MIS Quarterly

RESEARCH ARTICLE

TOWARD A UNIFIED MODEL OF INFORMATION SECURITY POLICY COMPLIANCE[1]

Gregory D. Moody
University of Nevada, Las Vegas, 4505 S. Maryland Parkway,
Las Vegas, NV 89154 U.S.A. {gregory.moody@unlv.edu}

Mikko Siponen
Faculty of Information Technology, University of Jyväskylä, P.O. Box 35,
FI-40014 Jyväskylä FINLAND {mikko.t.siponen@jyu.fi}

Seppo Pahnila
Faculty of Information Technology and Electrical Engineering, University of Oulu, P.O. Box 8000,
FI-90014 Oulu FINLAND {seppo.pahnila@oulu.fi}

Information systems security (ISS) behavioral research has produced different models to explain security policy compliance. This paper (1) reviews 11 theories that have served the majority of previous information security behavior models, (2) empirically compares these theories (Study 1), (3) proposes a unified model, called the unified model of information security policy compliance (UMISPC), which integrates elements across these extant theories, and (4) empirically tests the UMISPC in a new study (Study 2), which provided preliminary empirical support for the model. The 11 theories reviewed are (1) the theory of reasoned action, (2) neutralization techniques, (3) the health belief model, (4) the theory of planned behavior, (5) the theory of interpersonal behavior, (6) the protection motivation theory, (7) the extended protection motivation theory, (8) deterrence theory and rational choice theory, (9) the theory of self-regulation, (10) the extended parallel processing model, and (11) the control balance theory. The UMISPC is an initial step toward empirically examining the extent to which the existing models have similar and different constructs. Future research is needed to examine to what extent the UMISPC can explain different types of ISS behaviors (or intentions thereof). Such studies will determine the extent to which the UMISPC needs to be revised to account for different types of ISS policy violations and the extent to which the UMISPC is generalizable beyond the three types of ISS violations we examined. Finally, the UMISPC is intended to inspire future ISS research to further theorize and empirically demonstrate the important differences between rival theories in the ISS context that are not captured by current measures.

Keywords: Information system security, unified theory, survey

[1]Ron Thompson was the accepting senior editor for this paper. Raj Sharman served as the associate editor.

The appendices for this paper are located in the "Online Supplements" section of the *MIS Quarterly*'s website (http://www.misq.org).

Introduction

The rapidly increasing use of information technology (IT) by organizations has drastically altered assets and critical resources, as they have become digital and thus more easily transferrable (Johnston et al. 2015; Siponen 2005). In such organizations, it is important to ensure that information is not leaked or inadvertently modified (D'Arcy and Hovav 2007; Willison and Warkentin 2013). In protecting the resources and securing the important information of organizations from such threats, the starting point is the development of information security policy documents that list, for example, appropriate and inappropriate ISS actions for employees (Baskerville and Siponen 2002; Straub et al. 2008). A typical example of appropriate ISS behavior would be the requirement to have a difficult-to-guess password (Siponen and Vance 2010).

Unfortunately, research shows that employees seldom follow the appropriate ISS actions prescribed in the security policies, and that they rather behave in an insecure manner, even if they are aware of said policies (Boss et al. 2009; Puhakainen and Siponen 2010).[2] Understanding why individuals engage (or intend to engage) in such insecure information security actions has been a key area of ISS research over the past 30 years (D'Arcy and Herath 2011; Warkentin and Willison 2009). This research has advanced various models that have been taken from different disciplines, such as criminology (e.g., deterrence theory), psychology (e.g., theory of planned behavior), social psychology (e.g., habit), and health psychology (e.g., protection motivation theory) (D'Arcy and Herath 2011; Siponen and Vance 2014). Figuratively speaking, the application of theories from different disciplines has resulted in a jungle of competing ISS behavioral models that may not be easily comparable. More precisely, the untangling of this jungle for information security practitioners and ISS scholars can be hindered by a number of issues, including the following three: First, many of these models have components that resemble each other but are called by different names. For example, how are attitudes in the theory of reasoned action empirically different from protection motivation in protection motivation theory (D'Arcy and Herath 2011; Siponen and Vance 2014)? In the same way, how are sanctions in deterrence theory (D'Arcy and Hovav 2007; Siponen and Vance 2010) similar to costs in rational choice theory (Bulgurcu et al. 2010; Vance and Siponen 2012) or constraints in control balance theory (Tittle 1995)?

