Journal of the Association for Information Systems (2019) **20**(12), 1700-1742
doi: 10.17705/1jais.00583

RESEARCH ARTICLE

ISSN 1536-9323

Generally Speaking, Context Matters: Making the Case for a Change from Universal to Particular ISP Research

Sal Aurigemma[1], Thomas Mattson[2]

[1]University of Tulsa, USA, sal-aurigemma@utulsa.edu
[2]University of Richmond, USA, tmattson@richmond.edu

Abstract

The objective of our paper is to conceptually and empirically challenge the idea of general information security policy (ISP) compliance. Conceptually, we argue that general ISP compliance is an ill-defined concept that has minimal theoretical usefulness because the policy-directed security actions vary considerably from threat to threat in terms of time, difficulty, diligence, knowledge, and effort. Yet, our senior IS scholars' basket of journals has a strong preference to publish models in which the authors speculate that their findings are generalizable across all (or many) threats and controls contained in an organization's ISP document. In our paper, we argue that compliance with each of the mandatory threat-specific security actions may require different (as opposed to similar) explanatory models, which makes constructing a universal model of ISP compliance problematic. Therefore, we argue that future ISP compliance literature will be more valuable if it focuses on the mechanisms, treatments, and behavioral antecedents associated with the required actions around specific threats instead of attempting to build a model that purportedly covers all (or many) threat-specific security actions (or intentions thereof). To support this claim empirically, we conducted two studies comparing general compliance intentions (i.e., undefined security action) and threat-specific compliance intentions. In both studies, our data show that compliance intentions vary significantly across general compliance measures and multiple threat-specific security measures or scenarios. Our results indicate that it is problematic to generalize about the behavioral antecedents from general compliance intentions to threat-specific security compliance intentions, from one threat-specific security action to other threat-specific security actions, and from one threat-specific security action to general compliance intentions.

Keywords: Universalism, Particularism, Theory of Planned Behavior, Protection Motivation Theory, Deterrence Theory, Rational Choice Theory, Behavioral Information Security, Compliance

Mikko Siponen was the accepting senior editor. This research article was submitted on May 26, 2016 and underwent three revisions.

1 Introduction

Employees are required to follow a variety of policies contained in their organization's information security policy (ISP) document (Bulgurcu, Cavusoglu, & Benbasat, 2010; Crossler, Long, Loraas, & Trinkle, 2014; Moody, Siponen, & Pahnila, 2018). Typical ISP documents are organized around the preventative and mitigating actions associated with specific threats (Siponen & Vance, 2014). For example, one section of the ISP might detail an employee's required security actions pertaining to the ransomware threat whereas another section might outline an employee's requirements pertaining to the phishing threat. Each section of the ISP outlines threat-specific security actions with differing levels of time, difficulty, diligence, knowledge, and effort in order to comply

with the specific policies (Posey, Roberts, Lowry, Bennett, & Courtney, 2013; Workman, Bommer, & Straub, 2008). [1] That is, all policies and policy violations are not the same because there are many different types of ISP-mandated actions, mitigating controls, and infractions (Siponen & Baskerville, 2018). [2]

However, much of the ISP compliance research that has been published in our senior IS scholars' basket of journals[3] tends to focus on constructing models that attempt to explain generalized security behaviors across many or all ISP-directed actions (or intentions thereof). These papers make these claims by speculating about the generalizability of the threat-specific security action or actions that they investigated, by aggregating values across multiple threat-specific measures or scenarios, or by using generic (i.e., undefined security action) measures [4] (Crossler & Belanger, 2014; Posey, Roberts, & Lowry, 2015). Yet, while compliance with the policies for certain threats and their mitigating controls may be relatively effortless, compliance with other policies may be quite deliberate and mindful (Goel, Williams, & Dincelli, 2017). If employees use different thought processes to comply with the ISP-mandated policies related to different threats, then we assert that compliance intentions with each threat-specific security action should logically have different mechanisms, treatments, and behavioral antecedents. Therefore, we argue that this behavioral variability across different policy-mandated actions makes constructing a widely generalizable model of ISP compliance that encompasses the policy requirements related to all (or most) threat-specific security actions problematic.

The purpose of our paper is twofold: (1) to review the existing ISP compliance literature in the senior IS scholars' basket of journals (i.e., the publications that are shaping the direction of the field) to determine the implicit or explicit scope of generalization along with the type of evidence used to make those generalization claims; [5] and (2) to investigate empirically whether those generalization claims are valid. Our literature review reveals that having the perception of wide generalizability of empirical results appears to be a hurdle that authors must clear in order to publish an ISP compliance paper in one of our top journals. We suggest that this publication hurdle is not consistent with the variety of threat-specific security actions that employees are required to perform (per the ISP) on a daily basis. Therefore, we propose that developing a particular "model of phishing ISP compliance" or "model of tailgating ISP compliance" is more theoretically useful than speculating about whether the results from one threat-specific security action are universally generalizable to other threat-specific security actions, because different sections of the ISP require different types of security behaviors.[6]

We then conducted two empirical studies in different organizations where we compared general compliance intentions (i.e., "I intend to comply with the ISP", which does not refer to any threat-specific security action) and threat-specific security compliance intentions (i.e., "I intend to comply with the <<insert threat-specific security action here>> policies" or a scenario vignette covering a threat-specific security action). The threat-specific security actions that we investigated were phishing, tailgating, flash media, workstation locking, and password sharing. [7] We evaluated these different ISP-directed security actions

[1] An organization's ISP document may cover more stakeholders than just employees. For instance, a library's ISP may cover patrons connecting to its digital resources and a university's ISP may cover visitors as well as students connecting to its network. For simplicity, we use the term employee to refer to any individual who is covered by an organization's ISP.

[2] Not all ISPs are organized around specific threats. Certain ISPs are organized around mitigating controls or countermeasures, which may cover multiple threat-specific security actions in a single policy. Regardless, each policy requires specific security actions whether those actions cover a single threat or multiple threats.

[3] These journals are the following: *MIS Quarterly*, *Information Systems Research*, *European Journal of Information Systems*, *Information Systems Journal*, *Journal of the Association of Information Systems*, *Journal of Management Information Systems*, *Journal of Information Technology*, and *Journal of Strategic Information Systems*.

[4] These generic measures refer to the ISP document as a whole (i.e., compliance with all, most, or many of the policies contained in the ISP document without referring to a specific policy, threat, mitigating control, or countermeasure).

[5] The term generalization is a contentious term in the information systems literature. In our paper, we use the term to refer to the applicability of research findings to other threat-specific security actions as mandated by the ISP. This use most closely aligns with Tsang and Williams' (2012) idea of theoretical generalization and Lee and Baskerville's (2003) idea of generalizing from description to theory. Although Williams and Tsang (2015) argue that these two views of generalization are incompatible, the semantics of that debate are not germane to our discussion of universal versus particular models of ISP compliance.

[6] For our analyses, we refer to universal models as models that are expected to affect all (or most) security behaviors contained in the ISP, whereas particular models refer to a threat-specific security action as dictated by the ISP.

[7] Phishing uses authentic-looking electronic messages to trick users into revealing personal or confidential information. Tailgating is the act of gaining access to a restricted area by piggybacking someone who has legitimate access. Flash media involves plugging thumb drives or external hard drives into USB ports. Workstation locking involves locking a computer such that a user must enter a password in order to use the machine. Password sharing

across four theories: (1) theory of planned behavior (TPB), (2) protection motivation theory (PMT), (3) rational choice theory (RCT), and (4) deterrence theory (DT). In both empirical studies, we found some similarities but many significant differences in the behavioral antecedents (and model fit statistics) using each of these theoretical perspectives. For instance, we found that attitudes, perceived threat severity, perceived costs of compliance, perceived benefits of compliance, and perceived costs of noncompliance vary from threat to threat and according to general compliance intentions. Therefore, researchers should be cautious about making the following claims of generalization: (1) generalizing models measuring general compliance intentions to all threat-specific security compliance intentions; (2) generalizing threat- specific models to other threat-specific security actions; and (3) generalizing threat-specific models to general compliance intentions. As such, we claim that it may not be empirically possible or conceptually desirable to construct a model of general ISP compliance that covers the variety of threat-specific security actions covered by typical ISPs.

Our primary contribution to the literature is to challenge conceptually and empirically the idea of general ISP compliance. Our literature review reveals that prior top-tier ISP compliance research has spent significant time discussing the measurement of general ISP compliance across all or most of the ISP document, but much less time defining what a general model of ISP compliance is conceptually capturing. What does it mean when an employee generally plans to follow all (or most) of the policies and procedures contained in the ISP document? Conceptually, the extant literature has not clearly answered this question. However, prior literature on this topic has determined precise measurement (i.e., aggregating different threat-specific security vignettes or using generic measures related to an undefined security action) for this ill-defined concept. Before determining how to specifically measure general ISP compliance, we argue that it is first necessary to have a sound conceptual definition, which is lacking in many of the seminal ISP compliance papers. Furthermore, we question if it is necessary to have the same set of behavioral antecedents for all (or most) threat-specific security actions contained in an ISP? We argue that the answer to this question is no, because not all security-related actions covered by the ISP are the same. Forcing a universal model on all ISP-related behaviors masks the important threat-to-threat differences that are prevalent across the broad spectrum of ISP-related security actions.

involves sharing a personal password with a co-worker, contractor, or other individual.

2 Particular versus Universal

Many information systems (IS) scholars argue that the primary objective of social science research is to reveal broad generalities of social life (Cheng, Dimoka, & Pavlou, 2016; Tsang, 2014). That is, high- quality social science theories or models have universal applicability (universalism), whereas low- quality social science theories or models are applicable to a narrow context (particularism). However, it is certainly questionable if good science, as it relates to IS (or any other scientific discipline), has to be linked with perceptions of the level of generalization (Lee, 1991; Siponen & Tsohou, 2018; Straub, Boudreau, & Gefen, 2004). This idea has been debated since the founding of the IS discipline (Davison & Martinsons, 2016; Keen, 1980; Lee & Baskerville, 2003; Tsang & Williams, 2012). On the one hand, IS scholars want to uncover relationships that seemingly impact a wide range of technological and IS phenomena, which can be broadly applied to other IS and technological problems that individuals and organizations encounter (Cheng et al., 2016; Tsang & Williams, 2012). These purportedly universal constructs and relationships provide useful starting points for future research related to a wide range of IS problems. On the other hand, however, the adoption and use of IS is typically a unique endeavor. The industry, organizational or national culture, and the characteristics of the technology all affect the potential success or failure of an IS endeavor (Fernandez, 2016; Levina & Orlikowski, 2009; Sarker, 2016; Su, 2015).

IS is not unique in struggling with this generalizability conundrum (Grover & Lyytinen, 2015; Hanisch, Hulin, & Roznowski, 1998; Johns, 2006). Little (1998, pp. 96-98) argues that any social science discipline that involves human agency struggles with generalization because human behaviors are formed based on norms and values that are interpreted differently from culture-to-culture, society-to-society, organization-to-organization, and individual-to-individual. As such, models explaining the variance in human behaviors involve significant boundary conditions, contextual factors, social forces, and situational constraints that limit empirical and theoretical generalization (Bunge, 1998, p. 227; Lee & Baskerville, 2003; Walsham, 1995). Despite this widely recognized issue, however, social scientists (including ISP compliance researchers) tend to be quite cavalier about specifying where their models or theories will hold (Szostak, 2003, p. 33). This practice may have become the norm because these boundary conditions are perceived as research limitations or weaknesses in many social science disciplines, which can significantly limit the ability to publish research papers in these fields

(Suddaby, Hardy, & Huy, 2011). Yet, these boundary conditions may foster stronger model development and strengthen research validity; thus, the perception that boundary conditions are study limitations or weaknesses is questionable (Busse, Kach, & Wagner, 2017).

As ISP compliance researchers, we model general compliance behaviors, or ISP-directed threat-specific security behaviors (Moody et al., 2018).[8] Then, we speculate whether our models have a universal or a particular level of generalization. For example, a universal model of ISP compliance would be the universal application of PMT across all individuals associated with any threat-specific security action. In this type of universal model, the path coefficients (magnitude, sign, and significance) as predicted by PMT are theorized to be the same across all (or most) ISP-related behaviors. For example, Johnston and Warkentin (2010, p. 550) specifically state that "study findings should be generalizable to the impact of fear appeals in all decentralized environments in which end users exercise some degree of autonomous control over IT resources."[9] While they have a small caveat associated with "decentralized environments," they suggest a rather universal level of generalizability associated with their PMT model.

In contrast, a particular model of ISP compliance is a model that is specific to a certain threat-specific security action as dictated by the ISP document. For instance, a particular model could investigate an instantiation of PMT to help explicate behavioral reliance and actual performance using a fake website detection tool (Zahedi, Abbasi, & Chen, 2015). The path coefficients may be similar to or different from the path coefficients for other threat-specific security actions, even though both may be using PMT. This type of model simply attempts to solve the problems associated with a single threat-specific security action (or intentions thereof). Potentially, the level of generalization in this type of particular model for other organizations with similar ISPs, trainings, sanctions, and security cultures may be related to a single threat-specific security action contained in the ISP. This type of particular model would not explicitly attempt to generalize to any other threat-specific security action or policy-mandated behavior contained in the ISP.

3 Basket Journal Literature Review

We reviewed all of the literature in the senior IS scholars' basket of journals related to ISP compliance.[10] Although this basket of journals narrows the scope of ISP compliance literature, we used this basket of journals because these publications determine the direction of the field. If our top journals have a tendency to publish purportedly universal as opposed to particular models of ISP compliance, then this signals to the rest of the research community that future ISP compliance research should investigate widely generalizable models if those researchers want to get their papers published in the best IS journals. Furthermore, if this senior IS scholars' basket of journals has a preference for specific types of papers based on certain rigid beliefs concerning what constitutes good or exceptional scientific research in the ISP compliance space, then these issues need to be highlighted, debated, and discussed.

We determined the papers for our literature review by independently searching for the keywords "security," "policy," "ISP," and "compliance" from each journals' inception date through April 2018. We performed this keyword search on the publication titles, abstracts, and author-submitted keywords. We then manually read each paper that was identified via the keyword search to determine if each paper investigated behavioral ISP compliance issues as opposed to technical or end-user information security issues. The final step in our review process was to backward and forward trace the citations for each journal that we previously identified in order to ensure that we did not miss a basket journal article (Webster & Watson, 2002). Following this process, we identified 25 relevant papers. We then classified each of the 25 papers based on the implicit or explicit scope of generalization and the type of evidence used to make those generalization claims. We did this in a data-driven manner, similar to the approach taken by Vaast et al. (2013), in which we let our analysis of the data determine the groupings.

[8] In the ISP compliance research context, we do not build theories per se. We construct models using theories that were developed in other disciplines. For example, numerous ISP compliance researchers have used PMT or DT to model a variety of ISP-related behaviors but these theories were not developed by ISP compliance researchers. Therefore, we use the term model instead of theory in our paper.

[9] Interestingly, Johnston and Warkentin (2010) investigated a single security action (spyware) in their study. In their discussion section, however, they claim their spyware evidence should be somewhat universal across all other security actions (as evident by this quotation). We discuss type of evidence used to make claims of generalization in the next section of the paper.

[10] To be considered in our review, the research must focus on an ISP and compliance with the rules and regulations associated with that ISP. Well-cited end-user behavioral information security papers such as Anderson and Agarwal (2010), Boss et al. (2015), and Chen and Zahedi (2016) are not included in our review because the focus of those papers is on end-user information security behaviors and not ISP-directed behaviors.

Table 1. IS Senior Scholars' Literature

	Scope of generalization[a]		
	ISP-related behavioral information security research		
Measurement items (empirical evidence)	Universal (all ISP-directed actions)	Pseudo-universal (many but not necessarily all ISP-directed actions)	Particular (threat-specific security action such as phishing)
Generic measures (i.e., "I intend to comply with the requirements of the ISP")[b]	9	0	0
Threat-specific measures (i.e., "I intend to comply with the tailgating requirements in the ISP")[c]	4	0	2
Scenario vignettes (i.e., present the research subjects with a hypothetical scenario related to a threat-specific security action)	3	5	0
Qualitative (i.e., case study of one or more particular workplaces or organizational settings)	1	1	0

[a] Two researchers determined the implicit or explicit scope of generalization from the framing of each paper in the introduction, hypothesis development, and discussion sections.
[b] These measures generally refer to all required actions as directed by the ISP. These measures are not capturing a specific action or specific type of ISP violation.
[c] These measures refer to a single threat-specific security action contained in the ISP.

Using this process, we identified three categories related to generalization: (1) universal (generalizing to all ISP-related actions), (2) pseudo-universal (generalizing to more than one but not necessarily all ISP-related actions), and (3) particular (not attempting to generalize beyond the threat-specific security action that was investigated). We also identified four types of empirical evidence used to make the claims of generalization: (1) generic measures (i.e., undefined security action), (2) threat-specific measurement items, (3) threat-specific scenario vignettes, and (4) qualitative case studies. Table 1 summarizes the results of our literature review. Appendix A provides additional details concerning each paper in our literature review.

From a generalizability perspective, this basket of journals strongly prefers to publish papers that attempt to construct broadly generalizable models of ISP compliance. In total, 92% (23/25) of the studies in our literature review explicitly or implicitly attempted to construct universal or pseudo-universal models of ISP compliance across all or many threat-specific security actions contained in the ISP. A pseudo-universal model generally assumes that if a research model is empirically demonstrated to affect more than one (usually two) ISP-related actions in a similar manner, then it has a higher likelihood of being generalizable to all (or most other) ISP-related actions. In this research context, if the paper cannot reasonably be assumed to affect multiple (probably most) threats and mitigating controls contained in the ISP, then it appears to have a low probability of being published in this basket of journals. On the one hand, this practice makes sense because this basket of journals is designed for a general audience. Papers published in these outlets can be cited by a wide variety of future research both within and outside of the ISP compliance space.

