenient.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							

Information Security Policy Compliance Survey

23. Implementing ISP-directed _____-related security practices is costly.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

24. Implementing ISP-directed _____-related security practices negatively impacts my work.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

Information Security Policy Compliance Survey

5. Main Survey (cont.)

25. My organization disciplines employees who fail to follow the _____ requirements of ISP.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

26. My organization terminates employees who repeatedly fail to follow the _____requirements of the ISP.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

27. If I were caught violating the _____requirements of the ISP, I would be severely punished.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

28. Have you or someone you know ever been punished for failing to follow the _____requirements of the ISP?

	Yes	No
General Information Security:		
Phishing:		
Removable Flash Media:		
Tailgating:		

29. Employees that fail to follow the _____requirements of the ISP would be caught, eventually.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

30. The likelihood my organization would discover that an employee failed to follow the _____requirements of the ISP is:

	Very Low	Low	Somewhat Low	Neutral	Somewhat High	High	Very High
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

31. The chances of experiencing a _____threat at work is:

	Very Low	Low	Somewhat Low	Neutral	Somewhat High	High	Very High
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

32. There is a good possibility that I will encounter a/an _____threat to my organization:

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

33. I am likely to encounter a/an _____threat to my organization:

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

6. Main Survey (cont.)

34. _____threats to the security of my organization's information resources are:

	Very Harmless	Harmless	Somewhat Harmless	Neutral	Somewhat Severe	Severe	Very Severe
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

35. Having my organization's information resources accessed by unauthorized parties because of _____threat(s) is:

	Very Harmless	Harmless	Somewhat Harmless	Neutral	Somewhat Harmful	Harmful	Very Harmful
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

36. Having someone successfully attack and damage my organization's information resources because of a/an _____threat is:

	Very Harmless	Harmless	Somewhat Harmless	Neutral	Somewhat Harmful	Harmful	Very Harmful
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

37. Attacks on my organization's information resources due to _____ violations of the ISP are:

	Very Harmless	Harmless	Somewhat Harmless	Neutral	Somewhat Harmful	Harmful	Very Harmful
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

38. Efforts to keep my organization's information resources safe from _____ threats are:

	Very Ineffective	Ineffective	Somewhat Ineffective	Neutral	Somewhat Effective	Effective	Very Effective
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

39. The effectiveness of available measures to protect my organization's information resources from _____threats is:

	Very Ineffective	Ineffective	Somewhat Ineffective	Neutral	Somewhat Effective	Effective	Very Effective
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

40. The preventative measures available to me to comply with the _____ requirements of the ISP are:

	Very Ineffective	Ineffective	Somewhat Ineffective	Neutral	Somewhat Effective	Effective	Very Effective
General Information Security:							
Phishing:							
Removable Flash Media:							
Tailgating:							

41. I am confident that I can follow the guidance and actions directed by the ISP if I witnessed a general information security violation in progress by one of my _____.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
Executives							
Peers							
Subordinates (or those of lower rank/status)							

42. I am confident that I can follow the overall guidance and actions directed by the ISP if I witnessed a tailgating violation in progress by one of my _____.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
Executives							
Peers							
Subordinates (or those of lower rank/status)							

43. I am confident that I can follow the overall guidance and actions directed by the ISP if I witnessed a removable flash media violation in progress by one of my _____.

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
Executives							
Peers							
Subordinates (or those of lower rank/status)							

44. Enforcing specific guidance and actions directed in the ISP on your coworkers is within your control.

	Strongly Disgree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
Please choose one:							

45. Its mostly up to me to follow the guidance and actions directed in the ISP when I am required to enforce specific ISP policies on my coworkers.

	Strongly Disgree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
Please choose one:							

Information Security Policy Compliance Survey

7. Demographic Information

The information collected in this section is solely used for statistical analysis and can not and will not be used to determine respondent identity.

46. What is your gender?

- Male
- Female

47. What is the primary community in which you work?

- Administration
- Intelligence
- Operations
- Logistics and/or Maintenance
- Command, Control, Communication, Computers
- Command Staff Element
- Other (please specify)

48. How do you rate your knowledge of computers and Information Technology in general?

	Very Low	Low	Somewhat Low	Neutral	Somewhat High	High	Very High
- Please choose one:							

49. Choose your rank / pay grade / positional status in your organization.

- E1-E3
- E4-E6
- E7-E9
- GS1-GS6
- GS7-GS12
- GS13 and above
- O1-O2
- O3-O4
- O5 and above
- Other (please specify)

References

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior, In J. Kuhl & J. Beckman (Eds.), *Action control: From cognition to behavior*. Berlin, Germany: Springer& Verlag.