The second issue is that these competing theories in ISS are often tested in isolation rather than in comparison with each other. With few exception (e.g., Johnston et al. 2015; Siponen and Vance 2010), we cannot find studies that have empirically compared two or more approaches. Based on his review of successful science, Laudan (1978) argued that scientific theories (in natural sciences) are not evaluated in "a competitive vacuum," but rather against each other (p. 71). In other words, Laudan maintained that the acceptance of theories in science is based less on whether the theory in question meets some "absolute measures" and more on which theory or model among the available theories offers the best explanation or solution for the specific phenomenon (p. 71).

Third, while there are a few studies that have integrated two theories (e.g., Herath and Rao 2009; Johnston et al. 2015; Puhakainen and Siponen 2010) or extended reference theories (D'Arcy et al. 2007), little is known about the extent to which the different ISS behavioral models available in the literature complement each other.

In a similar situation in IT use research, scholars have called for unified models in order to progress toward a synthesis of the jungle of alternative theories (Venkatesh et al. 2003; Venkatesh et al. 2012). Unification is an attempt to find empirical commonalities between different theories that have similar concepts as well as to examine the extent to which the different models can be used to complement each other. Following Venkatesh et al. (2003), we first review 11 existing theories, which are either used or can be used to explain employees' (non)compliance (intention) with information security policies. Second, we empirically compare these theories in Study 1 (Venkatesh et al. 2003). Third, based on empirical and conceptual similarities across these models (Venkatesh et al. 2003), we propose a unified model called the unified model of information security policy compliance (UMISPC), which offers a tentative proposal to integrate elements from the reviewed theories. Finally, following Venkatesh et al. (2003), we test this unified model with a different data collection (in Study 2) than that used to compare the existing ISS models (in Study 1).

While the UMISPC must be further tested, or even revised, to account for different types of information security actions, we believe that the UMISPC and follow-up studies to examine it in different contexts contribute to IS security (1) research and theory, (2) practice, and (3) education. *For ISS research and theory*, a study that empirically compares and synthesizes the existing models would be valuable, since there are many ISS approaches (Hirschheim et al. 1995; Siponen 2005). The UMISPC takes a first step toward this goal by examining the extent to which the available models are empirically similar

[2]In this paper, "information policy compliance" refers to employees' compliance with information security policies, procedures, or guidelines. Their names and how many regulative documents there are in organizations may vary from one organization to another. Noncompliance is thus a synonym for information security policy violation.

as well as the extent to which the disparate theories complement each another. In regard to future research and theorizing, the UMISPC is intended to inspire future research in four ways. First, the UMISPC can be tested in different contexts to determine its boundaries and identify situations in which its components fail to explain a phenomenon. Second, future research can further extend the UMISPC by adding additional constructs and moderators in different contexts or by seeking to further the boundary conditions of the theory. Third, future research may find that some of the UMISPC constructs may be irrelevant in certain ISS contexts. Fourth, future research can test our results with different measures. Finally, we hope our unification research inspires future IS research to further theorize and empirically demonstrate the important differences between rival theories in the ISS context that are not captured by current measures.

ISS practitioners may be interested in understanding why employees do or do not comply with ISS policies (Siponen and Vance 2010). Such an understanding can offer a basis for information security education or for intervention campaigns in organizations. With the different ISS models/theories, practitioners face the issue of choosing which of them to apply. This raises the question: Should they choose from among deterrence theory, rational choice, habit, protection motivation theory, etc., or should they apply all of these at the same time, which can be impractical? Similarly, the extent to which the existing models complement each other empirically may be unclear. The UMISPC, albeit currently tentative, suggests one answer to these questions that future research may be able to refine or further support. Practitioners can use the UMISPC not only to diagnose why some employees fail to comply with ISS policies in an organization, but why others *do* comply. Finally, our article also offers an inventory of the existing models by listing all previously identified constructs on ISS behavior in one paper.

Expected contribution to ISS education. While students should be educated on the different ISS behavior theories/models available, it would be difficult to study all of them in one course (Siponen 2005). The UMISPC offers one model in one article that synthesizes the available theories into a single, comprehensive model.

The rest of the paper is organized as follows. The next section highlights previous theories in the information security research stream. The following section presents the methodology for comparing and contrasting these theories in the same context, and the subsequent section presents the results of this study, including the UMISPC. The final section presents the discussion, including contributions to theory and implications for research and practice.