On the other hand, however, this practice is problematic when the variety of behaviors in a specific domain are highly variable, which might negatively affect the application of generic research models to alternative contexts. We suggest that there is such behavioral variability in the ISP compliance space due to the variety of attacks and threats that employees are required to guard against on a daily basis. Therefore, we assert that it might not be plausible to construct a single model that covers all of the policies and procedures contained in an ISP document. To exemplify this issue, we consider an example of the US tax code. Is it possible to apply a single theory to model an individual's propensity to follow all (or most) of the income tax rules and regulations contained in the US tax code? Given the depth and breadth of the US tax code, the answer is probably no. For instance, one model may adequately explain compliance with depreciation rules but inadequately explain compliance with capital gains regulations. Even with advanced tax prep software, different amounts of diligence and thought are required to comply with different sections of the tax code, which makes it problematic to construct a single model for all (or most) of the tax code.

Similarly, in the ISP compliance context, we proffer that one set of behavioral antecedents may explain the majority of the variance for a high-effort threat-specific security action, whereas a different set of behavioral antecedents may be better at explaining the variance for a low-effort threat-specific security action. Despite these behavioral differences across security actions, however, our literature review reveals that having the perception of broad generalization is a key hurdle that authors must clear in order to publish ISP compliance papers in one of our top journals. From a measurement perspective, researchers attempted to make these universal claims of generalization in one of the following ways: (1) ask generic (i.e., undefined security action) questions concerning the ISP and generalize down to specific actions; (2) aggregate responses to questions concerning multiple ISP-related threat-specific security actions; (3) aggregate scenario vignettes concerning multiple ISP-related threat-specific security actions; or (4) qualitatively evaluate ISP compliance via case studies. Figure 1 displays our interpretation of the empirical evidence and the scope of generalization used in the prior ISP compliance literature.

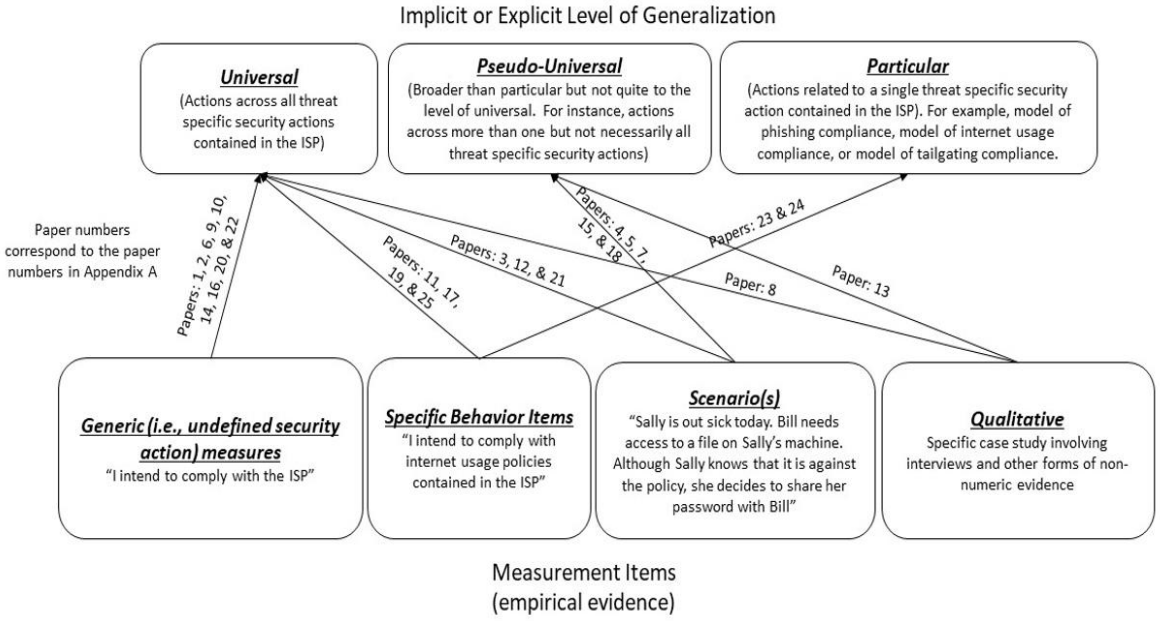

Figure 1. Empirical Evidence to Level of Generalization

3.1 Generic Measures

These measures refer to the ISP document as a whole (i.e., compliance with all, most, or many of the policies contained in the ISP document without referring to a specific policy, threat-specific security action, mitigating control, or countermeasure). Of the 17 papers that attempted to construct universal models of general ISP compliance, 53% (9/17) of them used generic measures not specific to any policy or security threat. Many of these papers did not provide any type of justification for why a generic measure was used besides citing a prior study as their justification. Of the papers that did explicitly justify why they chose to measure compliance using generic measures, the reason given was that a single threat-specific security action would potentially inhibit understanding of individuals' abilities to perform multiple security behaviors simultaneously (Crossler & Bélanger, 2014; Posey et al., 2013). Based on this justification, it is unclear what types of security actions employees are performing simultaneously because the measurement items refer to an undefined set of security actions. Siponen and Vance (2014) used an analogy of traffic violations to argue that most individuals will probably indicate that they will, in general, follow the traffic rules, but they might not know all of the traffic rules when asked questions about specific rules of the road.

We again consider our example of the US tax code to further exemplify the pitfalls with using these types of generic measures. We assume that most individuals, if asked, would indicate that they generally follow tax rules, but the US tax code is complicated. Therefore, if asked a direct question or presented with a scenario specifically concerning the depreciation schedule for an asset or the rules for a home deduction as a part of a small business expense, individuals would probably answer those questions differently due to the contextual differences between those two tax policies. There may be significant variability in the behavioral antecedents and underlying behavioral intentions from

rule to rule. We suspect that ISP compliance research using generic measures without grounding the questions with a threat-specific security action (or a specific mitigating control) will encounter similar issues due to the wide range of threat-specific security actions covered by a typical ISP. Therefore, we argue that it is difficult to derive any actionable conclusions from these types of generic measures because they do not capture any threat-specific security actions that are contained on the ISP document. If anything, we assert that these generic measures average out the effects across the ISP, which means that they are "on average" wrong (Savage, 2012, pp. 15-19).

3.2 Specific Behavior Items

Another measurement technique that papers in our top journals use to attempt to construct universal models of general ISP compliance is to capture responses for a threat-specific security action and generalize out to all (or most) other policies in the ISP. This type of measure captures specific behavioral intentions concerning, for instance, Internet usage (e.g., "I intend to comply with the Internet usage policies"), tailgating, phishing, or password-management ISP-directed behaviors. These measures capture one specific policy in the ISP document without contextualizing the security action to any specific type of situation (Moody et al., 2018). In our literature review, we found six papers that used this type of evidence and 66% (4/6) of them attempted to construct a universal model of ISP compliance using these types of specific behavioral items (i.e., the researchers saw evidence related to a single threat-specific security action and argued that other ISP-mandated actions would be similar).

We assert that generalizing from a measure that captures a single threat-specific security action to all (or most) other policies contained in the ISP is problematic because not all policies require the same amount of time, difficulty, diligence, knowledge, and effort to comply (Posey et al., 2013; Workman et al., 2008). These threat-to-threat differences may make the behavioral antecedents with each threat-specific security action different. For instance, we would not reasonably expect the behavioral antecedents associated with a socially interactive threat such as tailgating to have the same impact on compliance actions (or intentions thereof) as an individualized threat such as improper Internet usage (Aurigemma & Mattson, 2017). We argue that these two threat-specific security actions may or may not have overlapping behavioral antecedents because the policy-directed actions across both threats are different, which makes creating a universal model of ISP compliance from this type of evidence problematic.

3.3 Scenario Vignettes

Another type of evidence that ISP compliance researchers have used to develop universal or pseudo-universal models of ISP compliance is scenario vignettes. With this type of evidence, researchers develop a scenario vignette with a threat-specific security action and ask their research subjects to respond to the specific scenario. Many times, researchers ask their research subjects to respond to multiple scenario vignettes with different threat-specific security actions. Then, the researchers either aggregate all of the specific threats to a single metric or attempt to explain how their single threat-specific security action was representative of all, most, or many other threat-specific security actions contained in the ISP.

For example, D'Arcy, Hovav, and Galletta (2009) justified their examination of composite behaviors in that the focus of their research was to explore generalized patterns of information system misuse instead of individual threat responses. By aggregating individual behavioral responses via the scenario vignettes, they argued that researchers may be able to predict generalized patterns of deviant behavior better than by collecting data on generic measures (D'Arcy et al., 2009). This argument may be valid, but if researchers are aggregating threats that require different actions, then we assert that they are essentially smoothing or averaging out the effects. We therefore question what, exactly, this smoothed-out aggregated metric of different threat-specific security actions is measuring. Similar to the generic measures of ISP compliance, we are not sure that this aggregation is capturing anything meaningful. If there is conceptual value in this type of aggregation, then what does it mean if the threats being aggregated are not representative of all types of threat-specific security actions required by the ISP? Most researchers would probably agree that aggregating a nonrepresentative sample of threat-specific security actions or aggregating vastly different security-related actions would be a problematic metric for any type of security-related behavior.

Interestingly, most of the research in our literature review that investigated a single threat-specific security action via a scenario vignette or a specific behavior item explicitly recognized the limitation of constructing a universal model of general ISP compliance from a single threat-specific security action. For example, Johnston et al. (2016, p. 245) stated that "to some extent, the choice of one behavior limits the generalizability of the findings to other security misbehaviors" while still attempting to construct a rather universal model. Appendix A includes similar statements from most of the studies that investigated one or two threat-specific security actions while still attempting to construct a universal

model. Why is the research context a study limitation or a study weakness? A study limitation or weakness is, for example, having a biased sample, having an inadequate manipulation or an inadequate manipulation check, using incorrect statistical models, employing an unsystematic data gathering process, and making faulty mathematical assumptions (Lee, 1991). We posit that the specific ISP-related problem that is being investigated is not a study limitation. We would argue that solving one ISP-related problem well is theoretically more valuable than attempting to solve all ISP-related problems too generically. It is only perceived as a study limitation because our top journals have a strong preference for publishing universal models of ISP compliance instead of particular models related to a threat-specific security action.

3.4 Qualitative Case Studies

Two studies in our literature review used qualitative data to attempt to construct universal or pseudo-universal models of ISP compliance (Hedström, Kolkowska, Karlsson, & Allen, 2011; Kolkowska, Karlsson & Hedström, 2017). Qualitative data can be a rich source of nonnumerical data that researchers can use to make a variety of scientific conclusions (Klein & Myers, 1999; Lee, 1991). For our context, qualitative interviews can be used to gather data on generic ISP behaviors (undefined security actions) or threat-specific security actions. Both the Hedström et al. (2011) and Kolkowska et al. (2017) papers investigated or proposed to investigate specific (actual) security behaviors via qualitative means in order to construct rather broad models of ISP compliance.[11] These two qualitative papers were particular in terms of industry (health care industries) but universal (or pseudo-universal) in terms of the types of ISP-related actions covered by their models.

4 Research Design and Methods

To empirically evaluate the challenges associated with constructing a universal model of ISP compliance from either generic measures or threat-specific security measures, we conducted two empirical studies comparing general compliance intentions (i.e., undefined security action) and threat-specific compliance intentions. In order to make these comparisons, we evaluated behavioral intentions across multiple threat-specific security actions and multiple theories. The threat-specific security actions that we investigated were phishing, tailgating, flash media, workstation locking, and password sharing.

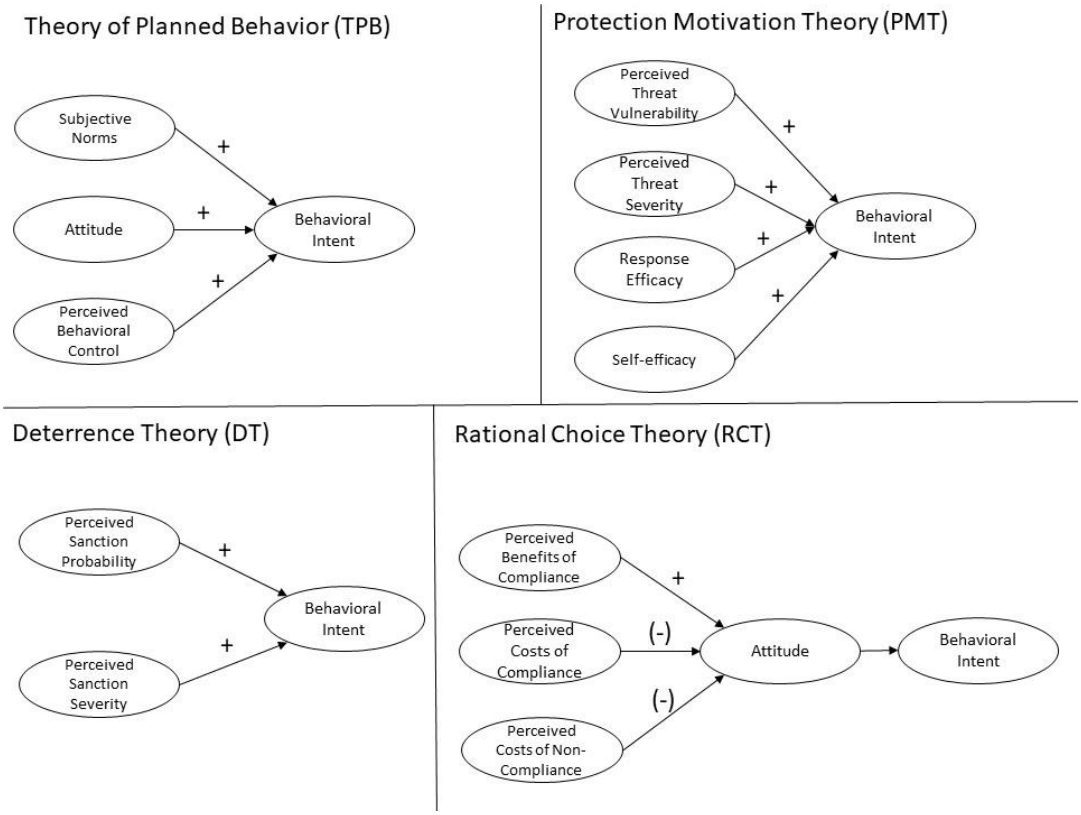

Figure 2. Theoretical Models

[11] Both of these papers were careful in stating how they could generalize their findings in their methods' sections. However, they were much more liberal with their generalization statements in their discussion sections.

Table 2. Theory and Conceptual Descriptions of the Constructs

Theory	Construct	Definition
The theory of planned behavior (TPB) posits that individual behaviors are determined by personal attitudes (feeling of favorability or desirability) towards the behavior, subjective norms (perceived social pressures from co-workers) to perform a behavior, and perceived behavioral control (a belief that the action can be performed given reasonable obstacles) over the specific behavior (Ajzen, 1991).		
TPB	Behavioral intent (BINT)	Intention to perform a security-related behavior.
TPB	Subjective norms (SNORM)	The perceived social pressure to engage or not to engage in a security-related behavior. Items adapted from Taylor and Todd (1995), Herath and Rao (2009)
TPB	Attitude (ATT)	The self-reported degree to which performance of a security behavior is positively or negatively valued. Items adapted from Ajzen (1991); Herath and Rao (2009)
TPB	Perceived behavioral control (PBC)	One's perceived ability to perform a given behavior in the presence of factors that may facilitate or impede performing the behavior. Items adapted from Taylor & Todd (1995)
In its simplest form, protection motivation theory (PMT) consists of an employee's self-efficacy (belief in one's ability) to perform a security action, the perceived response efficacy (perceived effectiveness) of the required action, the perception of their vulnerability (perceived likelihood that the threat will occur) from the related security threat, and the perceived severity (perceived impact of the threat) of the security threat being studied (Warkentin, Johnston, Shropshire, & Barnett, 2016).		
PMT	Self-efficacy (SEFF)	One's perceived ability to successfully complete a security-related behavior. Items adapted from Bandura (1991); Herath & Rao (2009)
PMT	Response efficacy (REFF)	The extent one believes a recommended security response effectively deters or mitigates a threat. Items adapted from Rippetoe & Rogers (1987), Milne et al. (2000), Workman et al. (2008)
PMT	Perceived vulnerability (PVUL)	One's belief in how susceptible they feel to a specified security threat. Items adapted from Champion (1984), Ng et al. (2009)
PMT	Perceived threat severity (TSEV)	One's perception of how serious a security threat would be to themselves. Items adapted from Ng et al. (2009)
Deterrence theory (DT) posits that a person weighs the probability of being caught (sanctioned) and the severity of the sanction in determining whether they will violate a mandate (Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005)		
DT	Perceived sanction severity (SSEV)	One's perception of how serious a penalty they would incur if they did not behave in accordance with formal security requirements. Items adapted from Herath & Rao (2009)
DT	Perceived sanction probability (SPROB)	The perceived chance that one would get caught and punished for violating a required security behavior. Items adapted from Herath & Rao (2009)
Rational choice theory (RCT) proffers that the 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).		
RCT	Perceived cost of compliance (PCOMP)	An estimate of the resources required and/or negative effects that result from complying with a required security behavior. Items adapted from Bulgurcu et al. (2010)
RCT	Perceived benefit of compliance (PBEN)	An estimate of the personal rewards received from complying with the required security behavior. Items adapted from Bulgurcu et al. (2010)
RCT	Perceived cost of noncompliance (PNCOMP)	An estimate of the negative effects that result from failing to comply with the required security actions. Items adapted from Bulgurcu et al. (2010)

These threat-specific security actions required different levels of time, difficulty, diligence, knowledge, and effort to comply with the ISP requirements, which provided us with sufficient behavioral variability to test threat-to-threat differences.[12] Appendix B contains the detailed policy directed behaviors for these threat-specific security actions in the two organizations that we studied. We also tested a generic measure of ISP compliance to compare whether the threat-specific security actions differed from generic ISP-related behaviors (or intentions thereof).