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

Ajzen, I. (2001). Nature and operation of attitudes. *Annual review of psychology*, *52*(1), 27–58.

Ajzen, I. (2002). Perceived Behavioral Control, Self Efficacy, Locus of Control, and the Theory of Planned Behavior1. *Journal of Applied Social Psychology*, *32*(4), 665–683.

Ajzen, I., & Albarracín, D. (2007). Predicting and changing behavior: A reasoned action approach. *Prediction and change of health behavior: Applying the reasoned action approach*, 1–22.

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior* (Vol. 278). Prentice-Hall.

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Security Policy Compliance: User Acceptance Perspective. *2012 45th Hawaii International Conference on System Sciences* (pp. 3317–3326). IEEE.

ALNAV 057/57. (2007). Safeguarding Personally Identiable Information (PII) from Unauthorized Disclosure. Retrieved from www.doncio.navy.mil/Download.aspx?AttachID=429

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–A15. doi:Article

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological bulletin*, *103*(3), 411.

Andress, J. (2011). Advanced Persistent Threat - Attacker Sophistication Continues to Grow? *Information System Security Association*, 18–24.

Armitage, C. J., & Conner, M. (2001). Efficacy of the theory of planned behavior: A meta-analytic review. *British Journal of Social Psychology*, *40*(4), 471–499.

Arthur, C. (2009, April 30). Facebook: phishing scam spreads through popular social networking site. Retrieved March 31, 2012, from http://www.guardian.co.uk/technology/2009/apr/30/facebook-phishing-scam

Bagozzi, R. P. (1981). Attitudes, intentions, and behavior: A test of some key hypotheses. *Journal of Personality and Social Psychology; Journal of Personality and Social Psychology*, *41*(4), 607.

Bagozzi, R. P., Yi, Y., & Phillips, L. W. (1991). Assessing construct validity in organizational research. *Administrative science quarterly*, 421–458.

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

Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational behavior and human decision processes*, *50*(2), 248–287.

Bandura, A. (1997). *Self-efficacy: The exercise of control*. Worth Publishers.

Baron, R.M., & Kenny, D.A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology, 51*(6), 1173-1182.

Beck, K. H. (1981). Driving while under the influence of alcohol: relationship to attitudes and beliefs in a college population. *The American Journal of Drug and Alcohol Abuse*, *8*(3), 377–388.

Blue, C. L. (1995). The predictive capacity of the theory of reasoned action and the theory of planned behavior in exercise research: An integrated literature review. *Research in nursing & health*, *18*(2), 105–121.

Bollen, K., & Lennox, R. (1991). Conventional wisdom on measurement: A structural equation perspective. *Psychological Bulletin*, *110*(2), 305-314.

Bollen, K. A., & Stine, R. A. (1992). Bootstrapping goodness-of-fit measures in structural equation models. *Sociological Methods & Research*, *21*(2), 205-229.

Boomsma, A. (1987). The robustness of maximum likelihood estimation in structural equation models. In P. Cuttance & R. Ecob (Eds.) *Structural equation modeling by example: Applications in educational, sociological, and behavioral research* (pp. 160-188). Cambridge, England: Cambridge University Press.

Brackney, R., & Anderson, R. (2004). *Understanding the Insider Threat* (Conference Proceedings). RAND National Security Research Division.

Brinberg, D., & Durand, J. (1983). Eating at Fast Food Restaurants: An Analysis Using Two Behavioral Intention Models. *Journal of Applied Social Psychology*, *13*(6), 459–472.

Bulgurcu, B. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523–548.

Brown, T.A. (2006). *Confirmatory factor analysis for applied research*. New York, NY: The Guilford Press.

Byrne, B.M. (2001). Structural equation modeling with AMOS: Basic concepts, applications, and programming. Mahway, NJ: Lawrence Erlbaum Associates

Calluzzo, V. J., & Cante, C. J. (2004). Ethics in information technology and software use. *Journal of Business Ethics*, *51*(3), 301–312.