Literature Review: Extant Models Used to Explain ISS Policy Compliance

We performed a literature review of extant ISS research and augmented this review with potential theories that are not yet used in ISS, such as the control balance theory, the theory of self-regulation, and the theory of interpersonal behavior. This review identified several theories to explain why individuals (intend to) behave in a manner that may be contrary to ISS policies. These are presented in Table 1.

Theory Summary

As an aid for the readers of this study, we summarized the main points of the theories in Table 1 and the main constructs in Table 2.

Techniques or Theory of Neutralization

Sykes and Matza (1957) proposed the theory of neutralization (ToN) to explain how individuals are able to overcome social norms and other deterrent mechanisms and engage in deviant behaviors. The basic tenet of this theory is that individuals rationalize reasons for why they are able to make an exception to a rule, policy, or law, thereby violating the accepted norm (Siponen and Vance 2010). The ToN expands our understanding of ISS research by suggesting that people generate excuses as rationalizations, through which they justify their insecure behaviors to themselves. Siponen and Vance (2010), Barlow et al. (2013), and Teh et al. (2015) used neutralization techniques to explain employee noncompliance (intention) with ISS policies within organizations.

Health Belief Model

M. H. Becker (1974) proposed the health belief model (HBM) to explain health behavior. Specifically, Becker argued that risk was assessed based on its severity and the individual's susceptibility to the risk. *Severity* refers to the perceived seriousness or magnitude of the risk associated with a given behavior (Witte et al. 1996). In turn, *susceptibility* denotes the perceived likelihood of experiencing the threat (Witte et al. 1996). A similar approach was adopted by the PMT (Rogers 1975) and the EPPM (Witte 1992).

Becker proposed that when individuals perceive a high risk associated with a behavior they will engage in what are perceived as safer behaviors in order to avoid the threat. In order for a behavior to be deemed safe, it must provide rewards and

Table 1. Summary of Reviewed Theories

Theory	Source	Field	Main Constructs	Intention Predictor	Behavior Predictor	Example Application
Neutralization theory (ToN)	Sykes and Matza (1957)	Criminology	Neutralization	N/A	N/A	How one rationalizes deviant acts (see Siponen and Vance 2010)
Health belief model (HBM)	Becker (1974)	Public health	- Costs - Rewards - Severity - Susceptibility	- Costs - Rewards - Severity - Susceptibility	- Intention	How to predict healthy security behaviors (see Ng et al. 2009)
Theory of reasoned action (TRA)	Fishbein and Ajzen (1975)	Psychology	- Attitude - Subjective norms	- Attitude - Subjective norms	- Intention	How beliefs and subjective norms logically shape behavior (see Bulgurcu et al. 2010)
Protection motivation theory (PMT)	Rogers (1975)	Psychology	- Response-efficacy - Self-efficacy - Severity - Susceptibility	- Response-efficacy - Self-efficacy - Severity - Susceptibility	- Intention	How threats, with adequate amounts of efficacy, can motivate one toward protection from the threat (see Herath and Rao 2009)
Theory of interpersonal behavior (TIB)	Triandis (1977)	Psychology	- Affect - Attitude - Costs - Facilitating conditions - Habit - Rewards - Role - Self-concept - Social influence - Subjective norms	- Affect - Attitude - Social influence	- Facilitating conditions - Habit - Intention	How emotions and the role within the group impact security-related behaviors (Pee and Woon 2008)
Deterrence theory and rational choice (DT; RCT)	Gibbs (1975); Paternoster and Simpson (1996)	Criminology	- Formal control - Informal control	- Formal control - Informal control	- Intention	How punishments can be used to deter noncompliance (Bulgurcu et al. 2010)
An extended theory of protection motivation (PMT2)	Maddux and Rogers (1983)	Psychology	- Costs - Response-efficacy - Rewards - Self-efficacy - Severity - Susceptibility	- Costs - Response-efficacy - Rewards - Self-efficacy - Severity - Susceptibility	- Intention	Extends PMT: how costs also impact the interplay between threats and efficacy in protecting oneself from a threat (Boss et al. 2015)
Theory of planned behavior (TPB)	Ajzen (1985)	Psychology	- Attitude - Perceived behavioral control - Subjective norms	- Attitude - Perceived behavioral control - Subjective norms	- Intention - Perceived behavioral control	Augmented TRA, showing how perceptions of control further shape behavior (D'Arcy et al. 2009)
Theory of self-regulation (TSR)	Bagozzi (1992)	Psychology	- Attitude - Desire - Subjective norms	- Attitude - Desire - Subjective norms	- Intention	How one can self-manage security goals based on thoughts and emotions (not applied in ISS)
Extended parallel processing model (EPPM)	Witte (1992)	Public health	- Fear - Response-efficacy - Self-efficacy - Severity - Susceptibility - Emotional coping	N/A	- Fear - Response-efficacy - Self-efficacy - Severity - Susceptibility	How threats and efficacy can be used to predict both protective and reactive responses toward security (Johnston and Warkentin 2010)
Control balance theory (CBT)	Tittle (1995)	Criminology	- Constraints - Control balance - Situational provocation - Violation motivation	N/A	- Constraints - Control balance - Violation motivation	How the amount of control exerted on and by one can influence their motivation to engage in deviant behaviors (not applied in ISS)