We evaluated the different ISP-directed security actions and the generic measure of ISP compliance across four theories: (1) theory of planned behavior (TPB), (2) protection motivation theory (PMT), (3) rational choice theory (RCT), and (4) deterrence theory (DT). Existing ISP research has relied on a number of theories such as (among many others) neutralization theory, theory of interpersonal behavior, control balance theory, DT, TPB, PMT, and RCT in order to explain the variability in ISP-related behaviors (Crossler & Belanger, 2014; Moody et al., 2018). Researchers in this space have not agreed on which theory (or version of a theory) is the most appropriate to use for a specific situation, context, organization, ISP, sample, and threat-specific security action. In our paper, we used DT, TPB, PMT, and RCT because many of the most commonly used constructs reported in the prior literature are contained in at least one of these theoretical models. We make no claims that every construct that has been reported in the prior literature is contained in DT, TPB, PMT, and RCT. However, these four theories provide ample theoretical diversity to objectively test model fit, explanatory power, path sign, magnitude, and significance across the different threat-specific security actions as mandated by the ISP. Figure 2 shows the versions of each theory we used to investigate differences between general compliance and threat-specific security actions. Table 2 contains a brief textual description of each theory and the conceptual definitions of each construct contained in each theory.

5 Study 1

In Study 1, we compared phishing, tailgating, flash media, and a generic (undefined security action) measure of ISP compliance across TPB, PMT, DT, and RCT using a sample of US Department of Defense (DoD) employees (military and civilian). Using the same survey instrument, we evaluated employees' self-reported intent to comply with the ISP requirements for phishing, tailgating, flash media, and a generic measure of ISP compliance. Based on the DoD ISP requirements, these three threat-specific security actions plus the generic measure of ISP compliance represent requirements for low interpersonal interactivity (phishing), high interpersonal interactivity (tailgating), situational interpersonal interactivity (improper flash media use), and indeterminate interpersonal interactivity (generic measure of ISP compliance). Each threat-specific security action also requires variable amounts of time, difficulty, diligence, knowledge, and effort to comply with the ISP-directed requirements. Appendix B displays the DoD's requirements for each one of these threat-specific security actions, which shows the behavioral differences across each threat-specific activity. These differences provided us with the variance in ISP-directed behaviors necessary to test differences across the different theories and threat-specific security actions.

At the time of our data collection, the DoD employed approximately 3.5 million military and civilian personnel. Every DoD employee (military and civilian) fell under the purview of the same ISP guidelines. At the time of our study, the DoD's ISP contained policies and procedures relating to 26 specific threats and their associated mitigating security actions. All participants in our study were required to pass an annual test with a 70% passing threshold concerning their ISP requirements in order to gain and maintain access to DoD electronic systems. Therefore, the presence of a codified set of ISPs, a robust security awareness and training program, an annual test pertaining to the ISP, and an organizational leadership that values the importance of information security made the DoD an excellent organization to test different models of ISP compliance.

5.1 Primary Data Collection

We adapted all of our measurement items from prevalidated scales taken from previous research.[13] Appendix B contains all of our measurement items. We measured all items reflectively using 7-point Likert scales. The order of the questions was randomized for each survey participant. Each survey participant answered all of the questions pertaining to the three threat-specific security actions and the generic measures. Our study participants had the option of completing the survey either online or on paper. We designed and administered the survey using best practices related to instruction wording (pp. 65-105)

[12] In addition to selecting these threat-specific security actions because the ISP mandated requirements were different, we also selected these actions based on our conversations with the senior IS leadership at the two organizations that we studied. These leaders informed us that they saw (anecdotally) different patterns of compliance with these particular threat-specific security actions.

[13] We used prevalidated scales because we wanted to use the same/similar scales that have been used in the prior ISP compliance literature. We did confirm discriminant and convergent validity on these scales for our dataset.

and question order (pp. 157-165) by Dillman et al. (2014). Additionally, in order to remedy potential common method bias procedurally via our instrument, we introduced a proximal separation between the measures of the independent and dependent variables along with using both positive and negative line items in our survey instrument (Podsakoff, MacKenzie, & Podsakoff, 2012). We piloted the survey instrument twice. The first pilot was with three DoD security management practitioners and the second pilot was with 20 DoD personnel and academics. As a result of each pilot, we made minor changes to the organization, structure, and content of the survey instrument.

A total of 1,380 DoD employees had the opportunity to participate in the final survey. Participation was completely voluntary and participants were assured of their anonymity (i.e., we obtained no identifying information during data collection). None of these survey participants received any monetary compensation for participating. After follow-ups, we collected a total of 239 completed surveys. Another 15 participants had a random collection of missing responses throughout their survey. For these 15 participants, we used the full information maximum likelihood (FIML) method in MPlus (v8) (Kline, 2016, p. 86). Therefore, our final analysis included 254 data points (67 enlisted, 115 officers, and 72 civilians).[14] To compare potential instrument bias between paper (n=50) and online (n=204) testing, we ran ANOVAs between the two groups of responders on each variable, which revealed no aggregate construct level differences, but there were several individual item differences. Finally, we successfully screened our 254 data points for issues that may have jeopardized our results, such as outliers, multicollinearity, and nonnormality (Kline, 2016, pp. 71-77).

5.2 Data Analysis and Results

We analyzed our research models using covariance-based structural equation modeling (CBSEM) (MPlus v8). Due to the nature of our data collection (i.e., cross-sectional data during the same time period collected via a self-reported questionnaire), common method variance attributed to measurement method instead of the constructs of interest may have biased our results (Podsakoff et al., 2012). To test for common method variance, we used the unmeasured latent method construct (ULMC) factor approach discussed by Podsakoff et al. (2012). Comparing the standardized loadings of the items on their respective constructs between CFAs with and without the ULMC marker construct, the average difference across all items' standardized loadings was less than 0.01 (with a maximum difference of 0.07) and none of the measured construct items loaded significantly on the marker construct. Additionally, the average variance extracted (AVE) from the ULMC in all threat conditions was less than 0.06, which indicated that the ULMC contributed very little of the overall variance explained by the CFA model. While the results of the ULMC analysis and the above design choices do not negate the possibility of bias, we did not find evidence of common method variance in our dataset.

We performed a separate confirmatory factor analysis (CFA) for each threat-specific security action and for the generic measure because we tested each separately. Table 3 displays our CFA results. Based on the criteria set forth by Petter, Straub, and Rai (2007), all of the construct measures met the requirements to be considered reflective indicators of their respective latent constructs for all three threat-specific security action measures plus the generic measures. While the recommended threshold for item loadings is 0.7, individual item loadings between 0.40 and 0.70 are acceptable for inclusion as long as composite reliabilities are above 0.70, which they were for all of our measurement items (Chin, 1998). The average variance extracted (AVE) is a measure of the amount of variance that is captured by a construct in relation to the amount of variance due to measurement error; AVE values above 0.5 are evidence of convergent validity, which was the case for our data (Fornell & Larker, 1981; Gefen & Straub, 2005). We verified discriminant validity across all three threat-specific security action measures plus the generic measures by comparing the difference between the AVE of each construct and its correlations with other constructs. To achieve sufficient discriminant validity, the square root of AVE of a construct should be greater than its correlations with all other constructs (Gefen & Straub, 2005), which was the case for all of our constructs (i.e., see the diagonal in Table 3).

Next, we evaluated the model fit for the CFA analysis, which included all latent constructs tested simultaneously across our four models: generic measures ($\chi^2 = 984.7$, $df = 587$, $p = 0.12$,[15] CFI = 0.947, RMSEA = 0.054), tailgating ($\chi^2 = 1314.3$, $df = 587$, $p = 0.31$, CFI = 0.906, RMSEA = 0.073), phishing ($\chi^2 = 1171.1$, $df = 587$, $p = 0.22$, CFI = 0.924, RMSEA = 0.065), and flash media use ($\chi^2 = 1190.2$, $df = 587$, $p = 0.21$, CFI = 0.924, RMSEA = 0.067).

[14] We could not determine how many of the 1,380 potential participants actually received the survey requests or the follow-ups (i.e., the emails may have been filtered to spam and/or were never opened by the potential participants).

[15] We report the Bollen-Stine p value (with 1000 bootstrap iterations) and Yuan-Bentler corrected χ^2 values in our paper because our data were not perfectly normal and deviations from normality have been known to inflate the chi-square values (Bollen & Stine, 1992).

Table 3. CFA Validity and Construct Correlations for Study 1

Generic Measure	CR	AVE	PBEN	BINT	SEFF	PVUL	TSEV	REFF	SNORM	PBC	ATT	SSEV	SPROB	PCOMP	PNCOMP
PBEN	0.809	0.589	0.767												
BINT	0.979	0.939	0.372	0.969											
SEFF	0.960	0.889	0.250	0.472	0.943										
PVUL	0.936	0.830	0.119	0.120	0.069	0.911									
TSEV	0.939	0.836	0.364	0.374	0.259	0.324	0.914								
REFF	0.898	0.746	0.470	0.342	0.304	-0.004	0.340	0.864							
SNORM	0.804	0.581	0.376	0.654	0.400	0.004	0.227	0.415	0.762						
PBC	0.889	0.727	0.430	0.478	0.797	0.104	0.217	0.278	0.440	0.853					
ATT	0.946	0.854	0.349	0.612	0.668	0.041	0.242	0.306	0.556	0.622	0.924				
SSEV	0.771	0.529	0.378	0.275	0.198	0.049	0.303	0.570	0.380	0.303	0.202	0.727			
SPROB	0.770	0.628	0.407	0.298	0.123	0.028	0.232	0.598	0.333	0.163	0.220	0.635	0.792		
PCOMP	0.900	0.753	-0.203	-0.186	-0.259	0.157	-0.097	-0.250	-0.199	-0.266	-0.185	0.023	-0.110	0.868	
PNCOMP	0.788	0.554	0.672	0.303	0.126	0.130	0.454	0.521	0.237	0.193	0.169	0.556	0.473	0.007	0.744
Phishing	CR	AVE	PBEN	BINT	SEFF	PVUL	TSEV	REFF	SNORM	PBC	ATT	SSEV	SPROB	PCOMP	PNCOMP
PBEN	0.810	0.589	0.767												
BINT	0.966	0.904	0.365	0.951											
SEFF	0.976	0.933	0.322	0.444	0.966										
PVUL	0.922	0.798	0.118	0.157	0.090	0.893									
TSEV	0.940	0.838	0.403	0.391	0.166	0.322	0.916								
REFF	0.900	0.750	0.447	0.296	0.249	-0.225	0.228	0.866							
SNORM	0.834	0.628	0.364	0.665	0.418	0.070	0.261	0.317	0.792						
PBC	0.875	0.700	0.396	0.514	0.779	0.011	0.244	0.377	0.520	0.837					
ATT	0.936	0.829	0.417	0.606	0.592	-0.021	0.323	0.389	0.501	0.711	0.911				
SSEV	0.816	0.596	0.416	0.179	0.169	-0.095	0.244	0.572	0.294	0.282	0.293	0.772			
SPROB	0.786	0.650	0.412	0.227	0.153	-0.013	0.204	0.457	0.221	0.183	0.318	0.641	0.806		
PCOMP	0.933	0.822	-0.222	-0.239	-0.325	0.041	-0.149	-0.148	-0.226	-0.313	-0.224	0.033	-0.052	0.907	
PNCOMP	0.785	0.551	0.619	0.288	0.136	0.102	0.449	0.456	0.288	0.131	0.197	0.519	0.484	-0.037	0.742
Removable Flash Media	CR	AVE	PBEN	BINT	SEFF	PVUL	TSEV	REFF	SNORM	PBC	ATT	SSEV	SPROB	PCOMP	PNCOMP
PBEN	0.865	0.681	0.825												
BINT	0.982	0.949	0.305	0.974											
SEFF	0.971	0.919	0.203	0.534	0.959										
PVUL	0.911	0.776	0.139	0.164	0.037	0.881									
TSEV	0.937	0.832	0.365	0.286	0.206	0.230	0.912								
REFF	0.892	0.735	0.438	0.187	0.288	-0.008	0.253	0.857							
SNORM	0.848	0.657	0.442	0.648	0.302	0.036	0.109	0.341	0.810						
PBC	0.873	0.697	0.209	0.480	0.941	0.078	0.252	0.328	0.301	0.835					
ATT	0.956	0.878	0.418	0.579	0.463	0.117	0.315	0.309	0.569	0.523	0.937				
SSEV	0.772	0.532	0.325	0.254	0.236	-0.033	0.273	0.450	0.327	0.261	0.303	0.730			
SPROB	0.692	0.534	0.267	0.193	0.256	0.013	0.223	0.391	0.133	0.262	0.210	0.600	0.731		
PCOMP	0.883	0.717	-0.268	-0.237	-0.268	0.205	-0.072	-0.247	-0.210	-0.303	-0.363	-0.035	-0.009	0.847	
PNCOMP	0.779	0.543	0.558	0.230	0.218	0.039	0.524	0.365	0.150	0.231	0.201	0.538	0.446	-0.003	0.737
Tailgating	CR	AVE	PBEN	BINT	SEFF	PVUL	TSEV	REFF	SNORM	PBC	ATT	SSEV	SPROB	PCOMP	PNCOMP
PBEN	0.825	0.613	0.783												
BINT	0.942	0.844	0.495	0.918											
SEFF	0.964	0.898	0.238	0.499	0.948										
PVUL	0.925	0.805	0.062	0.067	0.082	0.897									
TSEV	0.941	0.843	0.350	0.180	0.139	0.330	0.918								
REFF	0.927	0.810	0.472	0.315	0.123	-0.119	0.192	0.900							
SNORM	0.850	0.658	0.478	0.738	0.331	-0.071	0.071	0.453	0.811						
PBC	0.872	0.695	0.280	0.388	0.853	0.165	0.166	0.162	0.301	0.834					
ATT	0.895	0.740	0.352	0.381	0.492	0.026	0.236	0.222	0.347	0.564	0.860				
SSEV	0.842	0.641	0.528	0.373	0.125	-0.070	0.259	0.728	0.447	0.180	0.288	0.801			
SPROB	0.817	0.692	0.388	0.353	0.100	-0.033	0.151	0.613	0.353	0.139	0.217	0.741	0.832		
PCOMP	0.940	0.840	-0.239	-0.205	-0.303	0.112	-0.121	-0.222	-0.247	-0.356	-0.219	-0.077	-0.044	0.916	
PNCOMP	0.831	0.623	0.624	0.370	0.107	0.054	0.399	0.512	0.329	0.176	0.156	0.558	0.446	-0.151	0.789

Composite Reliability (CR), Average Variance Extracted (AVE), Perceived Vulnerability to Threat (PVUL), Perceived Threat Severity (TSEV), Response Efficacy (REFF), Subjective Norms (SNORM), Perceived Behavioral Control (PBC), Attitude (ATT), Perceived Sanction Severity (SSEV), Perceived Sanction Probability (SPROB), Perceived Cost of Compliance (PCOMP), Perceived Cost of non-Compliance (PNCOMP)
Note: Off diagonal numbers are interconstruct correlations; diagonal numbers are the square roots of AVE (average variance extracted).

Then, following the two-step modeling approach recommended by Kline (2011, p. 267), we conducted nested model comparisons between the CFA and the structural models for each theory and threat condition. In these nested model comparisons, the chi-square difference test was not significant (passing) for all of the CFA-structural model tests for each theory and all threat-specific security actions. As a final data check, we conducted factor invariance tests between the different threat-specific security actions and the generic measures for all four theories to make sure that the items used in the survey instrument loaded on the same construct across the threats. These tests satisfactorily showed both configural and metric invariance, which enabled us to conduct the statistical tests between the groups (Kline, 2016, p. 396).

Table 4 and Table 5 display the CBSEM model results for all three threat-specific security actions plus the generic measures for all four theories. In accordance with the supporting theory for the model, we used three main criteria to compare each theoretical model in terms of the different threat-specific security actions and the generic measures of (1) model fit, (2) dependent variable variance explained (R^2), and (3) path coefficient magnitude, sign, and significance of the antecedent variables.

For model fit, Kline (2016, pp. 273-277) recommends reporting χ^2, degrees of freedom (*df*), and *p* values as this is the only true statistical test of CBSEM model fit; all other measures are called "approximate fit indices" and are considered descriptive in nature. However, "model fit can be assessed inferentially by the χ^2 test or descriptively by applying other criteria" (Schermelleh-Engel & Moosbrugger, 2003 p. 31). In the strictest interpretation, if the chi-square model fit test fails ($p < 0.05$), then that specific model has inadequate model fit. However, there are several shortcomings to the χ^2 test related to violation of χ^2 distribution assumptions (normality, multivariate normality, sufficient sample size) that are not normally met in many practical applications of CBSEM due to model complexity (Schermelleh-Engel & Moosbrugger, 2003). That said, some researchers warn against trying to justify retaining a model based solely on approximate fit statistics, especially if the model failed the chi-square test (Barrett, 2007).