Cavalli, E. (2009, April 29). World of Warcraft Phishing Attempts on the Rise. Retrieved March 31, 2012, from http://www.wired.com/gamelife/2009/04/world-of-warcraft-phishing-attempts-on-the-rise/

Champion, V. L. (1984). Instrument development for health belief model constructs. *Advances in Nursing Science; Advances in Nursing Science*.

Cheung, G.W., & Lau, R.S. (2008). Testing mediation and suppression effects of latent variables: Bootstrapping with structural equation models. *Organizational Research Methods, 11*(2), 296-325.

Chin, W. W. (1998). Issues and Opinion on Structural Equation Modeling, *MIS Quarterly* (22:1), pp. vii-xvi.

CISCO Systems. (2008). *Data Leakage Worldwide White Paper: The High Cost of Insider Threats [Data Loss Prevention] - Cisco Systems* (White Paper No. C11-506224) (p. 6). Retrieved from http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-506224.html

CJCSI 6510.01F. (2011, February 9). Information Assurance (IA) and Support to Computer Network Defense (CND). Retrieved from www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf

Cloppert, M. (2009, July 22). Security Intelligence: Introduction (pt 1). Retrieved March 31, 2012, from http://computer-forensics.sans.org/blog/2009/07/22/security-intelligence-introduction-pt-1/

Computer Economics. (2009, March). Security Threats in Employee Misuse of IT Resources. Retrieved March 31, 2012, from http://www.computereconomics.com/article.cfm?id=1436

Conner, M., & Armitage, C. J. (1998). Extending the theory of planned behavior: A review and avenues for further research. *Journal of applied social psychology*, *28*(15), 1429–1464.

Conner, M., & Sparks, P. (2005). The theory of planned behaviour and health behaviours. *Predicting health behaviour*, *2*, 170–222.

Cummins, D. D. (1999). Cheater detection is modified by social rank: The impact of dominance on the evolution of cognitive functions. *Evolution and Human Behavior*, *20*(4), 229–248.

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

Daniel, L. (2010, May 10). Officials warn of "phishing" scams targeting troops. Retrieved March 31, 2012, from http://www.af.mil/news/story.asp?id=123203895

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

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

Defense Information Systems Agency (DISA). (2012). Information Assurance Awareness v10.0. Retrieved March 31, 2012, from http://iase.disa.mil/eta/iaav10/index.htm

Department of Defense (DOD). (2010). *Demographics 2010: Profile of the Military Community*. Retrieved from http://www.cpms.osd.mil/ASSETS/D07134577EB5472087A64F5968284C13/20100930%20FINAL.pdf

Diamantopoulos, A., & Winklhofer, H. M. (2001). Index construction with formative indicators: an alternative to scale development. *Journal of Marketing Research*, 269-277.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, *8*(7), 23.

Ernst & Young. (2011). *2011 Global Information Security Survey: Plugging the data leaks*. Retrieved from http://www.ey.com/GL/en/Services/Advisory/2011-Global-Information-Security-Survey---Plugging-the-data-leaks

Fishbein, M. (2008). A reasoned action approach to health promotion. *Medical Decision Making*, *28*(6), 834.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior*. Addison-Wesley.

Fishbein, M., & Cappella, J. N. (2006). The role of theory in developing effective health communications. *Journal of Communication*, *56*, S1–S17.

Fishbein, M., & Yzer, M. C. (2003). Using theory to design effective health behavior interventions. *Communication Theory*, *13*(2), 164–183.

Fornell, C., & Bookstein, F. L. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of Marketing Research*, 440-452.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 39-50.

Gall, C. (2006, April 15). At Afghan Bazaar, Military Offers Dollars for Stolen Data. Retrieved March 31, 2012, from http://www.nytimes.com/2006/04/15/world/asia/15afghanistan.html

Gefen, D., Straub, D. W., & Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice.

Gefen, D., Rigdon, E., & Straub, D. (2011). An Update and Extension to SEM Guidelines for Admnistrative and Social Science Research. *Management Information Systems Quarterly*, *35*(2), iii–xiv.

Giles, M., Mcclenahan, C., Cairns, E., & Mallet, J. (2004). An application of the Theory of Planned Behaviour to blood donation: the importance of self-efficacy. *Health Education Research*, *19*(4), 380.