Table 2. Summary of Relevant Constructs from Reviewed Theories

Construct	Definition	Source	Relevant Theories
Affect	The emotional response to a particular situation that is based on instinctive and unconscious processes in the mind	Triandis (1977)	CBT EPPM TIB
Attitude	The favorableness of engaging in a specific behavior	Fishbein and Ajzen (1975)	TIB TPB TRA
Avoidance	A maladaptive coping mechanism characterized by the effort to avoid dealing with a stressor	Witte et al. (1996)	EPPM TTAT
Control balance	The ratio of control that the individual exerts over others to the amount of control exerted by others on the individual	Tittle (1995)	CBT
Costs	The perceived personal efforts and/or intrinsic or extrinsic costs associated with engaging in the behavior	Janz and Becker (1984)	RCT/DT HBM PMT2 TIB
Desire	Cognitive or emotional inclinations that direct how one behaves	Bagozzi (1992)	TSR
Facilitating conditions	The ability of the individual to engage in the behavior as he or she intends to	Triandis (1977)	CBT DT TIB
Fear	A negatively valenced emotion that is elicited by a perceived threat, which is also perceived to be significant and relevant, and that results in a heightened sense of arousal	Witte (1992)	EPPM
Formal punishment	Established organizational “disincentives” or sanctions against committing a specific act	Siponen and Vance (2010)	RCT/DT
Habits	Behaviors that are or have become automatic insofar as they are performed without mindful instruction to do so	Bamberg and Schmidt (2003); Triandis (1977); Verplanken (2006)	TIB
Informal punishment	Socially based or unwritten policies used to disincentivize or sanction against committing specific acts	Siponen and Vance (2010)	DT/RCT
Intention	The inclination to engage in a specific behavior	Fishbein and Ajzen (1975)	All
Neutralization	Techniques that offer a way for persons to render existing norms inoperative by justifying behavior that violates those norms	Siponen and Vance (2010)	Neut.
Perceived behavioral control	The individual’s belief regarding their ability to enact the desired behavior	Ajzen (1985)	TPB
Reactance	The response of an individual who perceives that they are being externally controlled and who is likely to react to that perceived lack of self-determination by (re)asserting control	Lowry and Moody (2015)	EPPM
Response efficacy	The perceived effectiveness of the behavior in mitigating or avoiding the perceived threat	Rogers (1975)	EPPM PMT PMT2
Rewards	The perceived benefits of engaging in a specific behavior	Bandura (1977)	HBM PMT2 TIB
Roles	The social position that one holds within the relevant social groups of importance to the individual	Triandis (1977)	TIB
Self-concept	The individual’s perception regarding the appropriateness of a behavior in relation to adopted belief structures that help to define how the individual perceives him- or herself	Triandis (1977)	TIB
Self-control	Deliberative regulation of behavior	Curry (2005); Tittle (1995)	CBT
Self-efficacy	The ability of the individual to successfully complete the intended behavior	Rogers (1975)	EPPM PMT PMT2

Table 2. Summary of Relevant Constructs from Reviewed Theories (Continued)