Table 4. CBSEM Model Fit Results for Study 1

Model	χ^2	*df*	*p*	CFI	RMSEA
Theory of planned behavior					
Generic measure	96.638	48	0.359	0.983	0.065
Improper flash media	222.945	48	0.028	0.943	0.124
Phishing	249.525	48	0.01	0.927	0.133
Tailgating	214.511	48	0.141	0.922	0.121
Protection motivation theory					
Generic measure	140.591	80	0.222	0.984	0.056
Improper flash media	135.239	80	0.337	0.986	0.054
Phishing	109.538	80	0.471	0.992	0.039
Tailgating	168.488	80	0.166	0.975	0.068
Deterrence theory					
Generic measure	48.732	17	0.028	0.98	0.088
Improper flash media	29.218	17	0.232	0.992	0.055
Phishing	25.126	17	0.2	0.994	0.045
Tailgating	43.716	17	0.02	0.979	0.080
Rational choice theory					
Generic measure	113.943	83	0.429	0.989	0.039
Improper flash media	180.002	83	0.051	0.969	0.070
Phishing	165.400	83	0.112	0.971	0.065
Tailgating	183.842	83	0.138	0.959	0.072

Table 5. CBSEM Model Structural Path Results for Study 1

Model	Generic Measure	Improper Flash Media Use	Phishing	Tailgating
Theory of planned behavior				
R^2 (BINT)	0.528	0.526	0.544	0.588
SNORM → BINT	0.355***	0.326***	0.319***	0.487***
ATT → BINT	0.320***	0.169**	0.280***	0.089(NS)
PBC → BINT	0.059(NS)	0.191***	0.006(NS)	0.101 (p=0.08)
Protection motivation theory				
R^2 (BINT)	0.32	0.333	0.33	0.323
TSEV → BINT	0.111***	0.09**	0.118***	0.035(NS)
PVUL → BINT	0.005(NS)	0.037(p=0.074)	0.02(NS)	0.015(NS)
REFF → BINT	0.105*	0.007(NS)	0.084*	0.158***
SEFF → BINT	0.308***	0.494***	0.220***	0.471***
Deterrence theory				
R^2 (BINT)	0.101	0.074	0.055	0.155
SPROB → BINT	0.109*	0.053(NS)	0.084 (p=.066)	0.088(NS)
SSEV → BINT	0.068(NS)	0.105*	0.02(NS)	0.124*
Rational choice theory				
R^2 (BINT)	0.38	0.339	0.361	0.151
R^2 (ATT)	0.142	0.239	0.193	0.161
PBEN → ATT	0.157***	0.174***	0.225***	0.211***
PCOMP → ATT	-0.037(NS)	-0.133***	-0.053*	-0.06*
PNCOMP → ATT	-0.031(NS)	0.013(NS)	-0.032(NS)	-0.052(NS)
ATT → BINT	0.643***	0.500***	0.455***	0.438***

Notes: For ease of visually differentiating significant and nonsignificant path relationships in the CBSEM results, we used NS to signify not significant. *$p < 0.05$, **$p < 0.01$, ***$p < 0.001$.

BINT: Behavioral Intent, ATT: Attitude, PBC: Perceived Behavioral Control, SPROB: Perceived Sanction Probability, SSEV: Sanction Severity, SEFF: Self-Efficacy, TSEV: Perceived Threat Severity, PVUL: Perceived Vulnerability, REFF: Response Efficacy, PBEN: Perceived Benefit from Compliance, PCOMP: Perceived Benefit from Complying, PNCOMP: Perceived Cost from Noncompliance, NS: Not Significant ($p > 0.1$).

In our paper, we evaluated the performance of four established theoretical models of human behavior across a range of threat-specific security actions. Our goal was not to present a new model and justify its fit as good or bad or recommend changes to the underlying model. Instead, our goal was to compare how these baseline models vary within the same sample of participants while varying only the threat condition. Thus, we report both the χ^2 test results and approximate fit indices (CFI and RMSEA) to allow readers the opportunity to assess the results of our analyses both inferentially and/or descriptively. While there is debate on what constitutes a satisfactory threshold value for different fit indices, in this paper we use CFI > 0.90 and RMSEA < 0.10 as descriptive indicators of adequate model fit (see Schermelleh-Engel & Moosbrugger (2003) for a discussion on fit indices). It should be noted, however, that not all of the approximate fit metrics need to be below or above the recommended cutoffs for the overall model fit to be considered acceptable (Gefen et al., 2011). When comparing models with otherwise similar characteristics, the model with the better overall fit metrics is generally considered superior. In our data, both inferential and descriptive model fit varied widely by both theory and threat-specific security actions.

The model fit results for the TPB show the most variability (see Table 4). Only the models related to the generic measure (undefined security action) and tailgating threat-specific security action passed the χ^2 fit test. Additionally, the tailgating threat approximate fit indices were markedly worse than the generic measurement model (including an unsatisfactory RMSEA). What does this mean? If one were to evaluate generic measures alone for the TPB model, one could inaccurately conclude that the TPB model fit is acceptable for all threat-specific security actions, which is clearly not the case for both the flash media and phishing threat-specific security actions (and possibly for the tailgating threat-specific security action). When a model fails the inferential χ^2 test, a researcher may take steps to attempt to resolve the model fit issues, such as reexamining the data for distributional violations, deleting additional outlier data, dropping some items from construct measurement, or even changing the fundamental structure of the model (as long as this is theoretically justifiable) (Barrett, 2007). In our paper, however, we are trying to determine *if* model fit is different between threat conditions, not *why*. Thus, in our sample of the same participants surveyed with validated and consistent items related to well-established theoretical models, we can draw conclusions about generalization problems from the fact that model fit fails in one threat-specific security action but passes in another threat-specific security action or in the generic undefined security condition. Of the models evaluated, only PMT shows consistent inferential and descriptive model fit results across the threat-specific security actions and the generic undefined security condition.

Comparing the R^2 values across models allows us to determine which model explains the most amount of variance of our dependent variables. All other things being equal, the model with the highest R^2 is considered superior. In our data, the R^2 values were fairly consistent across all models and threat-specific security actions with one exception: the R^2 associated with RCT and the tailgating threat-specific security action explained less than half of the variance in behavioral intent compared with the other threat-specific security actions that we evaluated using RCT. However, in all cases other than the above exception, the R^2 explained by the generic measures (undefined security action) was the lowest across all models compared with the other ISP-mandated threat-specific security actions.

Of these CBSEM model evaluation criteria, however, arguably the most important in terms of comparing our model results are the path coefficients and their theorized relationships. Confirming the characteristics of variable relationships is the distinguishing mark of a successful or unsuccessful ISP compliance model. After all, one of the main goals of ISP compliance research is to better understand the behavioral antecedents of ISP-directed behaviors (and intentions thereof). In our data, we observed considerable variability in the path coefficients for each theoretical model across the three threat-specific action measures and the generic measures. The generic measures and the phishing threat-specific security action had similar variable path characteristics (i.e., significance and similar coefficient magnitudes) for the TPB, DT, and PMT. However, the path characteristics for the other threat-specific security actions varied across all four theoretical models. In these instances, one or more variables were significant when we measured general ISP compliance intentions but were not significant when we measured a specific ISP-related security action (and vice versa).

To assess the statistical magnitude of the differences in construct path coefficients, we conducted Wald χ^2 tests to determine if the difference in coefficients was statistically significant (Muthen & Muthen, 2015 p. 711).[16] Table 6 displays the results for these multigroup statistical tests between all pairs of threat-specific security actions along with the undefined security action. These tests reveal that there is a statistically significant difference between the different measurement techniques for certain path coefficients. For instance, in the PMT model, self-efficacy is strongly significant for all three threat-specific security actions plus the generic undefined security measure. However, self-efficacy is a statistically stronger contributor to behavioral intent in the flash media and tailgating threat-specific security actions than for the generic and phishing threat-specific security actions. This type of differentiation on the relative importance of a behavioral antecedent would have been missed had we not examined the different threat-specific security actions. Likewise, a similar condition exists in the RCT model regarding the impact of the perceived cost of complying with a security action on attitudes towards that security behavior. This path is significant for all but the generic undefined security action, but there is a statistically significant difference in the coefficients between the flash media and tailgating threat-specific security actions. Therefore, the statistically significant beta coefficient differences provide some evidence that suggests we should be cautious about making speculative claims of universal generalization that have been made in the prior ISP compliance literature.

[16] We were able to run these multigroup statistical tests comparing the beta coefficients because both configural and metric invariance were established in our data (Kline, 2016, p. 396).

Table 6. Study 1 Path Coefficient Differences

Theory of planned behavior					**Deterrence theory**				
SNORM → BINT		GEN	FL	PH	SPROB → BINT		GEN	FL	PH
	FL	0.029				FL	0.056		
	PH	0.036	0.007			PH	0.025	0.031	
	TG	0.132	0.161*	0.168*		TG	0.021	0.035	0.004
ATT → BINT		GEN	FL	PH	SSEV → BINT		GEN	FL	PH
	FL	0.151				FL	0.037		
	PH	0.04	0.112			PH	0.066	0.103	
	TG	0.231*	0.08	0.191*		TG	0.056	0.019	0.122
PBC → BINT		GEN	FL	PH					
	FL	0.132*							
	PH	0.053	0.185*						
	TG	0.042	0.09	0.095					
Protection motivation theory					**Rational choice theory**				
TSEV → BINT		GEN	FL	PH	PBEN → ATT		GEN	FL	PH
	FL	0.029				FL	0.017		
	PH	0.036	0.007			PH	0.068	0.051	
	TG	0.132	0.161*	0.168*		TG	0.054	0.037	0.014
PVUL → BINT		GEN	FL	PH	PCOMP → ATT		GEN	FL	PH
	FL	0.151				FL	0.096		
	PH	0.04	0.112			PH	0.016	0.08	
	TG	0.231*	0.08	0.191*		TG	0.031	0.127*	0.047
REFF → BINT		GEN	FL	PH	PNCOMP → ATT		GEN	FL	PH
	FL	0.132*				FL	0.018		
	PH	0.053	0.185*			PH	0.001	0.019	
	TG	0.042	0.09	0.095		TG	0.016	0.039	0.02
SEFF → BINT		GEN	FL	PH	ATT → BINT		GEN	FL	PH
	FL	0.186*				FL	0.143*		
	PH	0.088	0.274*			PH	0.188*	0.045	
	TG	0.163*	0.09	0.251*		TG	0.205*	0.062	0.017

Notes:

BINT: Behavioral Intent, ATT: Attitude, PBC: Perceived Behavioral Control, SPROB: Perceived Sanctional Probability, SSEV: Sanction Severity, SEFF: Self-Efficacy, TSEV: Perceived Threat Severity, PVUL: Perceived Vulnerability, REFF: Response Efficacy, PBEN: Perceived Benefit from Compliance, PCOMP: Perceived Benefit from Complying, PNCOMP: Perceived Cost from Noncompliance., GEN: Generic Measure, FL: Improper Flash Media Use, PH: Phishing, TG: Tailgating.

* means passed the Wald Chi-square significance test confirming a statistically significant difference for that model path between the two reference security threat conditions.

Cell numbers indicate the difference between the coefficient values for the two corresponding constructs.

5.3 Study 1 Limitations

Our first study had two primary limitations. First, we had a lack of variance in our dependent variables across the three threat-specific security actions and the generic undefined security action measures, which is similar to the limitation of several published studies in our literature review such as Bulgurcu et al. (2010). In our sample, most of our study participants did intend to comply with the policies and procedures contained in the ISP. Therefore, the model differences that we observed were in relation to employees who generally intended to follow the rules. Our first study does not offer empirical evidence for employees or individuals on the other end of the spectrum (i.e., employees who had a lesser tendency to follow the rules and regulations contained in the ISP). The fact that the DoD has a culture of compliance and conformity is a positive aspect of the DoD culture but other organizations may not have this type of information security culture.

Second, our measures captured current behaviors (self-reported) via behavior statements (i.e., "If I were caught violating the tailgating requirements of the ISP, I would be severely punished") without contextualizing the threat-specific security actions in any type of scenario or real-life use-case. Per Moody et al. (2018), capturing current behaviors is valuable but adding context to the security actions is also valuable to evaluate relationships in different situations. Using scenario vignettes and adding context to hypothetical situations is one alternative to account for these types of situational effects (Moody et al., 2018; Siponen & Vance, 2010). This scenario approach can reduce the potential for positive response bias and can capture prospective behavioral intentions instead of retrospective intentions that may be captured in the behavior statement approach (D'Arcy et al., 2009; Moody et al., 2018; Pogarsky, 2004; Siponen & Vance, 2010). With these two limitations in mind, we designed and executed our second study.

6 Study 2

In Study 2, we collected data from a private university in the US that had an ISP that applied to both employees and other users (such as students and visitors) who accessed the university's information resources. The ISP-directed behaviors that we investigated were workstation locking and password sharing along with a generic undefined security action measure. Similar to Study 1, these two ISP-directed security actions were different based on the mandated requirements. Based on the ISP requirements at the time of our study, their requirements ranged from low interpersonal interaction (workstation locking) to high interpersonal interaction (password sharing). These two threat-specific security actions also varied significantly in terms of the level of thought and effort required to comply with the ISP-directed policies. Appendix B displays the university's requirements for each one of these threat-specific security actions, which shows the behavioral differences across each threat-specific security action. We evaluated these security actions along the same theoretical lines of the TPB, PMT, DT, and RCT that we used in Study 1.

At the time of our study, the ISP for this private university covered roughly 5,500 faculty, staff, visitors, and students. In contrast to the DoD, however, the university's employees and students were not subject to rigorous annual training and testing on ISP requirements. They only had to affirm that they would follow the ISP when they first received their university accounts, logged onto university-owned computers, and connected to university wireless networks (via a captive portal) while using personal computing devices. Therefore, this setting provided a nice contrast to the DoD environment. However, we still wanted to ensure that all of our study participants were aware of the ISP content because the ISP content is a core component of ISP-related research. As such, our online survey instrument provided a link to the official ISP along with the text of the ISP specifically related to workstation locking and passwords at the beginning of our survey instrument. Participants were required to acknowledge that they understood this ISP content before they could access the survey questions.

6.1 Primary Data Collection

We adapted all of our measurement items from prevalidated scales taken from previous research. The generic measurement items were the same in both Study 1 and Study 2. Similar to Study 1, each survey participant answered all of the questions pertaining to both threat-specific security actions and the generic measures. The order of the questions was randomized for each survey participant. All latent construct items were measured using 7-point Likert scales (both negative and positive). However, we used scenario vignettes in Study 2 to capture the threat-specific security actions instead of the behavioral statements that we used in Study 1. We used Moody et al. (2018) and Siponen and Vance (2010) as our guides to construct the two scenarios related to workstation locking and password sharing compliance. The scenarios specifically identified that the potential security action in the vignette was forbidden by the ISP. Appendix B contains the actual scenarios along with the full list of measurement items that we used in Study 2.

We designed and administered the survey following the same best practices we used in Study 1. However, Study 2 incorporated more negatively worded questions than Study 1. We piloted the survey instrument twice. The first pilot was with a group of 10

employees and 10 students. The first pilot started with the same workstation locking and password sharing scenarios found in Siponen and Vance (2010) and Moody et al. (2018). However, based on feedback from the first pilot study, we modified the scenarios to tailor the vignettes based on whether the survey participant was an employee or a student. After we made this modification, we performed a second pilot study. The second pilot included 10 participants (five employees and five students) who participated in the first pilot study along with an additional 20 participants (10 employees and 10 students). As a result of the second pilot study, we made minor adjustments to the instructions to remove any potential sources of ambiguity.

A total of 1,263 participants (organizational employees and students) were invited to voluntarily participate in the study without any monetary compensation. Participants were assured of their anonymity before agreeing to participate. Unlike in Study 1, study participants in Study 2 only had the option of participating online. After all follow-up emails, we collected a total of 231 responses (102 employees and 129 students) of which 11 had a random collection of missing responses throughout their surveys. For these 11 participants, we used the full information maximum likelihood (FIML) method in MPlus (v8) (Kline, 2016, p. 86). Similar to Study 1, we could not determine how many of the 1,263 potential Study 2 participants actually received and read the survey requests or the follow-up emails. A weakness of Study 1 was a lack of variance in our dependent variables. This issue was not prevalent in Study 2.

6.2 Data Analysis and Results

We used CBSEM in MPlus (v8) to analyze our data. We assessed the potential adverse impact of common method variance in Study 2 in the same manner as Study 1 using the ULMC factor approach, which (similar to Study 1) did not provide any evidence of the presence of common method variance in our dataset.

We performed a separate CFA for both threat-specific security actions and for the general undefined security action condition because we tested each separately. Table 7 displays our CFA results and the correlation matrix.[17] The results of our CFA analyses revealed that all of our constructs met the requirements to be considered reflective indicators for their respective constructs for both threat-specific security actions and the generic undefined security action (Petter et al., 2007). All composite reliabilities were above 0.7 for all of our tested threat-specific security actions and the generic undefined security action, which is evidence of convergent validity. The square root of the AVE for each of our constructs was greater than its correlations with all of the other constructs, which is evidence of divergent validity. Next, we evaluated the model fit for the CFA analysis, which included all latent constructs tested simultaneously for all four models: generic measures (χ^2 = 1070.3, *df* = 624, Bollen-Stine *p* = 0.126, CFI = 0.944, RMSEA = 0.057), workstation locking (χ^2 = 1072.9, *df*= 624, Bollen-Stine *p* = 0.3, CFI = 0.906, RMSEA = 0.058), and password sharing (χ^2 = 1450.8, *df* = 624, Bollen-Stine *p* = 0.11, CFI = 0.916, RMSEA = 0.079). We also evaluated nested model comparisons using the same procedures as we used in Study 1, which were not statistically significant. Finally, we conducted invariance tests using the same procedures from Study 1 between the different threat-specific security actions and the generic undefined security action measures for all four theories, which satisfactorily showed both configural and metric invariance. Table 8 and Table 9 display the CBSEM model results for both threat-specific security actions (workstation locking and password sharing) plus the generic undefined security action measures for all four theories.

Similar to Study 1, in Study 2 we compared the CBSEM model results across each theoretical model and threat-specific security action including the generic undefined security action measures using model fit, dependent variable variance explained (R^2), and path coefficient magnitude, sign, and significance. As shown in Table 8, all three of the TPB model runs failed the χ^2 fit test (with satisfactory CFI and mediocre to unsatisfactory RMSEA values). Model fit for PMT was satisfactory for all threat-specific security actions, but the overall fit for the generic undefined security action measure was notably better (lower χ^2 and RMSEA, higher CFI) than the other threat-specific security actions (with the password sharing threat having the poorest overall fit statistics). For the DT, only the password sharing threat-specific security action passed the χ^2 test. Lastly, for the RCT model, the workstation locking threat condition failed the χ^2 test. Thus, as in Study 1, the Study 2 disparate model fit results across threat-specific security actions within the four theoretical models make it difficult to justify generalizing from the generic undefined security action measures to the tested specific threat-specific security actions (and vice versa).