Godin, G. (1993). The theories of reasoned action and planned behavior: Overview of findings, emerging research problems and usefulness for exercise promotion. *Journal of Applied Sport Psychology*, *5*(2), 141–157.

Godin, G., & Kok, G. (1996). The theory of planned behavior: a review of its applications to health-related behaviors. *American journal of health promotion*, *11*(2), 87–98.

Goodin, D. (2013). New Microsoft patch purges USB bug that allowed complete system hijack. In *Risk Assessment / Security & Hacktivism*. Retrieved March 13, 2013, from http://arstechnica.com/security/2013/03/new-microsoft-patch-purges-usb-bug-that-allowed-complete-system-hijack/.

Greenlees, C. (2009, July 21). Social engineering: an intruder's tale. Retrieved March 31, 2012, from http://eandt.theiet.org/magazine/2009/13/intruders-tale.cfm

Grewal, R., Cote, J. A., & Baumgartner, H. (2004). Multicollinearity and measurement error in structural equation models: Implications for theory testing. *Marketing Science*, *23*(4), 519-529.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems*, *28*(2), 203–236.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2010). *Multivariate data analysis* (Vol. 7). Upper Saddle River, NJ: Prentice Hall.

Hardcastle, Jonathan, G., Colleen, Kjeldsen, P., & Shiffler III, G. (2012). Forecast Alert: IT Spending, Worldwide, 2008-2014, 4Q10 Update | 1512016. Retrieved March 24, 2012, from http://www.gartner.com/id=1512016

Hausenblas, H. A., Carron, A. V., & Mack, D. E. (1997). Application of the theories of reasoned action and planned behavior to exercise behavior: A meta-analysis. *Journal of Sport & Exercise Psychology*.

Heck, R. H. (1998). Factor analysis: Exploratory and confirmatory approaches. *Modern Methods for Business Research*, 177–215.

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

Herath, Tejaswini, & Rao, H. R. (2009b). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165.

Hoffer, J. A., & Straub, D. W. (1989). The 9 to 5 underground: Are you policing computer crimes. *Sloan Management Review*, *30*(4), 35–43.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74–81.

Hu, L., & Bentler, P. M. (1998). Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification. *Psychological methods*, *3*(4), 424.

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, *6*(1), 1–55.

Huh, H. J., Kim, T. T., & Law, R. (2009). A comparison of competing theoretical models for understanding acceptance behavior of information systems in upscale hotels. *International Journal of Hospitality Management*, *28*(1), 121–134.

Ifinedo, P. (2011). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*.

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research*, *30*(2), 199-218.

Jensen, J. (2011, January 1). Ready to Tailgate? Retrieved March 31, 2012, from http://www.securitymagazine.com/articles/81596-ready-to-tailgate

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, *34*(1).

Jöreskog, K. G., & Goldberger, A. S. (1975). Estimation of a model with multiple indicators and multiple causes of a single latent variable. *Journal of the American Statistical Association*, *70*(351a), 631-639.

Jöreskog, K. G., & Sörbom, D. (1989). LISREL 7: A guide to the program and applications.

Jöreskog, K. G., and Sörbom, D. 2001. LISREL 8: User's Reference Guide, Chicago: Scientific Software International.

Kaplan, D. (2012, January 27). Univ. of Hawaii settles with 98,000 over five breaches. *SC Magazine*. Retrieved from http://www.scmagazine.com/univ-of-hawaii-settles-with-98000-over-five-breaches/article/225158/

Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs. *Mis Quarterly*, 183–213.

Kirscht, J. P., Haefner, D. P., Kegeles, S. S., & Rosenstock, I. M. (1966). A national study of health beliefs. *Journal of Health and Human Behavior*, *7*(4), 248–254.

Knapp, K., Marshall, T., Rainer, R., & Ford, F. (2005). Managerial dimensions in information security: A theoretical model of organizational effectiveness.(ISC) Inc. *Framingham, Massachusetts and Auburn University, Auburn, Alabama*.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security*, *10*(2), 57–63.

Leonard, L., & Cronan, T. (2001). Illegal, inappropriate, and unethical behavior in an information technology context: A study to explain influences. *Journal of the Association for Information Systems*, *1*(12), 1–31.