Construct	Definition	Source	Relevant Theories
Severity	The perceived seriousness or magnitude of the risk associated with a given behavior	Witte (1992)	EPPM HBM PMT PMT2
Shame	A feeling of guilt or embarrassment induced if others know of the individual's socially undesirable actions	Siponen and Vance (2012)	Neut. DT/RCT
Social factors	The summative influence perceived by an individual due to social norms, roles within the group, and the individual's self-concept relevant to the group	Triandis (1977)	TIB
Subjective norms	The individual's perception of the favorableness of the behavior by significant others	Fishbein and Ajzen (1975)	TIB TPB TRA
Susceptibility/ Vulnerability	The perceived likelihood of experiencing the threat	Witte (1992)	EPPM HBM PMT PMT2
Violation motivation	The stimulus or force that drives the individual to engage in deviance	Tittle (1995)	CBT

have minimal costs. The basic idea is that desired behaviors will reward the individual by lowering risk, with minimal effort expended by the individual. *Rewards* refer to the perceived benefits of engaging in a specific behavior (Bandura 1977), whereas *costs* are defined as the personal efforts and/or intrinsic or extrinsic costs associated with engaging in a desired behavior (Janz and Becker 1984).

HBM has been applied to ISS to explain secure emailing behaviors within organizations. Ng et al. (2009) extended the health belief model to ISS by proposing that individuals have become aware of the threat posed by a given technology (i.e., malware). They suggested that individuals will thus engage in secure email behaviors when they perceive a threat and see that the recommended behaviors are helpful and not difficult to adhere to.

Theory of Reasoned Action

The basic tenet of the theory of reasoned action (TRA) is that behaviors are largely intentional (Fishbein and Ajzen 1975). These intentions are, in turn, predicted by the individual's attitudes toward the behavior and any relevant subjective norms that may influence the performance of the behavior (Fishbein and Ajzen 1975).

This theory has received wide empirical support (Floyd et al. 2000; Sheppard et al. 1988). *Attitude* is defined as the favorableness of engaging in a specific behavior (Fishbein and Ajzen 1975). *Subjective norms* are defined as the individual's perception of the favorableness of the behavior by significant others (Fishbein and Ajzen 1975). TRA applications in ISS include Bulgurcu et al. (2010) and Siponen et al. (2014).

Protection Motivation Theory

As the theory of reasoned action was proposed to explain an individual's rational response to the context of the behavior, it does not explain behavioral responses evoked by health threats (Rogers 1975). A health threat is likely to evoke fear, and thereby emotional—as opposed to rational—processing. Rogers (1975) proposed the protection motivation theor (PMT) to explain behaviors that are elicited as a response to a fear appeal. PMT differs from TRA in that it does not necessarily assume rational, nonemotional responses to messages. Further, PMT is based on the assumption that the individual is responding to a fear appeal, which is not found in TRA (Floyd et al. 2000). Like the health belief model, PMT proposes that individuals are able to perceive and respond to threats in their environment. Again, both the severity and susceptibility of the threat must be perceived to evoke a threat in the individual. However, PMT extends beyond HBM by explaining a secondary process enacted when threat is evoked: the appraisal and coping process.

The coping process is initiated once the individual appraises and determines that he or she is able to cope with the perceived threat. This process is built upon a dual-stage appraisal of (1) the efficacy of the communicated response and (2) the self-efficacy of the individual. *Response efficacy*

refers to the perceived effectiveness of the behavior in mitigating or avoiding the perceived threat (Rogers 1975). *Self-efficacy* refers to the ability of the individual to successfully complete the intended behavior (Rogers 1975). Thus, if an individual believes that the behavior can mitigate or avoid the threat and that he or she has the ability to do so, the individual will engage in a coping behavior that protects against the identified threat.

Several studies have applied PMT in ISS research (Herath and Rao 2009; Pahnila et al. 2007). Liang and Xue (2009) proposed the technology threat avoidance theory (TTAT), which applies PMT to technology-based threats that computer users may encounter. They also expanded PMT to include both protective behaviors that reduce the likelihood of experiencing the full threat and emotional coping behaviors that merely reduce the discomfort produced by the emotions evoked by the threat without affecting the outcomes.

Theory of Interpersonal Behavior

The theory of interpersonal behavior (TIB) was proposed due to the perceived restrictive nature of TRA (Triandis 1977). Triandis (1977) suggested that behaviors are more complicated and cannot be adequately estimated by norms, attitudes, and intentions alone. Thus, he proposed a model that includes affective components, additional social factors, predictors of attitudes, and conditions besides intentions that could further predict behaviors (e.g., facilitating conditions and habits).