[17] As displayed in Table 5, self-efficacy and perceived behavioral control (PBC) were highly correlated. This high level of correlation is not surprising because there are similarities between these two constructs. As such, many researchers have justified using self-efficacy as a substitute for PBC under certain circumstances (Aurigemma & Mattson, 2017, Bulgurcu et al., 2010). However, this correlation is not an issue in our study because we do not use both self-efficacy and PBC in the same model for any of our analyses other than the CFA.

Table 7. CFA Validity and Construct Correlations for Study 2

Generic Measure	CR	AVE	PNCOMP	BINT	SEFF	PVUL	TSEV	REFF	SNORM	PBC	ATT	SSEV	SPROB	PCOMP	PBEN
PNCOMP	0.936	0.831	0.912												
BINT	0.967	0.907	0.109	0.953											
SEFF	0.956	0.878	0.222	0.384	0.937										
PVUL	0.944	0.850	0.017	-0.030	-0.033	0.922									
TSEV	0.937	0.833	-0.011	-0.060	0.056	-0.594	0.913								
REFF	0.900	0.752	0.289	0.176	0.238	0.387	-0.391	0.867							
SNORM	0.879	0.708	0.186	0.273	0.477	0.112	-0.040	0.190	0.842						
PBC	0.879	0.711	0.188	0.354	0.912	-0.068	0.105	0.235	0.467	0.843					
ATT	0.939	0.838	0.267	0.349	0.583	-0.031	0.087	0.241	0.664	0.578	0.915				
SSEV	0.893	0.737	-0.432	-0.060	0.025	-0.147	0.238	-0.403	-0.221	0.036	-0.186	0.858			
SPROB	0.886	0.722	0.338	0.012	-0.080	0.139	-0.033	0.331	0.207	-0.013	0.134	-0.662	0.850		
PCOMP	0.913	0.780	-0.308	-0.142	-0.325	-0.059	0.211	-0.258	-0.225	-0.293	-0.189	0.193	-0.064	0.883	
PBEN	0.869	0.690	0.515	0.199	0.299	0.071	-0.086	0.373	0.264	0.290	0.239	-0.389	0.377	-0.335	0.831
Workstation Locking	CR	AVE	PNCOMP	BINT	SEFF	PVUL	TSEV	REFF	SNORM	PBC	ATT	SSEV	SPROB	PCOMP	PBEN
PNCOMP	0.921	0.795	0.892												
BINT	0.977	0.934	-0.333	0.967											
SEFF	0.951	0.867	0.208	-0.147	0.931										
PVUL	0.861	0.676	-0.299	0.356	0.004	0.822									
TSEV	0.952	0.869	0.372	-0.179	0.084	-0.688	0.932								
REFF	0.873	0.698	0.431	-0.171	0.556	-0.256	0.390	0.836							
SNORM	0.898	0.746	-0.340	0.593	-0.103	0.281	-0.236	-0.160	0.864						
PBC	0.870	0.691	0.274	-0.231	0.956	-0.008	0.070	0.587	-0.087	0.832					
ATT	0.901	0.753	0.348	-0.305	0.666	-0.250	0.268	0.652	-0.226	0.781	0.868				
SSEV	0.916	0.786	-0.535	0.324	-0.026	0.446	-0.250	-0.271	0.366	-0.074	-0.223	0.886			
SPROB	0.914	0.781	0.602	-0.204	0.109	-0.399	0.563	0.429	-0.336	0.080	0.264	-0.638	0.883		
PCOMP	0.935	0.827	-0.240	0.537	-0.261	0.290	-0.146	-0.274	0.338	-0.342	-0.368	0.313	-0.174	0.910	
PBEN	0.874	0.703	0.724	-0.283	0.325	-0.291	0.363	0.528	-0.281	0.350	0.501	-0.397	0.560	-0.300	0.838
Password Sharing	CR	AVE	PNCOMP	BINT	SEFF	PVUL	TSEV	REFF	SNORM	PBC	ATT	SSEV	SPROB	PCOMP	PBEN
PNCOMP	0.929	0.813	0.902												
BINT	0.985	0.957	-0.315	0.978											
SEFF	0.968	0.911	0.237	-0.239	0.954										
PVUL	0.941	0.843	-0.542	0.402	-0.266	0.918									
TSEV	0.957	0.882	0.462	-0.251	0.172	-0.653	0.939								
REFF	0.927	0.809	0.487	-0.276	0.484	-0.485	0.502	0.899							
SNORM	0.875	0.701	-0.324	0.778	-0.201	0.346	-0.249	-0.300	0.837						
PBC	0.882	0.714	0.301	-0.301	0.990	-0.305	0.259	0.555	-0.266	0.845					
ATT	0.933	0.823	0.341	-0.471	0.624	-0.419	0.384	0.622	-0.448	0.702	0.907				
SSEV	0.924	0.803	-0.496	0.156	-0.142	0.349	-0.297	-0.319	0.169	-0.155	-0.181	0.896			
SPROB	0.939	0.836	0.467	-0.132	0.203	-0.374	0.570	0.406	-0.179	0.248	0.276	-0.516	0.914		
PCOMP	0.939	0.838	-0.260	0.482	-0.417	0.294	-0.127	-0.279	0.460	-0.442	-0.361	0.135	-0.115	0.915	
PBEN	0.871	0.698	0.656	-0.285	0.332	-0.391	0.354	0.550	-0.293	0.381	0.359	-0.386	0.446	-0.314	0.835

Composite Reliability (CR), Average Variance Extracted (AVE), Perceived Vulnerability to Threat (PVUL), Perceived Threat Severity (TSEV), Response Efficacy (REFF), Subjective Norms (SNORM), Perceived Behavioral Control (PBC), Attitude (ATT), Perceived Sanction Severity (SSEV), Perceived Sanction Probability (SPROB), Perceived Cost of Compliance (PCOMP), Perceived Cost of non-Compliance (PNCOMP)

Note: Off diagonal numbers are interconstruct correlations; diagonal numbers are the square roots of AVE (average variance extracted).

Table 8. CBSEM Model Fit Results for Study 2

Model	χ^2	*df*	*p*	CFI	RMSEA
Theory of planned behavior					
Generic measure	144.411	48	0.013	0.959	0.095
Workstation locking	117.513	48	0.028	0.971	0.082
Password sharing	167.394	48	0.01	0.957	0.108
Protection motivation theory					
Generic measure	110.992	80	0.416	0.991	0.042
Workstation locking	134.088	80	0.362	0.983	0.055
Password sharing	194.728	80	0.098	0.972	0.082
Deterrence theory					
Generic measure	66.303	24	0.001	0.976	0.089
Workstation locking	72.037	24	0.001	0.975	0.095
Password sharing	35.013	24	0.438	0.995	0.046
Rational choice theory					
Generic measure	190.032	83	0.090	0.965	0.076
Workstation locking	187.334	83	0.016	0.961	0.082
Password sharing	193.658	83	0.444	0.965	0.079

While we found the R^2 values in Study 1 to be relatively consistent across security actions, we found that the R^2 values varied greatly according to security action and theoretical model in Study 2. Specifically, the R^2 values in the TPB model were 14.9% for ISP compliance with the generic undefined security action measure, 39.4% for workstation locking, and 62.4% for password sharing. The R^2 values in the RCT model were low for the generic measures (12.1%) and workstation locking (10.9%) but high for password sharing ISP compliance (72.3%). Typical workstations have an automatic locking feature after a specified period of inactivity, which might render a rational cost-benefit analysis much less relevant for that threat-specific security action. Additionally, the R^2 value on attitude for password sharing was over 90% but less than 10% for the generic undefined security action measures. If we had just used a generic undefined security action measure of ISP compliance, we might inaccurately conclude that costs and benefits have minimal impact on shaping an individual's attitudes towards ISP compliance intentions due to the low R^2 value. Perceived costs and benefits do matter for ISP compliance, but perhaps only for certain threat-specific security actions. As with Study 1, the R^2 values for DT were unsurprisingly low. The R^2 values in the PMT model were reasonably consistent across threat-specific security actions and the generic undefined security action measures. However, it is worth noting that the R^2 values for the PMT conditions were roughly 50% lower than the R^2 values for the PMT conditions in Study 1.

The path coefficient magnitude and significance associated with each theoretical model also varied considerably across the different threat-specific security actions and the generic undefined security action measures.[18] In the RCT models, the perceived benefits and costs of compliance were significant for the threat-specific security actions but were not significant for the generic undefined security action measures. Interestingly, the perceived costs of noncompliance construct in the RCT models was significant when we used the generic undefined security action measures but not significant for either password sharing or workstation locking. Therefore, just using the generic undefined security action measures yielded vastly different results in the context of RCT. These differences were also evident with our PMT results. All three instances had different sets of

[18] The path coefficients for the PMT model for the workstation locking and password sharing threat-specific security actions were impacted (suppressed) by the large impact of perceived vulnerability on intentions. We conducted a post hoc analysis where we removed perceived vulnerability from the PMT structural model, which resulted in threat severity having a larger and significant impact on intentions for the workstation locking threat. This post hoc analysis also revealed that self-efficacy had a larger and significant impact on intentions for the password sharing threat-specific security action. A similar phenomenon occurred in the TPB model due to the very strong relationship between subjective norms and behavioral intentions.

significant path coefficients. In the TPB, our data showed that subjective norms were a significant factor when measuring threat-specific security intentions for both password sharing and workstation locking but not significant when using the generic undefined security action measures. Again, the generic undefined security action measures would lead us to believe that subjective norms may not be an important factor in ISP compliance, but they do matter for password sharing and workstation locking. Additionally, as shown in Table 9 and Table 10, the influence of attitudes on behavioral intentions in the RCT models are significantly stronger for both threat-specific security actions compared to the generic undefined security action measure. Furthermore, there is something different influencing the attitudes of participants regarding password sharing compared to the other threat-specific security actions (and the generic undefined security action measure), but we would not have seen this relationship if we had relied upon generic undefined security action measures to drive our analysis and scientific inquiry.

Table 9. CBSEM Model Structural Path Results for Study 2

Model	Generic Measure	Workstation Locking	Password Sharing
Theory of planned behavior			
R^2 (BINT)	0.149	0.394	0.624
SNORM → BINT	0.048(NS)	0.707***	0.831***
ATT → BINT	0.248 (p=.097)	0.028(NS)	0.222(p=.10)
PBC → BINT	0.208*	0.404(NS)	0.05(NS)
Protection motivation theory			
R^2 (BINT)	0.155	0.168	0.183
TSEV → BINT	0.088(NS)	0.176(NS)	0.037(NS)
PVUL → BINT	0.087(NS)	0.484***	0.461***
REFF → BINT	0.079(NS)	0.035(NS)	0.034(NS)
SEFF → BINT	0.365*	0.119(NS)	-0.283(p=.10)
Deterrence theory			
R^2 (BINT)	0.01	0.105	0.03
SPROB → BINT	0.044(NS)	0.003(NS)	0.084(NS)
SSEV → BINT	0.086(NS)	0.439***	0.156(NS)
Rational choice theory			
R^2 (BINT)	0.121	0.109	0.723
R^2 (ATT)	0.087	0.317	0.911
PBEN → ATT	0.120(NS)	0.317***	0.211*
PCOMP → ATT	-0.09(NS)	-0.145***	-0.206***
PNCOMP → ATT	-0.139*	-0.041(NS)	-0.100(NS)
ATT → BINT	0.455***	0.634***	0.810***

Notes: For ease of visually differentiating significant and non-significant path relationships in the CBSEM results, we used NS to signify not significant. *p < 0.05, **p < 0.01, ***p < 0.001

BINT: Behavioral Intent, ATT: Attitude, PBC: Perceived Behavioral Control, SPROB: Perceived Sanction Probability, SSEV: Sanction Severity, SEFF: Self-Efficacy, TSEV: Perceived Threat Severity, PVUL: Perceived Vulnerability, REFF: Response Efficacy, PBEN: Perceived Benefit from Compliance, PCOMP: Perceived Benefit from Complying, PNCOMP: Perceived Cost from Noncompliance, NS: Not Significant (p > 0.1).

Table 10. Study 2 Path Coefficient Differences

Theory of planned behavior				**Deterrence theory**			
SNORM → BINT		GEN	WL	SPROB → BINT		GEN	WL
	WL	0.659*			WL	0.041	
	PS	0.782*	0.127		PS	0.04	0.081
ATT → BINT		GEN	WL	SSEV → BINT		GEN	WL
	WL	0.22*			WL	0.353*	
	PS	0.026	0.194*		PS	0.07	0.283*
PBC → BINT		GEN	WL				
	WL	0.196*					
	PS	0.158*	0.354*				
Protection motivation theory				**Rational choice theory**			
TSEV → BINT		GEN	WL	PBEN → ATT		GEN	WL
	WL	0.088			WL	0.197*	
	PS	0.051	0.139*		PS	0.081	0.106
PVUL → BINT		GEN	WL	PCOMP → ATT		GEN	WL
	WL	0.397*			WL	0.136	
	PS	0.374*	0.023		PS	0.197*	0.061
REFF → BINT		GEN	WL	PNCOMP → ATT		GEN	WL
	WL	0.044			WL	0.098	
	PS	0.045	0.001		PS	0.039	0.059
SEFF → BINT		GEN	WL	ATT → BINT		GEN	WL
	WL	0.246*			WL	0.179*	
	PS	0.082	0.164*		PS	0.355*	0.176

Notes:

BINT: Behavioral Intent, ATT: Attitude, PBC: Perceived Behavioral Control, SPROB: Perceived Sanctional Probability, SSEV: Sanction Severity, SEFF: Self-Efficacy, TSEV: Perceived Threat Severity, PVUL: Perceived Vulnerability, REFF: Response Efficacy, PBEN: Perceived Benefit from Compliance, PCOMP: Perceived Benefit from Complying, PNCOMP: Perceived Cost from Noncompliance, GEN: Generic measure, WL: Workstation locking, PS: Password sharing.

* means passed the Wald chi-square significance test confirming a statistically significant difference for that model path between the two reference security threat conditions.

Cell numbers indicate the difference between the coefficient values for the two corresponding constructs.

6.3 Study 2 Limitations

The primary weakness of our second study was the lack of required recurrent training and a much weaker security culture in the private university that we studied. The individuals covered by this university's ISP were not required to be repeatedly trained and tested on the contents of the ISP. Training repetition helps create a security culture within an organization that positively impacts long-term compliance intentions (Dhillon, Syed, & Pedron, 2016). Although we tried to control for this by requiring our survey participants to read the policies related to workstation locking and password sharing (and by including the proper ISP actions in the actual scenario wording), it is possible that this was the first time that some of our research subjects had read their ISP. If participants were not knowledgeable about the contents of their ISP, then the generic undefined security action measures became even more problematic since the individuals were unaware of what is generally covered by their ISP. Therefore, the lack of ISP-related knowledge was more of a confounding variable in Study 2 than it was in Study 1.

7 Discussion and Conclusion

The objective of ISP compliance research is (or at least should be) to discover the mechanisms, treatments, and behavioral antecedents that will maximize employees' compliance behaviors (or intentions thereof) (Crossler et al., 2014; Posey et al., 2013; Siponen & Vance, 2014). In other words, how can we encourage more employees to follow the rules and regulations outlined in their organizations' ISP documents? Our literature review revealed that the vast majority of the prior ISP compliance research that has been published in our top journals has attempted to answer this question by developing universal or pseudo-universal models of ISP compliance that purportedly cover many or all of the policies contained in organizational ISPs. Contrarily, we have argued in our paper that constructing particular models of threat-specific security actions will be more useful at accomplishing this objective because particular models are grounded in a specific security action instead of an undefined or aggregated collection of different (somewhat arbitrary) security actions. Essentially, we are suggesting that we can maximize employee compliance one threat-specific security action at a time, because compliance with each security action often requires different thought processes, time, diligence, knowledge, and effort to comply.

There is significant behavioral variability in ISP-mandated actions (Siponen & Vance, 2014), so we (as a research community) have to think critically about the types of behaviors that a universal model of ISP compliance is actually modeling (Siponen & Baskerville, 2018). ISP-related behaviors range from simple actions such as running software updates when automatically prompted to do so to much more complicated actions such as preventing a superior from tailgating into a restricted area. From a measurement perspective, we assert that it is difficult for researchers to capture this behavioral variability in a single set of measures (whether they are focused on a single threat-specific security action, multiple threat-specific security actions, or one generic measure related to an undefined security action). Our results suggest that it is problematic to make the following claims of generalization: (1) generalizing models measuring general compliance intentions to all threat-specific security compliance intentions, (2) generalizing threat-specific models to other threat-specific security actions, and (3) generalizing threat-specific models to general compliance intentions.

As reviewers and editors of academic papers, we should challenge our colleagues to better justify the types of measures (undefined security actions, behavioral items, scenario vignettes or qualitative) that are used along with the level of generalization that the authors are attempting to make with those measures. For example, simply citing a prior study as justification (which is the norm for ISP research) for using generic undefined security action measures is not a solid justification (by itself). Specifically concerning generic undefined security action measures, we should challenge our colleagues to clearly identify the following: (1) the types of behaviors that these generic undefined security action measures are capturing, (2) how these generic undefined security action measures are relevant for the advancement of the ISP compliance field, and (3) why these generic undefined security action measures are preferable to threat-specific security measures for their research objectives. Similarly, when reviewing papers that are aggregating scenario vignettes across different security actions, we should push and challenge the authors to clearly demonstrate why this type of aggregation is better for the advancement of ISP-related knowledge than analyzing the different scenarios separately. If we aggregate across multiple threats that all require different actions, then what are we conceptually capturing with this aggregation? Our empirical results show different path coefficient characteristics, explanatory power, and model fit metrics across ISP-mandated threat-specific security actions, which suggests that this type of aggregation might be averaging or smoothing out the effects. Is this smoothed-out collection of ISP-mandated threat-specific security actions the types of behaviors that we want organizations to promote among their employees? Reviewers and editors should push and challenge our colleagues to address these questions conceptually and empirically.