Leonard, L., Cronan, T., & Kreie, J. (2004). What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics? *Information & Management*, *42*(1), 143–158.

Limayem, M., & Hirt, S. G. (2003). Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for Information Systems*, *4*(1), 3.

Lynn III, W. (2010, October). Defending a New Domain. Retrieved March 31, 2012, from http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

Mahon, D., Cowan, C., & McCarthy, M. (2006). The role of attitudes, subjective norm, perceived control and habit in the consumption of ready meals and takeaways in Great Britain. *Food Quality and Preference*, *17*(6), 474–481.

Manstead, A. S. ., & Parker, D. (1995). Evaluating and extending the theory of planned behaviour. *European review of social psychology*, *6*(1), 69–95.

MARADMIN 143/06. (2006, March 24). Lost Privacy Act Data. Retrieved March 31, 2012, from http://www.marines.mil/news/messages/Pages/2006/Messages0622.aspx

Marcoulides, G. A. & Chin, W. W. (2012). You write, but others read: Common methodological misunderstandings in PLS and related methods. *7th International Conference on Partial Least Squares and Related Methods*, May 19-May 22, 2012 Houston, Texas, USA

Marsh, H. W., Hau, K.-T., & Wen, Z. (2004). In search of golden rules: Comment on hypothesis-testing approaches to setting cutoff values for fit indexes and dangers in overgeneralizing Hu and Bentler's (1999) findings. *Structural Equation Modeling*, *11*(3), 320–341.

Mealey, L., Daood, C., & Krage, M. (1996). Enhanced memory for faces of cheaters. *Ethology and Sociobiology*, *17*, 119–128.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and Intervention in Health-Related Behavior: A Meta-analytic Review of Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(1), 106–143.

Mitnick, K. D., Simon, W. L., & Wozniak, S. (2002). *The art of deception* (Vol. 1). Wiley Indianapolis.

Moscaritolo, A. (2010, July 7). Hacker accesses sensitive University of Hawaii server. *SC Magazine*. Retrieved from http://www.scmagazine.com/hacker-accesses-sensitive-university-of-hawaii-server/article/174118/

Mowday, R. T. (1999). Reflections on the study and relevance of organizational commitment. *Human Resource Management Review*, *8*(4), 387–401.

Muthén, L. K., & Muthén, B. O. (2002). How to use a Monte Carlo study to decide on sample size and determine power. *Structural Equation Modeling*,*9*(4), 599-620.

National Institute for Standards and Technology (NIST). (2008). *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems* (Special Report). 800-116.

Nejad, L., Wertheim, E., & Greenwood, K. (2005). Comparison of the health belief model and the theory of planned behaviour in the prediction of dieting and fasting behaviour. *E-journal of applied psychology*, *1*(1), 63–74.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (Calvin). (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825.

Oliver, R. L., & Bearden, W. O. (1985). Crossover effects in the theory of reasoned action: A moderating influence attempt. *Journal of Consumer Research*, 324–340.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on* (p. 156b–156b). IEEE.

Panko, R. (2009). *Business computer and network security*. Englewood Cliffs, NJ: Prentice-Hall.

Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS quarterly*, 115–143.

Peace, A. G., Galletta, D. F., & Thong, J. Y. . (2003). Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems*, *20*(1), 153–178.

Pechmann, C., Zhao, G., Goldberg, M. E., & Reibling, E. T. (2003). What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes. *The Journal of Marketing*, *67*(2), 1–18.

Perugini, M., & Bagozzi, R. P. (2001). The role of desires and anticipated emotions in goal directed behaviours: Broadening and deepening the theory of planned behaviour. *British Journal of Social Psychology*, *40*(1), 79–98.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of applied psychology*, *88*(5), 879.

Raykov, T., & Marcoulides, G. A. (2006). *A first course in structural equation modeling*. Lawrence Erlbaum.

Reeder, K. (2012). VeriSign repeatedly hacked in 2010 | TechRepublic. Retrieved March 31, 2012, from http://www.techrepublic.com/blog/security/verisign-repeatedly-hacked-in-2010/7379

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816–826. doi:doi: DOI: 10.1016/j.cose.2009.05.008

Richardson, R. (2011). 2011 CSI Computer Crime and Security Survey. *Computer Security Institute*.