TIB expands upon TRA by explicitly modeling antecedents to attitude. Triandis proposed that attitudes are shaped by the perceived rewards and costs of engaging in a behavior. A second extension of TRA by TIB is the inclusion of affect, or the emotional reasoning that may predict behaviors (Triandis 1977). Triandis argued that an individual's general feeling toward a behavior (affect) should also be considered, as behaviors do not always rely solely upon logical or rational factors. *Affect* is defined as the emotional response to a particular situation that is based on instinctive and unconscious processes in the mind (Triandis 1977).

A third extension of TRA by TIB includes a more extensive inclusion of social influences that may alter behavioral intentions. Beyond the subjective norm to engage in a behavior, Triandis also proposed that an individual's relevant role and self-concept also influence the intention to engage in a behavior. *Role* is defined as the social position that one holds within relevant social groups of importance to the individual (Ashforth and Mael 1989; Ashforth et al. 2011; Triandis 1977). An individual's role within a group will influence their intention, as additional pressures or norms are often applied within groups that provide additional normative influence on individuals to behave in manners consistent with their role.

Self-concept refers to the individual's perceptions regarding the appropriateness of a behavior given adopted belief structures that help to define how the individual perceives himself or herself (Triandis 1977). In an effort to avoid cognitive dissonance (Festinger 1957), individuals will experience increased normative pressure to engage in behaviors that others believe define who that individual is; for example, an ISS manager of a company who has publicly espoused the importance of locking computers subsequently begins several such initiatives within her company. The ISS manager could thus perceive pressure to adhere to such locking principles. However, such pressure may not exist if the manager does not believe that others have defined her by her belief in locking computers.

Finally, Triandis extended TRA by including both habits and facilitating conditions in TIB. *Habits* refer to behaviors that are or have become automatic insofar as they are performed without mindful instruction to do so (Bamberg and Schmidt 2003; Verplanken 2006). As habitual behaviors can be performed without conscious processing by the individual, they lie outside of the intentional process within TIB.

Facilitating conditions refer to the ability of an individual to engage in a behavior as he or she intends to (Triandis 1977). TIB recognizes that although individuals may have intentions to engage in a behavior, environmental conditions or the behaviors of others can often attenuate this relationship by making the behavior more costly to perform or making the performance of the behavior improbable or nearly impossible (Triandis 1977).

Only one ISS study to date has relied upon the TIB. Pee et al. (2008) reported a TIB-based model to predict nonwork-related computing in the workplace. In addition, the role of habits was explained in the context of ISS policy violations (Vance et al. 2012).

Deterrence Theory and Rational Choice Theory

Gibbs (1975) proposed the deterrence theory (DT) to explain criminal behavior. The main tenet of DT is that individuals engage in crimes when the benefits outweigh the potential costs. Similarly, rational choice theory (RCT) proposed by G. S. Becker (1974) and Paternoster and Simpson (1996), assumes that criminals are rational individuals who calculate the perceived benefits and costs of engaging in a crime and the potentiality of being detected (Paternoster 2010). Both

DT and RCT contain formal sanctions. Some authors later included informal sanctions in DT (Braithwaite 1989), which are also examined in ISS. For example, following the criminological literature, Siponen and Vance (2010) viewed shame as an informal deterrent mechanism. Rational choice models also contain benefits as rewards (Paternoster and Simpson 1996; Vance and Siponen 2012).

RCT regards sanctions, both formal and informal, as costs (Paternoster and Simpson 1996). More precisely, costs include the negative outcomes of engaging in a behavior. Consistent with DT and RCT, we assume that each of these costs has a severity and susceptibility component, which are both necessary for invoking a perceived threat for an individual in order to enable actual deterrence (Akers et al. 1979; Paternoster 2010).

We also included shame as a specific cost or informal control method per Siponen and Vance (2010). As shame can be an effective method for informally controlling employees when formal methods may be seen as too harsh, we likewise included this specific form of informal control in our review of the literature and test of the theory.

DT has been widely used in ISS research. The seminal ISS research article by Straub (1990) relied on this theory to explain computer abuse within organizations. DT has continued to be a popular theory in ISS research (D'Arcy et al. 2009; Lee et al. 2004; Theoharidou et al. 2005).

Extended Protection Motivation Theory

Shortly after PMT was proposed, the rewards and costs of an intended behavior were also included as extensions to the original theory (PMT2; Maddux and Rogers 1983). These extensions were built upon the PMT model and extant research on PMT, which has continually showed the importance of rewards as motivators to engage in a behavior, and the importance of costs as motivators to disengage from a behavior. Effectively, PMT synthesizes with HBM to explain why individuals protect themselves from perceived threats.