Our literature review implies that our top journals have a strong preference to publish allegedly universal or pseudo-universal models of ISP compliance. The authors of these papers seemingly have to speculate that their threat-specific security action is widely generalizable to many or most threat-specific security actions contained in an organization's ISP. As such, the authors routinely issue an obligatory apology statement as a result of their decision to investigate a particular threat-specific security action contained in the ISP. It is interesting how researchers classify their research context as a research limitation or weakness.

We assert that the specific ISP-related problem that is being investigated is not a study limitation or weakness. A research limitation or weakness is, for instance, violating the assumptions of a statistical model or unjustifiably leading interviewees in a qualitative case study (Lee, 1991). Why should the authors apologize for investigating, say, the ISP-related preventative or mitigating actions associated with ransomware? Ransomware is a timely and significant problem facing organizations. It is only perceived as a research limitation or weakness because researchers who want to increase their probability of getting a ransomware ISP compliance paper published

in one of our leading journals seemingly have to speculate that the ISP-mandated actions associated with ransomware are similar to many or most other policies contained in the ISP document. To do so, the authors must make very speculative claims of generalization regarding their ransomware empirical observations. For instance, the authors would have to claim that ransomware compliance is somehow representative of all, many, or most other policies contained in an organization's ISP document. We posit that making this type of generalization is problematic given the wide variety of threat-specific security actions covered by typical ISPs.

We argue that solving the problem of compliance with the ransomware policies and procedures in-depth has tremendous theoretical value even if the ransomware ISP-directed behaviors are completely unrelated to the other policies and procedures contained in the ISP document. Why should a paper be considered to be more publishable (in our top journals) if there are overlapping (generalizable) mechanisms, treatments, and behavioral antecedents for ransomware compliance and tailgating compliance? As ISP compliance scholars, we spend a significant amount of time and energy arguing about whether our research models are generalizable to other contexts. At the end of the day, however, it is almost pure speculation (Davison & Martinsons, 2016). Additionally, part of the scientific process is testing different models with different types of behaviors. In the ISP compliance space, however, our literature review implies that we are primarily interested in discovering the factors affecting all (or at least many) compliance behaviors while largely ignoring important contextual components related to scientific discovery.

If our discipline were to switch its publication bias from universal to particular models of ISP compliance, we posit that this switch would open the door to a variety of meta-analyses that might be very meaningful. For instance, if there are a dozen or so models of phishing compliance all using different or similar theoretical perspectives, then we might be able to gain a very deep understanding of the factors influencing phishing ISP behaviors by performing a meta-analysis. We might also be able to compare and contrast the models that use the same theories to explain different ISP-mandated security actions in order to determine both similarities and differences across multiple types of security actions. We suggest that this approach to enhancing ISP knowledge would be richer than the generic undefined security action measures or the aggregation of different scenario vignettes that have been used in the prior literature. However, this approach can only work if our discipline publishes particular models in our top journals. If these particular models are being filtered out of our top journals because they are not universal enough to begin with, then this type of future research cannot be reasonably accomplished.

Our paper is the first to examine differences between different types of ISP-directed threat-specific security actions and generic undefined security action measures of ISP compliance actions (or intentions thereof). Comparing and contrasting ISP compliance models across different threat-specific security actions and generic undefined security-action measures is necessary in order to support or refute the speculative claims of generalization that are routinely made in our top-level publications. Siponen and Baskerville (2018, p. 250) refer to this as a proverbial horse race between models using different theories, constructs, and relationships. Prior research has infrequently compared different models to see which theoretical perspective is best at solving a particular ISP-related behavioral problem. If the prior literature is correct in their speculative claims of empirical generalization, then we should have seen similar or more consistent effects (i.e., model fit, R^2, and path coefficient characteristics) across the different theories and threat-specific security actions even though the ISP-directed actions were different. However, our data revealed many significant differences across both of our empirical studies. For instance, perceived behavioral control is an important behavioral antecedent to ISP-related security actions but only for certain threat-specific security actions. Our empirical results suggest that attempting to generalize the effect of perceived behavioral control to all or most other ISP-directed security actions is potentially problematic. The type of ISP-related action will ultimately determine whether perceived behavioral control and other important variables impact ISP compliance actions (or intentions thereof). The threat-to-threat differences that we found in our data question whether a universal model of ISP compliance can be constructed empirically given the variety of security behaviors covered by typical ISPs.

We investigated threat-specific security actions as the area of particularism that we proposed to be relevant to ISP-related behaviors. We make no claims that the threat-specific security action is the only particularism dimension that is relevant for ISP-related behaviors. We suggest that our theoretical and empirical insights could motivate future research related to other ISP-related differences. For instance, future research might investigate cultural differences at the national or organizational levels, behavioral variability at the industry level, mitigating control differences (e.g., compliance with the use of anti-malware software versus compliance with the use of VPN software), or device differences (e.g., compliance with the policies related to locking a bring your own device such as a tablet or smartphone versus a company desktop or laptop).

Additionally, future research might investigate phishing (or a different threat-specific security action) using the TPB or PMT in the context of a bank, which might be an interesting contextual boundary condition to either one of those theories. For example, bankers might have (or need) greater sensitivity to phishing scams due to the nature of their jobs. Banks may be subject to phishing attempts more than educators or construction office staff due to the added attention that banks get from cybercriminals. Banks control trillions of dollars in assets, so developing a banking-specific model of ISP phishing compliance would potentially be extremely impactful and a useful extension to the TPB, PMT, or an alternative theoretical perspective. We would also suggest that future research tackling this problem should not have to apologize for investigating bankers as their contextual extension (even if bankers are unique and not related to lawyers working in law firms or educators working at universities).

We used two different organizations with vastly different information security cultures. Even though our results were similar across these two organizational settings, caution should still be taken when applying our results to other types of organizations without clearly understanding the demographic, industry, and cultural differences. However, the point of our study was not to conclude that every organization will have the same model fit statistics, coefficient path magnitudes, or significance levels across these threat-specific security actions but instead to conclude that specific ISP-directed security actions will have different behavioral antecedents. How those differences may play out in different settings is an open theoretical and empirical question. We are not suggesting that a bank or a hospital will be the same as our two organizations; rather, we are suggesting that research in each organizational context should be cautious when attempting to generalize the behavioral antecedents to and from different threat-specific security actions as dictated by their organizations ISPs.

From a theoretical perspective, we have argued that particular models of ISP compliance have more theoretical value because different security actions may have dissimilar behavioral antecedents. From a practical perspective, however, it is ultimately an empirical question as to whether security managers would prefer universal or particular models of ISP compliance. As ISP compliance researchers, it is our job to construct models that provide conceptual clarity to whatever we are investigating and to provide sound empirical evidence supporting those conceptually clear models. If we do an exemplary job with this, then the security managers can decide which types of models are best for their specific organizations. Instead of attempting to speculate as to what security managers may prefer, we as researchers should provide all types of empirical evidence and conceptual models concerning ISP compliance and give the practitioners the autonomy to decide which models are most relevant to their organizations.

In our paper, we do not address the *why* question. Based on the design and implementation of our two studies, we speculate that the differences in our empirical results are due to the different ISP-mandated requirements surrounding our chosen threat-specific security actions. From our analysis of the specific ISP policies of our chosen threat-specific security actions across the two organizations that we studied, we noticed differences in terms of time, difficulty, diligence, knowledge, social interactivity and effort to comply with the specific policies. Future research should build off of our conceptual and empirical analyses to investigate why we see different results between different threat-specific security actions and the generic undefined security action measures. Our research objective was to foster debate and discussion by conceptually pointing out the challenges associated with universal models of ISP compliance and empirically evaluating measurement and generalization issues with ISP compliance actions (or intentions thereof). Our paper will have been successful if it helps the research community reflect upon on the types of papers that are getting published in our top journals, debate whether these journals are hindering or facilitating the advancement of knowledge in the ISP compliance space due to their publication preferences, and think critically about the types of measures and the claims of generalization that we as ISP compliance researchers are making in the journal articles that are driving the direction of the field.

Acknowledgments

An earlier version of this manuscript was presented at the 2015 IFIP Dewald Roode Workshop on Information Systems Security Research in Newark, Delaware.

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

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

Aurigemma, S., & Mattson, T. (2017). Privilege of procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. *Computers & Security, 66*(1), 218-234.

Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational Behavior and Human Decision Processes, 50*(2), 248-287.

Barrett, P. (2007). Structural equation modelling: Adjudging model fit. *Personality and Individual Differences*, 42(5), 815-824.

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

Boss, S., Galletta, D., Lowry, P., Moody, G., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837-864.

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

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

Bunge, M. (1998). *Social science under debate: a philosophical perspective*. Toronto: University of Toronto Press.

Busse, C., Kach, A. P., & Wagner, S. M. (2017). Boundary conditions: What they are, how to explore them, why we need them, and when to consider them. *Organizational Research Methods, 20*(4), 574-609.

Champion, V. L. (1984). Instrument development for health belief model constructs. *Advances in Nursing Science, 6*(3), 73-85.

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems, 29*(3), 157-188.

Chen, Y., & Zahedi, F. M. (2016). Individual's Internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly, 40*(1), 205-222.

Cheng, Z. A., Dimoka, A., & Pavlou, P. A. (2016). Context may be king, but generalizability is the emperor. *Journal of Information Technology, 31*(1), 257-264.

Chin, W. W. (1998). Commentary: Issues and opinion on structural equation modeling. *MIS Quarterly, 22*(1), vii-xvi.

Crossler, R., & Belanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database, 45*(4), 51-71.

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

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

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.

Davison, R. M., & Martinsons, M. G. (2016). Context is King! Considering particularism in research design and reporting. *Journal of Information Technology, 31*(1), 241-249.

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

Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). *Internet, phone, mail, and mixed-mode surveys: The tailored design method*. Hoboken, NJ: Wiley.

Fernandez, W. D. (2016). Commentary on Davison and Martinsons' "Context is King! Considering Particularism in research design and reporting." *Journal of Information Technology, 31*(1), 265-266.

Fornell, C., Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39-50.

Foth, M. (2016). Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence. *European Journal of Information Systems, 25*(2), 91-109.

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems*, *16*(1), 5.

Gefen, D., Straub, D. W., & Rigdon, E. E. (2011). An update and extension to SEM guidelines for administrative and social science research. *MIS Quarterly, 35*(2), iii-xiv.

Goel, S., Williams, K., & Dincelli, E. (2017). Got Phished? Internet security and human vulnerability. *Journal of the Association for Information Systems, 18*(1), 22-44.

Grover, V., & Lyytinen, K. (2015). New state of play in information systems research: The push to the edges. *MIS Quarterly, 39*(2), 271-296.

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.

Hanisch, K. A., Hulin, C. L., & Roznowski, M. (1998). The importance of individuals' repertoires of behaviors: The scientific appropriateness of studying multiple behaviors and general attitudes. *Journal of Organizational Behavior, 19*(5), 463-480.

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems, 20*(4), 373-384.

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

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

Johns, G. (2006). The Essential impact of context on organizational behavaior. *Academy of Management Review, 31*(2), 386-408.

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

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

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

Keen, P. G. W. (1980). *MIS Research: Reference Disciplines and a Cumulative Tradition.* Paper presented at the International Conference for Information Systems.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly, 23*(1), 67.

Kline, R. B. (2011). *Principles and Practice of Structural Equation Modeling* (3rd ed.). New York, NY: Guilford.

Kline, R. B. (2016). *Principles and practice of structural equation modeling* (4th ed.). New York, NY: Guilford.

Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Towards analysing the rationale of information security non-compliance: Devising a value-based compliance analysis method. *The Journal of Strategic Information Systems*, *26*(1), 39-57.

Lee, A. S. (1991). Integrating positivist and interpretive approaches to organizational research. *Organization Science, 2*(4), 342-365.

Lee, A. S., & Baskerville, R. L. (2003). Generalizing generalizability in information systems research. *Information Systems Research, 14*(3), 221-243.

Li, H., Sarathy, R., Zhang, J., & Luo, X. (2014). Exploring the effects of organizational justice, personal ethics and sanction on Internet use policy compliance. *Information Systems Journal, 24*(6), 479-502.

Levina, N., & Orlikowski, W. J. (2009). Understanding shifting power relations within and across organizations: A critical genre analysis.

Academy of Management Journal, 52(4), 672-703.

Little, D. (1998). *Microfoundations, method, and causation: On the philosophy of the social sciences*. New Brunswick, NJ: Transaction.

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal, 25*(5), 433-463.

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

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User Motivations in Protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*(4), 1203-1230.

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.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of security policy compliance. *MIS Quarterly, 42*(1), 285-311.

Muthén, L. K., & Muthén, B. (2015). *Mplus users guide* (7th ed.). Los Angeles, CA: Muthen & Muthen.

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

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

Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly, 31*(4), 623-656.

Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology*, *63*(1), 539-569.

Pogarsky, G. (2004). Projected offending and contemporaneous rule-violation: Implications for heterotypic continuity. *Criminology*, *42*(1), 111-136.

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

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly, 37*(4), 1189-1210.

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, 52*(3), 596-604.

Sarker, S. (2016). Building on Davison and Martinsons' Concerns: A call for balance between contextual specificity and generality in IS research. *Journal of Information Technology, 31*(3), 250-253.

Savage, S. L. (2012). *The flaw of averages: Why we underestimate risk in the face of uncertainty*. Hoboken, NJ: Wiley.

Schermelleh-Engel, K., Moosbrugger, H., & Müller, H. (2003). Evaluating the fit of structural equation models: Tests of significance and descriptive goodness-of-fit measures. *Methods of Psychological Research* Online, *8*(2), 23-74.

Siponen, M. T., & Baskerville, R. (2018). Intervention effect rates as a path to research relevance: information systems security example. *Journal of the Association for Information Systems*, *19*(4), 247-265.

Siponen, M. T., & Tsohou, A. (2018). Demystifying the influence IS legends of "positivism." *Journal of the Association for Information Systems, 19*(7), 600-617.

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

Siponen, M. T., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *European Journal of Information Systems, 23*(3), 289-305.

Straub, D. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Straub, D., Boudreau, M, & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems, 13*(1), 380-427.

Su, N. (2015). Cultural sensemaking in offshore information technology service suppliers: A cultural frame Perspective. *MIS Quarterly, 39*(4), 959-983.

Suddaby, R., Hardy, C., & Huy, Q. N. (2011). Introduction to special topic forum: Where are the new theories of organization? *Academy of Management Review, 36*(2), 236-246.

Szostak, R. (2003). Classifying natural and social scientific theories. *Current Sociology, 51*(1), 27-49.

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.

Tsang, E. W., & Williams, J. N. (2012). Generalization and induction: Misconceptions, clarifications, and a classification of induction. *MIS Quarterly, 36*(3), 729-748.

Tsang, E. W. (2014). Case studies and generalization in information systems research: A critical realist perspective. *Journal of Strategic Information Systems, 23*(2), 174-186.

Vaast, E., Davidson, E. J., & Mattson, T. (2013). Talking about technology: The emergence of a new actor category through new media. *MIS Quarterly, 37*(4), 1069-1092.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems, 29*(4), 263-290.

Vance, A. O., Lowry, P. B., & Eggett, D. (2015). Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Quarterly, 39*(2), 345-366.

Walsham, G. (1995). The emergence of interpretivism in IS research. *Information Systems Research, 6*(4), 376-394.

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems, 92*(1), 25-35.

Webster, J., Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly, 26*(2), xiii-xxiii.

Williams, J. N., Tsang, E. W. (2015). Classifying generalization: Paradigm war or abuse of terminology? *Journal of Information Technology, 30*(1), 18-29.

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal, 28*(2), 266-293.

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.

Zahedi, F. M., Abbasi, A., & Chen, Y. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. *Journal of the Association for Information Systems, 16*(6), 448.

Appendix A

Table A1. Empirical Evidence and Level of Generalization

		Measurement items (empirical evidence)[a]				Level of generalization		
	Citation	**Generic measures**	**Scenario vignettes**	**Threat-specific**	**Qualitative**	**Universal**	**Pseudo-universal**	**Particular**
1	Boss, Kirsch, Angermeier, Shingler & Boss (2009)	x				x		
2	Bulgurcu, Cavusoglu, & Benbasat (2010)	x				x		
3	Chen, Ramamurthy, & Wen, (2012)		x[b]			x		
4	D'Arcy, Herath, & Shoss (2014)		x				x	
5	D'Arcy, Hovav, & Galletta, (2009)		x				x	
6	Foth (2016)	x				x		
7	Guo, Yuan, Archer, & Connelly (2011)		x				x	
8	Hedström, Kolkowska, Karlsson, & Allen (2011)				x[c]	x[c]		
9	Herath & Rao (2009)	x				x		
10	Hsu, Shih, Hung, & Lowry (2015)	x				x		
11	Johnston, Warkentin, McBride, & Carter (2016)			x		x		
12	Johnston, Warkentin & Siponen (2015)		x			x		
13	Kolkowska, Karlsson & Hedström (2017)				x		x	
14	Li, Sarathy, Zhang, & Luo (2014)	x				x		
15	Lowry & Moody (2015)		x				x	
16	Lowry, Posey, Bennett, & Roberts (2015)	x				x		
17	Menard, Bott & Crossler (2017)			x[d]		x		
18	Moody, Siponen & Pahnila (2018)		x				x[e]	
19	Myyry, Siponen, Pahnila, Vartiainen, & Vance (2009)			x		x		
20	Posey, Roberts, & Lowry (2015)	x				x		
21	Siponen & Vance (2010)		x			x		

Table A1. Empirical Evidence and Level of Generalization

22	Straub (1990)	x				x		
23	Vance, Lowry, & Eggett (2013)			x				x
24	Vance, Lowry, & Eggett (2015)			x				x
25	Willison, Warkentin & Johnston (2018)			x[f]		x		

[a] Generic measures (i.e., "I intend to comply with the requirements of the ISP") relate to an undefined security action, threat-specific measures (i.e., "I intend to comply with the tailgating requirements in the ISP"), scenario vignettes (i.e., present the research subjects with a hypothetical scenario related to a threat-specific security action), or qualitative measures (i.e., case study of a particular workplace or setting).