Riemenschneider, C. K., Harrison, D. A., & Mykytyn, P. P. (2003). Understanding IT adoption decisions in small business: integrating current theories. *Information & Management*, *40*(4), 269–285.

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology; Journal of Personality and Social Psychology*, *52*(3), 596.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*, *91*(1), 93–114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology: A sourcebook*, 153–176.

Rotter, J. B. (1966). Generalized expectancies for internal versus external control of reinforcement. *Psychological Monographs: General & Applied*.

Russell, D. W. 2002. In Search of Underlying Dimensions: The Use (and Abuse) of Factor Analysis. *Personality and Social Psychology Bulletin* (28), pp. 1629-1646.

Rutter, D. R. (1989). Models of belief-behaviour relationships in health. *Health Psychology Update*, *4*, 3–10.

Schneier, B. (2011). *Secrets and lies: digital security in a networked world*. Wiley.

Shimp, T. A., & Kavas, A. (1984). The theory of reasoned action applied to coupon usage. *Journal of Consumer Research*, 795–809.

Simon, H. A. (1955). A behavioral model of rational choice. *The quarterly journal of economics*, *69*(1), 99–118.

Siponen, M. T. (2005). Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. *Information and organization*, *15*(4), 339–375.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487–502.

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

Sparks, P., Hedderley, D., & Shepherd, R. (1992). An investigation into the relationship between perceived control, attitude variability and the consumption of two common foods. *European Journal of Social Psychology*, *22*(1), 55–71.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124–133. doi:doi: DOI: 10.1016/j.cose.2004.07.001

Straub, D., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, *13*(24), 380–427.

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

Straub, D. W., & Straub, W. (1990). Effective IS security. *Information Systems Research*, *1*(3), 255–276.

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

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

Stone-Romero, E. F., & Rosopa, P. J. (2004). Inference problems with hierarchical multiple regression-based tests of mediating effects. *Research in Personnel and Human Resources Management*, 23, 249-290.

Symantec. (2012). Claims by Anonymous about Symantec Source Code | Symantec. Retrieved March 31, 2012, from http://www.symantec.com/theme.jsp?themeid=anonymous-code-claims

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information systems research*, *6*(2), 144–176.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, *24*(6), 472–484. doi:doi: DOI: 10.1016/j.cose.2005.05.002

Trafimow, D., Sheeran, P., Conner, M., & Finlay, K. A. (2002). Evidence that perceived behavioural control is a multidimensional construct: Perceived control and perceived difficulty. *British Journal of Social Psychology*, *41*(1), 101–121.

Triandis, H. C. (1977). *Interpersonal behavior*. Brooks/Cole Pub. Co.

United Nations. (2005). Information Economy Report 2005. Retrieved March 31, 2012, from http://www.unctad.org/en/templates/download.aspx?docid=6479&lang=1&intItemID=1397

Venkatesh, V. (1999). Creation of favorable user perceptions: exploring the role of intrinsic motivation. *MIS quarterly*, 239–260.

Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information systems research*, *11*(4), 342–365.

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

Venkatesh, V., & Davis, F. D. (1996). A model of the antecedents of perceived ease of use: Development and test*. *Decision Sciences*, *27*(3), 451–481.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management science*, 186–204.

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

Verisign. (2009). *Fraud Alert: Phishing: The Latest Tactics and Potential Business Impact.* (White Paper). Retrieved from http:// www.verisign.com/static/phishing-tactics.pdf

Von Hirsch, A., Bottoms, A. E., Burney, E., & Wikstrom, P. (1999). *Criminal deterrence and sentence severity: An analysis of recent research*. Hart.

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*(3), 191–198. doi:doi: DOI: 10.1016/j.cose.2004.01.012

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, *18*(2), 101–105.

Wells, J. T. (2005). *Principles of fraud examination*. John Wiley.

Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM*, *46*(8), 91–95.

Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security. *Proceedings of the Twenty-Sixth International Conference on Information Systems. Las Vegas, Nevada.*

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Security Journal: A Global Perspective*, *16*(6), 315–331.

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

Yi, M. Y., & Hwang, Y. (2003). Predicting the use of web-based information systems: self-efficacy, enjoyment, learning goal orientation, and the technology acceptance model. *International Journal of Human-Computer Studies*, *59*(4), 431–449.

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