Theory of Planned Behavior

Similarly, TRA was later revised to include an additional construct (i.e., perceived behavioral control) that had been tested in the extant literature (Ajzen 1985). The theory of planned behavior (TPB) expanded TRA by positing that both intentions and behaviors are predicted by the perceived behavioral control of the individual. *Perceived behavioral control* refers to the perceived ease or difficulty of performing a behavior (Ajzen 1985). TPB thus proposes that if an individual believes he or she is able to perform a behavior, he or she will be more likely to intend to perform it, and will consequently do so. In the same manner, despite positive attitudes and norms toward a behavior, if an individual is unable to perform it, it is unlikely to occur. TPB has been widely used in ISS research (Bulgurcu et al. 2010; Galletta and Polak 2003; Mishra and Dhillon 2006).

Theory of Self-Regulation

The theory of self-regulation (TSR) is a complementary theory to TRA. Bagozzi (1992) expanded upon TRA by including desires. *Desires* are defined as cognitive or emotional inclinations that direct how one behaves (Bagozzi 1992). Bagozzi criticized TRA in that although one may have an attitude in favor of a behavior and have social normative pressures to perform it, conflicting desires may preclude such an action. Further, other needs or objectives may have a higher priority for the individual, cognitively and/or emotionally, which would indicate the importance of considering the desires of the individual when predicting behavior.

Despite the rich theoretical explanations proposed by Bagozzi, this theory has not been applied in ISS. However, it has continued to be used as a complementary model to both TRA and TPB in psychology research (Frattaroli 2006; Leone et al. 1999).

Extended Parallel Processing Model

The extended parallel processing model (EPPM) was proposed to explain why individuals either accept or reject public health campaigns (Witte 1992; Witte et al. 1996). Witte found that programs focused on abstinence, smoking cessation, and other actions resulted in two types of behaviors: Some individuals altered their behaviors and adopted the "healthy" behavioral practices, while others discounted such campaigns and continued in their unhealthy behaviors. Like PMT, EPPM contains the same dual-appraisal process of threat appraisal and coping, which is used to determine whether individuals will protect themselves from a threat, as explained by PMT, or emotionally cope with fear induced by the fear appeal. The other theories reviewed here do not include this emotional coping route of EPPM, and this must be explained.

EPPM posits that if a perceived threat is greater than the perceived efficacy of the recommended response to it, then the individual will feel the emotion of fear. *Fear* is defined as a negatively valenced emotion that is elicited by a perceived

threat believed to be significant and relevant, and which results in a heightened sense of arousal (Witte 1992; Witte et al. 1996). As fear is discomforting, the individual has a strong incentive to reduce the discomfort induced by this emotion and thus engages in emotional coping mechanisms. Thus, rather than engaging in a behavior that reduces the threat, the individual merely deals with the effects of the threat itself. These coping mechanisms are referred to as fear control responses within EPPM.

A variety of emotional coping mechanisms can be used depending on the context of the model and the desired behaviors. Witte (1992) posited avoidance and reactance as two common emotional coping mechanisms. We thus adopted these for the study as well. *Avoidance* refers to the fear control response whereby an individual ignores information or cues that would evoke fear and thereby fails to feel fear. *Reactance*, on the other hand, refers to the purposeful rejection of information and cues that would give rise to fear, thus causing the individual to actively disbelieve and challenge the cause(s) of fear.

Control Balance Theory

Control balance theory (CBT) was proposed by Tittle (1995) as a general theory of deviance. The basic tenet of this theory is that individuals engage in deviance or crime in order to return to a state of control balance or further extend their control over others. *Control balance* refers to the ratio of control that the individual exerts over others to the amount of control exerted by others on the individual (Tittle 1995). Thus, two types of imbalances exist: control surplus and control deficit (Tittle 1995). If an individual has a control surplus, he or she will have an increased incentive to further control others and thus increase his or her control surplus (Tittle 1995).

However, if an individual perceives that he or she is being controlled more than he or she is able to control his or her own life, the resulting control deficit will lead the individual to engage in submissive deviance (Tittle 1995). Individuals under a control deficit attempt to increase the control they feel in order to achieve a control balance. Deviant behavior enables the individual to exert more control and thereby shift his or her control imbalance toward increased balance (Tittle 1995).