[b] The scenarios in this study varied certainty of control, punishment, and reward. However, the behaviors measured general compliance of employees with policies regarding passwords, email use, and acceptable of computing technologies.

[c] This paper was particular in terms of industry (health care) but universal in terms of the types of ISP-related behaviors.

[d] The stated purpose of this study was to help managers improve their employees' intentions to engage in secure behavior. However, the behavior examined was the voluntary use of a password manager application. Although the term ISP compliance was not directly used in this paper, the focus on managers implies some policy directed behaviors.

[e] Although the title of this paper might suggest that this paper should be classified as universal, the authors outline certain constructs that might be generic (universal) and others that may be specific to the particular information security action (pg. 21-23). Therefore, we have their unified model classified as pseudo-universal instead of universal in our classification system.

[f] This study used multiple scenarios to measure the effect of varying levels of organizational justice, perceived sanction severity and certainty, and neutralization. However, they used a single security threat (password theft) in all their scenarios.

Table A2. Quotes about Generalization and Limitations

Citation	Quotes or comments
Boss, Kirsch, Angermeier, Shingler & Boss (2009)	"In this study, precaution taking is defined as the degree to which individuals perceive they take measures to secure their computers and deal with information security in accordance with prescribed corporate security policies and procedures as well as through individual, proactive actions. Thus, in addition to following prescribed security policies and procedures, individuals should be generally aware of security threats. This general awareness can be enhanced through management formation and communication of formal information security policies (Straub, 1990; Straub & Welke, 1998)." p. 155 "Finally, this study used individuals that are employed in the health-care industry and, given the nature of the industry and the implementation of federal health privacy laws; it could be argued that this group is more accepting of formal controls than those in a different setting, therefore affecting the generalizability of the study." p. 161
Bulgurcu, Cavusoglu, & Benbasat (2010)	"For the sake of the generalizability of our results, we opted out of objective measurements of the ISP and actual compliance behavior. Case studies about ISP compliance that focus on employees from one or a few organizations would also be useful future research since such case studies could provide an opportunity to measure employees' ISA and their actual compliance with the requirements of their organizations' ISP objectively." p. 543 "Another limitation of the study may be that it captures compliance at a high level of abstraction. Use of scenarios can help reveal the differences in an employee's intentions to comply with specific rules and regulations, since scenarios can provide detailed explanations about specific policies (i.e., password policy, Internet use policy, remote access policy, and so on). Hence, future research should investigate employee compliance behavior in regard to these specific policies by providing detailed scenarios." p. 543

Table A2. Quotes about Generalization and Limitations

Chen, Ramamurthy, & Wen, (2012)	"We examined fairly extensively information security policy practices prevailing in industry [35] and surveyed the existing literature to ensure that our scenarios were realistic, familiar, and succinct, and that our corresponding findings were generalizable based on the scenarios." p. 170 "Since no 'optimal' number of scenarios has been suggested in the literature [76], we pilot tested the number of scenarios used in the study to ensure its adequacy." p. 170 "Care also needs to be taken when generalizing our findings to other companies in the financial industry." p. 171
D'Arcy , Herath , & Shoss (2014)	"Second, the phenomenon of ISP violations in this study is limited to more common, less extreme incidents that require minimal technical sophistication. Although we intentionally chose this route based on our literature review and feedback from IS security practitioners, a trade-off is that our findings may not generalize to more extreme, potentially disastrous security incidents. However, as research suggests a link between minor policy violations and more serious computer abuses [69], our findings have potential implications beyond the five types of ISP violations included here." p. 307-308
D'Arcy, Hovav, & Galletta, (2009)	"Because the goal of this study was to examine generalized patterns of IS misuse rather than specific behaviors depicted in each scenario, we created composite measures … by summing the responses to these items across the four misuse scenarios. Therefore, our general measures ... general indices of these variables. Silberman (1976) provides a theoretical rationale for using composite measures by suggesting that we may be able to predict generalized patterns of deviant behavior better than specific deviant events." p. 86 "Third, the measurement of IS misuse in this study is limited to the specific hypothetical scenarios chosen. Although the scenarios cover a wide range of security issues, they do not include every type of IS misuse. Future research should test the explanatory power of our model on a larger number of IS misuse behaviors. Additional analysis by scenario (e.g., Leonard and Cronan 2001, Leonard et al. 2004) could also test for differences in the impact of the security countermeasures on individual IS misuse behaviors." p. 94
Foth (2016)	None.
Guo, Yuan, Archer, & Connelly (2011)	"Second, this study used four specific security scenarios to solicit participant responses. Although this scenario-based method is commonly accepted in the literature, a limitation of this method is that the scenarios do not include every possible type of security violation. Future research should include more types of NMSVs to further test the proposed model. Third, the model focuses on NMSV intention as the ultimate independent variable. Although this practice is not uncommon in the IS literature, future research should try to measure actual security violations in a field setting to improve the model's external validity and generalizability. Finally, in the current study we limited our scope to NMSVs, which is one of the possible ways of how users deal with IS security issues at work. Future research should investigate how NMSVs relate to other types of security behavior. One particular issue is the investigation of the similarity and differences between NMSVs and malicious violations. For example, do they share any common antecedents? Can the two types of violations be explained from the same theoretical perspective?" p. 227
Hedström, Kolkowska, Karlsson, & Allen (2011)	"We use a qualitative case study (Benbasat et al., 1987; Myers, 2009) in order to understand the rationalities drawn upon by health care professionals in their information security practice." p. 376 "Other limitations concern the use of the model—which has been evaluated in one organization. This model was further developed in a Swedish context, and although we believe that the model as such is possible to transfer to other national settings, the use and results of the model, will of course depend on the specific culturally context where it is used." p. 383

Table A2. Quotes about Generalization and Limitations

Herath & Rao (2009)	None.
Hsu, Shih, Hung, & Lowry (2015)	None.
Johnston, Warkentin, McBride, & Carter (2016)	"Our study integrates situational and dispositional factors into a comprehensive model of information security policy violation intentions." p. 245 "In addition, we only assessed a single type of information security policy violation. Non-compliance with information security policies by failing to encrypt data removed from the workplace is only one of many possible violation behaviors (Guo, 2013; Willison & Warkentin, 2013). To some extent, the choice of one behavior limits the generalizability of the findings to other security misbehaviors. However, given the large number of manipulations included in the study, adding multiple violations was not feasible." p. 245
Johnston, Warkentin, & Siponen (2015)	None.
Kolkowska, Karlsson & Hedström (2017)	"Although our study indicates the usefulness of the VBC method, we do not claim that our findings are valid beyond the cases investigated. Indeed, some researchers have argued for the use of a nomothetic approach, because case studies are seen to be too context-specific to offer the possibility of generalisation (Benbasat et al., 1987). However, in order to evaluate the VBC method's usefulness we needed to apply the method in real settings, similar to those in which it will be applied in future. Here, case studies provide such settings (Yin, 1994), making case study-based research a relevant choice when combined with DSR." Section 3 para 2. "Employees' lack of compliance with information security policies is a perennial problem for many organisations. Currently, information security managers lack an ISAM to analyse the different rationalities that exist in relation to information security." Section 6, para 1.
Li, Sarathy, Zhang, & Luo (2014)	"Another limitation of our study is that we only examined internet abuses in general without differentiating specific types of internet abuses such as online shopping and cyberstalking in the workplace. The model may not be extendable to severe cybercrimes." p. 17
Lowry & Moody (2015)	"Finally, for exploratory purposes, we summarised the means for reactance according to ISP topic, which demonstrates that some ISPs naturally create more reactance than others, even when the underlying controls are the same (Table 7). Future research should identify the factors that distinguish ISP target behaviours cherished by users as highly personal freedoms from behaviours not similarly valued." p.453
Lowry, Posey, Bennett, & Roberts (2015)	"Likewise, we were unable to ensure that all our respondents had experienced similar organisational disincentives within similar periods. Rather, our findings represent the expressions of individuals from various organisational environments and internal security cultures. This fact, however, gives our study greater generalisability because of the broad nature of the sample and the respondents' organisational experiences. However, with regard to the links between specific disincentives and behaviours, longitudinal or experimental research would be illuminating." p. 218
Menard, Bott & Crossler (2017)	"Several secure behaviors have been analyzed using security appeals, but our study featured just one recommended behavior: the installation and use of a password manager, which was selected due to its current low adoption rate. While our findings are insightful for PMT adaptations and overall behavioral InfoSec research, retesting our appeals using a variety of other behaviors, such as performing data backups or using antivirus software, may highlight interesting differences. Researchers may elect to study just one behavior or craft several different appeals focusing on single specific behaviors." p. 1225

Table A2. Quotes about Generalization and Limitations

Moody, Siponen & Pahnila (2018)	"We explained the non-significance of social factors or subjective norms due to the types of scenarios (types of these insecure acts) we had. We maintain that different results could be obtained by scenarios that examine different types of ISS behavior. For example, our scenarios, such as sharing passwords or insecure USB practices, may not be visible socially, nor are they widely socially unacceptable in a work environment (Siponen et al. 2010)." p. 306 "Our scenarios contained three types of ISS policy violations; hence, the applicability of the UMICPS beyond these three types of violations is not known, as discussed in the previous subsection." p. 307
Myyry, Siponen, Pahnila, Vartiainen, & Vance (2009)	"Our study used a case wherein a nurse pondered whether he should share his password with co-workers and, again, care should be taken in generalizing these findings to other situations. Another limitation of our study is its use of a single scenario. In studying hypothetical moral reasoning, one finds that the use of at least three scenarios is recommended (Rest, 1979; Colby & Kohlberg, 1987). However, deVries & Walker (1986) based their scoring of moral judgment on a single case. Therefore, while the use of three scenarios is common, previous research has also utilized just one scenario." p. 136
Posey, Roberts, & Lowry (2015)	Uses Posey et al. (2013) to justify universal PMB measurements. Includes numerous past PMBs in the analyses.
Siponen & Vance (2010)	"To ensure the generalizability of our findings across different kinds of IS security policy violations, we designed three different scenarios describing common and important policy violations in coordination with 54 information security professionals" p. 492
Straub (1990)	None.
Vance, Lowry, & Eggett (2013)	None. Conclusions focused on access policy violations and did not generalize beyond this security threat context.
Vance, Lowry, & Eggett (2015)	None. Conclusions focused on access policy violations and did not generalize beyond this security-threat context.
Willison, Warkentin & Johnston (2018)	None.

Appendix B

Table B1. Study 1 ISP-Mandated Requirements

Security threat	DoD security policy requirements (Study 1)
Phishing	Assume all unsolicited information requests are phishing attempts
	Do not access the web by selecting links in emails or pop-up messages
	Delete any suspicious email
	View all email in the plain text
	Report emails requesting personal information to your security POC
	Use caution when visiting sites with expired certificates
	Report trusted sites with expired certificates
	Never reveal any personal information in an email
	Look for digital signatures
	Contact sender by other means before opening a doubtful attachment or link
	Never give out organizational, personal, or financial information to anyone by email
Tailgating	Use **ONLY** (emphasis included) your own security badge or key code
	Never grant access for someone else
	Maintain possession of your security badge at all times
	Challenge people without proper badges
	Be wary when people with visitor's badges ask about other people's office locations
	Report suspicious activity
Removable Flash Media	Use of removable flash media is forbidden except in case of command-directed and documented mission essential tasks per Chairman of the Joint Chiefs of Staff Instruction 6510.01F. If approved, the following conditions must be met:
	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.
	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.

Table B2. Study 1 Survey Measurement Items

Construct	Definition and item source(s)	Survey question / Measurement item
Behavioral intent (BINT)	Self-reported intention to perform a security-related behavior. Items adapted from Ajzen (1991), Bulgurcu et al. (2010).	I intend to comply with the _____ requirements of the ISP of my organization in the future.
		I intend to protect information and technology resources according to the _____ requirements of the ISP of my organization in the future.
		I intend to carry out my _____ responsibilities prescribed in the ISP of my organization when I use information and technology in the future.
Subjective norms (SNORM)	The perceived social pressure to engage or not to engage in a security-related behavior. Items adapted from Taylor and Todd (1995), Herath and Rao (2009).	My peers/colleagues think that I should comply with the _____ requirements of the ISP.
		My executives think that I should comply with the _____ requirements of the ISP.
		My subordinates (or those junior to me) think that I should comply with the _____ requirements of the ISP.
Attitude (ATT)	The self-reported degree to which performance of a security behavior is positively or negatively valued. Items adapted from Ajzen (1991); Herath and Rao (2009).	Adopting ISP-related security technologies and practices is important for protecting against _____ threats.
		Adopting ISP-related security technologies and practices is beneficial for protecting against _____ threats.
		Adopting ISP-related security technologies and practices is helpful for protecting against _____ threats.
Perceived behavioral control (PBC)	One's perceived ability to perform a given behavior in the presence of factors that may facilitate or impede performing the behavior. Items adapted from Taylor & Todd (1995).	I would be able to follow the ISP for _____ threats.
		Following the ISP for _____ threats is entirely within my control.
		I have the resources and knowledge and ability to follow the ISP for _____ threats.
Self-efficacy (SEFF)	One's perceived ability to successfully complete a security-related behavior. Items adapted from Bandura (1991); Herath & Rao (2009).	I have the necessary skills to fulfill the _____ requirements of the ISP.
		I have the necessary knowledge to fulfill the _____ requirements of the ISP.
		I have the necessary competencies to fulfill the _____ requirements of the ISP.
Response efficacy (REFF)	The extent one believes a recommended security response effectively deters or mitigates a threat. Items adapted from Rippetoe & Rogers (1987), Milne et al. (2000), Workman et al. (2008).	Efforts to keep my organization's information resources safe from _____ threats are:
		The effectiveness of available measures to protect my organization's information resources from _____ threats is:
		The preventative measures available to me to comply with the _____ requirements of the ISP are:
Perceived vulnerability (PVUL)	One's belief in how susceptible they feel to a specified security threat. Items adapted from Champion (1984), Ng et al. (2009).	The chances of experiencing a/an _____ threat at work is:
		There is a good possibility that I will encounter a/an _____ threat to my organization:
		I am likely to encounter a/an _____ threat to my organization:

Table B2. Study 1 Survey Measurement Items

Perceived threat severity (TSEV)	One's perception of how serious a security threat would be to themselves. Items adapted from Ng et al. (2009).	Having my organization's information resources accessed by unauthorized parties because of _____ threats is:
		Having someone successfully attack and damage my organization's information resources because of a/an _____ threat is:
		Attacks on my organization's information resources due to _____ violations of the ISP are:
Perceived sanction severity (SSEV)	One's perception of how serious a penalty they would incur if they did not behave in accordance with formal security requirements. Items adapted from Herath & Rao (2009).	My organization disciplines employees who fail to follow the _____ requirements of ISP.
		My organization terminates employees who repeatedly fail to follow the _____ requirements of the ISP.
		If I were caught violating the _____ requirements of the ISP, I would be severely punished.
Perceived sanction probability (SPROB)	The perceived chance that one would get caught and punished for violating a required security behavior. Items adapted from Herath & Rao (2009).	Employees that fail to follow the _____ requirements of the ISP would be caught, eventually.
		The likelihood the organization would discover that an employee failed to follow the _____ requirements of the ISP is:
Perceived cost of compliance (PCOMP)	An estimate of the resources required and/or negative effects that result from complying with a required security behavior. Items adapted from Bulgurcu et al. (2010).	Complying with the _____ requirements of the ISP is time consuming for me.
		Complying with the _____ requirements of the ISP is time burdensome for me.
		Complying with the _____ requirements of the ISP is time costly for me.
Perceived benefit of compliance (PBEN)	An estimate of the personal rewards received from complying with the required security behavior. Items adapted from Bulgurcu et al. (2010).	My compliance with the _____ requirements of the ISP would be favorable to me.
		My compliance with the _____ requirements of the ISP would result in benefits to me.
		My compliance with the _____ requirements of the ISP would create advantages for me.
Perceived cost of noncompliance (PNCOMP)	An estimate of the negative effects that result from failing to comply with the required security actions. Items adapted from Bulgurcu et al. (2010).	My noncompliance with the _____ requirements of the ISP would be harmful to me.
		My noncompliance with the _____ requirements of the ISP would impact me negatively.
		My noncompliance with the _____ requirements of the ISP would create disadvantages for me.

Table B3. Study 1 Factor Loadings

Construct	Item	Generic measure			Flash media			Phishing			Tailgating		
		Factor load	Mean	Std dev	Factor load	Mean	Std dev	Factor load	Mean	Std dev	Factor load	Mean	Std dev
Behavioral intent (BINT)	BINT1	0.95	6.66	0.48	0.97	6.67	0.58	0.92	6.74	0.45	0.95	6.57	0.65
	BINT2	0.97	6.66	0.48	0.98	6.69	0.56	0.98	6.73	0.48	0.94	6.60	0.63
	BINT3	0.99	6.66	0.48	0.97	6.67	0.58	0.92	6.71	0.49	0.86	6.56	0.70
Subjective norms (SNORM)	SN1	0.89	6.42	0.73	0.95	6.35	0.89	0.90	6.49	0.70	0.92	6.33	0.87
	SN2	0.67	6.66	0.56	0.61	6.66	0.64	0.71	6.68	0.54	0.65	6.59	0.66
	SN3	0.71	6.29	0.84	0.83	6.21	1.00	0.75	6.33	0.84	0.83	6.15	1.04
Attitude (ATT)	ATT1	0.94	6.60	0.50	0.96	6.49	0.70	0.90	6.57	0.57	0.80	6.53	0.68
	ATT2	0.94	6.61	0.51	0.94	6.51	0.71	0.97	6.56	0.60	0.91	6.52	0.68
	ATT3	0.89	6.62	0.49	0.91	6.50	0.72	0.87	6.53	0.63	0.87	6.55	0.65
Perceived behavioral control (PBC)	PBC1	0.85	6.39	0.66	0.88	6.56	0.60	0.82	6.49	0.64	0.85	6.51	0.66
	PBC2	0.86	6.30	0.84	0.76	6.44	0.84	0.81	6.21	0.98	0.81	6.36	0.93
	PBC3	0.85	6.34	0.73	0.86	6.47	0.73	0.88	6.31	0.81	0.84	6.42	0.81
Self-efficacy (SEFF)	SE1	0.94	6.52	0.58	0.96	6.58	0.59	0.96	6.49	0.70	0.93	6.54	0.67
	SE2	0.95	6.47	0.59	0.95	6.58	0.57	0.98	6.48	0.67	0.95	6.53	0.62
	SE3	0.95	6.52	0.57	0.97	6.59	0.58	0.96	6.49	0.68	0.97	6.55	0.61
Response efficacy (REFF)	RE1	0.82	5.74	0.89	0.87	5.65	0.99	0.82	5.65	0.99	0.93	5.39	1.25
	RE2	0.92	5.76	0.81	0.95	5.67	0.93	0.93	5.67	0.93	0.95	5.41	1.21
	RE3	0.84	5.97	0.79	0.74	5.85	0.93	0.84	5.85	0.93	0.82	5.66	1.19
Perceived vulnerability (PVUL)	PVUL1	0.83	4.42	1.66	0.71	4.75	1.65	0.82	4.75	1.65	0.81	4.24	1.67
	PVUL2	0.97	4.67	1.60	0.98	4.86	1.61	0.95	4.86	1.61	0.97	4.39	1.62
	PVUL3	0.93	4.57	1.62	0.94	4.78	1.65	0.90	4.78	1.65	0.90	4.29	1.66
Perceived threat severity (TSEV)	TSEV1	0.95	6.00	1.07	0.91	6.07	1.05	0.95	6.07	1.05	0.90	5.79	1.21
	TSEV2	0.90	6.23	0.99	0.91	6.25	0.96	0.90	6.25	0.96	0.93	6.03	1.22
	TSEV3	0.90	6.04	1.05	0.93	6.06	1.05	0.91	6.06	1.05	0.92	5.86	1.16
Perceived sanction severity (SSEV)	SSEV1	0.71	5.35	1.36	0.74	5.54	1.31	0.77	5.14	1.51	0.82	5.04	1.62
	SSEV2	0.74	4.42	1.50	0.64	4.43	1.50	0.75	4.30	1.44	0.76	4.22	1.53
	SSEV3	0.74	5.11	1.47	0.80	5.33	1.46	0.80	4.91	1.60	0.82	4.80	1.65
Perceived sanction probability (SPROB)	SP1	0.72	5.44	1.22	0.63	5.61	1.20	0.72	5.31	1.30	0.78	5.12	1.46
	SP2	0.86	4.88	1.37	0.82	5.35	1.38	0.88	4.86	1.47	0.88	4.61	1.53
Perceived cost of compliance (PCOMP)	PC1	0.81	3.97	1.76	0.87	3.90	1.94	0.86	3.27	1.72	0.90	3.34	1.73
	PC2	0.99	3.46	1.71	0.92	3.75	1.91	0.99	2.98	1.60	0.97	3.08	1.60
	PC3	0.77	2.88	1.63	0.74	3.10	1.84	0.87	2.67	1.54	0.87	2.71	1.54
Perceived benefit of compliance (PBEN)	PB1	0.65	5.86	1.10	0.75	5.64	1.35	0.67	5.92	1.10	0.72	5.77	1.15
	PB2	0.85	5.45	1.27	0.88	5.20	1.48	0.86	5.49	1.27	0.87	5.36	1.32
	PB3	0.79	4.93	1.37	0.84	4.69	1.49	0.76	4.97	1.34	0.76	4.87	1.36
Perceived cost of non-compliance (PNCOMP)	PNC1	0.71	5.69	1.39	0.71	5.73	1.34	0.69	5.73	1.41	0.81	5.58	1.39
	PNC2	0.81	5.83	1.25	0.82	5.77	1.34	0.82	5.87	1.24	0.87	5.64	1.43
	PNC3	0.70	5.42	1.60	0.67	5.33	1.65	0.71	5.45	1.61	0.68	5.30	1.63

Table B4. Study 2 ISP-Mandated Requirements

Security threat	University-specific security policy requirements (Study 2)
Password sharing	Access to computers, software applications, and electronic information is frequently controlled through user identifiers and passwords. Users are responsible for creating and protecting passwords that grant them access to resources. Because shared passwords and identifiers present a major security risk, user identifiers and passwords must never be shared. Passwords that provide access to university resources must not be stored on personal computers and must not be displayed on sticky notes or scraps of paper sitting by computers.
Workstation lock	Users shall log off from applications, computers, and networks when finished. If computers are located in secure offices or laboratories, Users shall not leave unattended personal computers with open sessions without locking office doors, locking the computer, or providing similar protection. If computers are located in the open or in a shared computer lab, users shall complete their session and log off fully. The use of boot or other start-up passwords is recommended in environments where unauthorized persons may have physical access to computers. Shutting off computer monitors when not in use can also discourage such persons from attempting to use computers for snooping and other unauthorized activity (while also conserving energy). Many monitors have an automatic shut-down feature that does this. Reactivating the monitor to use the computer must require a password, the same way a screensaver would.

Table B5. Study 2 Scenarios

Security threat	Employee[a]	Student[a]
Workstation locking/logout[b]	Jordan works in the front office of a popular degree program offered at the university. His duties require frequent interaction with faculty, staff, students, and outside clients both at and away from his desk. Jordan is aware of the university's policy that employees must log out of or lock their computer workstation when not using it. When Jordan knows or believes he is going to be away from his desk for an extended period of time (one hour or longer), he locks his computer. However, based upon his typical schedule of frequent departures to and from his desk, Jordan mostly keeps his user account logged in to save him time in performing his normal duties.	Jordan is studying in one of the open computer labs on campus. He'll be there for most of the day working on assignments for a couple of different classes and preparing for an exam. Generally, he spends most of his time in the computer room when he studies, but he takes lots of breaks to go to the restroom, eat a snack or drink, or talk to his friends. Jordan is aware of the university's policy that students must log out of or lock their computer workstation when not using it. When Jordan knows or believes he is going to be away from his desk for an extended period of time, he locks or logs out of the computer. However, since he won't usually be too far from the computer room, Jordan mostly keeps his user account logged in to save him time when he does need to use the computer.
Password sharing[b]	Casey splits her time working in the offices of two different degree programs offered at the university. In one of the offices, she is responsible for tracking the current status of research grant funding allocations for the entire department; this information is accessed using a special program that is only loaded on her office computer hard drive. Casey is aware of the university's policy that each computer workstation must be password protected and that passwords are not to be shared. However, since Casey moves between job locations regularly, she shared the password to her office computer with several co-workers so that they can get the information they need when they need it. Casey expects that sharing her password will save her co-workers a lot of time and effort since they won't have to wait for her to get back to the office.	Casey is a college junior that is active in several student groups and is an officer in her sorority. Because she has a work study that allows her to print anything she needs related to her schoolwork, she never uses any of her 1000 free pages of printing each semester. Casey is aware of the university's policy that individual account user id's and passwords are not to be shared. However, because many of her sorority sisters and friends have run out of their print quota, she provides her user ID and password to those that need it so that they can print from her personal account.

[a] Study 2 participants who identified themselves as employees were shown the employee-specific scenarios while all others were shown the student-specific scenarios

[b] We used Moody et al. (2018) and Siponen and Vance (2010) as our guides to construct these two scenarios, but we did adapt these scenarios to fit our organizational context.

Table B6. Study 2 Survey Measurement Items

Construct	Survey Question/Measurement Item
Behavioral intent (BINT)	It is likely that I would probably do what Jordan did in the described scenario.
	I would act in the same way as Jordan did if I were in the same situation.
	If I experienced similar circumstances as Jordan, I would probably operate in a similar manner.
Subjective norms (SNORM)	My peers/colleagues think that I should do what Jordan did.
	My supervisors/managers think that I should do what Jordan did.
	My subordinates/juniors (or those who look up to me) think that I should do what Jordan did.
Attitude (ATT)	It is important for Jordan to follow the TU workstation lock/logout policy in order to protect the organization against security threats.
	It would be beneficial for Jordan to follow the TU workstation lock/logout policy in order to protect the organization against security threats.
	In order to protect the organization against security threats, it would be helpful for Jordan to following the TU workstation lock/logout policy.
Perceived behavioral control (PBC)	I would be able to follow TU's workstation lock/logout policy.
	Personally following the workstation lock/logout policy is entirely within my control.
	I have the resources and knowledge and ability to follow the workstation lock/logout policy.
Self-efficacy (SEFF)	I have the necessary skills to fulfill the workstation lock/logout policy requirements.
	I have the necessary knowledge to fulfill the workstation lock/logout policy workstation lock/logout policy requirements.
	I have the necessary competencies to fulfill workstation lock/logout policy requirements.
Response efficacy (REFF)	Doing the opposite of what Jordan did would make my organization's information resources safer.
	Following the workstation lock/logout policy is effective at protecting my organization's information resources from security threats related to unauthorized access:
	The preventative measures described in the workstation lock/logout policy are:
Perceived vulnerability (PVUL)	The chances of experiencing a security threat doing what Jordan did is:
	The possibility that I will encounter an information security threat to my organization by doing what Jordan did is:
	Encountering an information security threat related to unauthorized computer access at my organization is:
Perceived threat severity (TSEV)	Having my organization's information resources accessed by unauthorized parties because of Jordan's failure to follow the workstation lock/logout policy is:
	Having someone successfully attack and damage my organization's information resources because Jordan's failure to follow the workstation lock/logout policy is:
	Attacks on my organization's information resources because of Jordan's failure to follow the workstation lock/logout policy are:
Perceived sanction severity (SSEV)	My organization will discipline employees, like Jordan, who fail to follow the workstation lock/logout requirements of ISP.
	My organization will terminate employees who repeatedly fail to follow the workstation lock/logout requirements of the ISP.

Table B6. Study 2 Survey Measurement Items

	If I were caught doing what Jordan did, I would be severely punished.
Perceived sanction probability (SPROB)	My organization will discipline employees, like Jordan, who fail to follow the workstation lock/logout requirements of the ISP.
	My organization will terminate employees who repeatedly fail to follow the workstation lock/logout requirements of the ISP.
	If I were caught doing what Jordan did, I would be severely punished.
Perceived cost of compliance (PCOMP)	Complying with the workstation lock/logout policy is time consuming.
	Complying with the workstation lock/logout policy is burdensome.
	Complying with the workstation lock/logout policy is inconvenient.
Perceived benefit of compliance (PBEN)	Doing the opposite of Jordan (i.e., complying with the workstation lock/lockout policy) would be favorable to me.
	My compliance with the workstation lock/logout policy would result in benefits to me.
	My compliance with the workstation lock/logout policy would create advantages for me.
Perceived cost of noncompliance (PNCOMP)	Violating the workstation lock/lockout like Jordan did would be harmful to me.
	Behaving like Jordan and violating the workstation lock/lockout policy would impact me negatively.
	My noncompliance with the workstation lock/logout policy would create disadvantages for me.

Notes: Construct definitions and sources for Study 2 were the same as in Study 1 (shown in Table B1) with the following comments and exceptions:

1) The generic measures were the same for both Study 1 & Study 2.
2) Scenario-focused items used to measure workstation locking/logout and password sharing compliance were modified using Moody et al. (2018) and Siponen & Vance (2010) as a guide.
3) Latent construct items were measured on a 7-point Likert scales (both positive and negative). Study 1 also used both negative and positive scales but Study 2 incorporated more negatively worded items than Study 1.
4) The name "Jordan" and threat-specific security action "workstation lock/logout" is replaced with "Casey" and "password sharing" for all items related to the password-sharing scenario.

Table B7. Study 2 Factor Loadings

Construct	Item	Generic measure			Workstation locking			Password sharing		
		Factor load	Mean	Std dev	Factor load	Mean	Std dev	Factor load	Mean	Std dev
Behavioral intent (BINT)	BINT1	0.92	6.25	1.33	0.96	4.02	1.88	0.97	2.88	1.86
	BINT2	0.97	6.33	1.25	0.98	3.94	1.88	0.98	2.86	1.84
	BINT3	0.96	6.33	1.19	0.96	4.00	1.88	0.98	2.87	1.86
Subjective norms (SNORM)	SN1	0.88	5.74	1.21	0.91	3.89	1.62	0.88	3.35	1.81
	SN2	0.77	6.16	1.18	0.77	3.16	1.59	0.71	2.51	1.59
	SN3	0.88	5.75	1.28	0.91	3.74	1.61	0.91	3.17	1.70
Attitude (ATT)	ATT1	0.92	6.26	1.10	0.75	5.63	1.21	0.88	5.80	1.21
	ATT2	0.94	6.22	1.10	0.89	5.73	1.08	0.91	5.72	1.21
	ATT3	0.89	6.21	1.10	0.95	5.82	1.02	0.93	5.83	1.16
Perceived behavioral control (PBC)	PBC1	0.74	5.99	1.22	0.81	5.92	1.11	0.79	6.03	1.10
	PBC2	0.83	5.77	1.33	0.74	6.14	1.09	0.83	6.16	1.18
	PBC3	0.95	5.64	1.40	0.93	6.21	1.02	0.91	6.21	1.08
Self-efficacy (SEFF)	SE1	0.91	5.76	1.32	0.96	6.24	0.98	0.92	6.25	0.99
	SE2	0.95	5.68	1.36	0.90	6.20	1.04	0.98	6.22	1.06
	SE3	0.96	5.78	1.33	0.93	6.25	0.95	0.96	6.22	1.11
Response efficacy (REFF)	RE1	0.88	5.42	1.06	0.70	5.45	1.27	0.88	5.65	1.25
	RE2	0.94	5.33	1.07	0.92	5.49	1.18	0.96	5.60	1.21
	RE3	0.77	5.39	1.04	0.87	5.47	1.16	0.85	5.60	1.19
Perceived vulnerability (PVUL)	PVUL1	0.87	3.83	1.61	0.85	4.02	1.45	0.93	3.49	1.52
	PVUL2	0.96	3.96	1.65	0.91	4.11	1.44	0.94	3.71	1.57
	PVUL3	0.94	3.91	1.62	0.69	3.96	1.47	0.88	3.64	1.56
Perceived threat severity (TSEV)	TSEV1	0.92	4.00	1.73	0.90	4.02	1.47	0.89	4.48	1.57
	TSEV2	0.97	3.83	1.81	0.96	3.96	1.54	0.95	4.38	1.57
	TSEV3	0.85	4.01	1.72	0.93	3.87	1.47	0.97	4.41	1.53
Perceived sanction severity (SSEV)	SSEV1	0.84	3.36	1.60	0.89	3.85	1.53	0.88	3.56	1.60
	SSEV2	0.92	3.38	1.87	0.93	4.00	1.78	0.96	3.78	1.78
	SSEV3	0.82	3.38	1.79	0.85	4.23	1.76	0.85	3.74	1.74
Perceived sanction probability (SPROB)	SP1	0.86	4.70	1.58	0.87	4.16	1.54	0.94	4.51	1.56
	SP2	0.86	4.48	1.60	0.91	4.11	1.52	0.92	4.46	1.63
Perceived cost of compliance (PCOMP)	PC1	0.83	4.75	1.67	0.88	4.09	1.61	0.88	4.43	1.60
	PC2	0.92	3.25	1.52	0.92	3.63	1.80	0.90	2.76	1.62
	PC3	0.97	3.06	1.49	0.94	3.47	1.72	0.98	2.87	1.65
Perceived benefit of compliance (PBEN)	PB1	0.75	2.61	1.43	0.86	3.92	1.81	0.86	3.12	1.71
	PB2	0.74	5.26	1.22	0.66	5.16	1.39	0.65	5.16	1.50
	PB3	0.93	5.25	1.19	0.91	4.84	1.45	0.96	5.04	1.42
Perceived cost of noncompliance (PNCOMP)	PNC1	0.81	5.00	1.21	0.92	4.67	1.49	0.87	4.94	1.43
	PNC2	0.86	4.86	1.46	0.83	4.55	1.50	0.87	4.91	1.50
	PNC3	0.97	4.88	1.45	0.92	4.47	1.50	0.93	4.86	1.51

About the Authors

Sal Aurigemma. Sal Aurigemma researches employee information security policy compliance, improving end-user and small business information security practices, and end-user computing. He has published in a variety of peer-reviewed journals, including *Journal of the Association for Information Systems*, *Computers & Security*, *Information and Computer Security*, *Decision Support Systems*, *Journal of Organizational and End User Computing*, and *Journal of Information Systems Security*.

Thomas Mattson. Thomas Mattson is an assistant professor at the University of Richmond. He has published in a variety of peer-reviewed journals, including *MIS Quarterly*, *Journal of the Association for Information Systems*, *Communications of the Association for Information Systems*, and *Computers & Security*. He researches a variety of information systems topics including behavioral information security and online networks of practice.