CBT proposes three other constructs. First, CBT proposes that *violation motivation* will increase the intention to violate a policy, rule, or law. As previously mentioned, a control imbalance serves as a motivator for deviance, which is likely to increase an individual's motivation to engage in deviance. This motivation is further increased when the individual is made aware of his or her control imbalance. This can be accomplished through situational cues that raise the saliency of the control exerted over the individual or the control that he or she is able to exert over others (Tittle 1995).

Finally, like DT, CBT posits that deviance will only be enacted as long as there are no perceivable constraints that would deter the individual from engaging in deviance, similar to the reasoning provided by DT. CBT has never been used in any ISS research.

Methodology

Pilot Test and Measures

Our two studies used a paper-based survey to collect data. We used previously validated and reported instruments (Appendix A), with some minor adjustments to fit the context of this study. A common way to measure ISS policy violations (or insecure acts) in previous research has been the use of generic measures (Siponen and Vance 2014) such as "I comply with the information security policies of my organizations" (Pahnila et al. 2007). These are generic because they do not refer to (and hence do not measure) a specific type of IS policy violation (or insecure act). The downside of generic measures is that scholars cannot know about which insecure acts the respondents are thinking. By responding to the question "I comply with the information security policies of my organizations," are the respondents thinking, for example, about not locking a computer, picking a password that is easy to break, or something else? Siponen and Vance (2014) raised another concern in the use of generic measures. Let us presume that there is the question, "Do you break the law?," which is a generic question because it does not refer to any specific law. Most of us might tend to reply "No" to this question, but the reply could be different if the question were, "Do you ever drive over the speed limit?" (Siponen and Vance 2014). Similarly, there is a possibility that the responses will be different depending on which ISS acts are being referred to, which the generic measures cannot capture. To overcome this potential concern, scholars have two options for self-reports. ISS scholars can use (1) scenario-based techniques to measure prospective behavior (Pogarsky 2004) or (2) traditional one-line survey statements (e.g., adapted from IT use literature) to measure current or retrospective behavior (Siponen and Vance 2014), as shown in Table 3. The strengths and weaknesses of these approaches are discussed in Appendix F and summarized in Table 3.

Table 3. Two Alternatives to Capture the Type of Secure or Insecure Act

Approach	Illustrative Example	What it Measures	Strengths and Weaknesses
Behavior statement	"I comply with the password policy of my company."	Current behavior	+ Can specify the type of violation (insecure act) + Measures current self-reported behavior - Lacks contexts - Cannot capture prospective behavior - Intimidating concern
Scenario	"Jim is an employee in your organization. One day, while Jim is out of the office on a sick day, one of his coworkers needs a file on Jim's computer. The co-worker is of equal rank and performs job functions similar to Jim's. The coworker calls Jim and asks for the password. Although Jim knows that your organization has a policy that passwords must not be shared, he shares his password with the coworker." (D'Arcy et al. 2014, p. 313).	Prospective behavior (intention)	+ Can specify the type of violation (insecure act) + Has contexts + Can capture prospective behavior (intention) + Less intimidating, admitting concern - Does not measure current self-reported behavior

Of these self-report approaches specifying the type of violation (Table 3), the scenario approach is more widely used in ISS (Siponen and Vance 2014). The realism of the scenarios is important for practical applicability (Siponen and Vance 2014). To assure this, three scenarios were obtained from Siponen and Vance (2010), who developed their scenarios based on interviews with 54 information security managers. These managers identified these three behaviors as the most likely and relevant ISS policies for their organizations.

First, our study was pretested by 10 faculty members and graduate students to ensure that the questions matched the selected theories and that the questions were readable. After this process, the survey instrument was pilot tested by master's students enrolled in a business school course at a Finnish university. We obtained 49 usable responses. We revised several questions based on the feedback received from these two initial pilot studies.

Second, participants were asked to first read one of three security-related scenarios. After reading the scenario, participants were then asked to provide answers for the constructs used in the various theories.

Our pilot study used a paper-based questionnaire that consisted of questions and an area in which respondents could leave remarks and feedback about the questions asked. We used these responses to ascertain the validity of the questions and to identify any points of confusion within the survey. Based on feedback and initial statistical analysis, several questions were removed from our instrument prior to the final data collection.

Study 1: Data Collection

The final data were collected from working professionals in Finland through a paper-based questionnaire. The survey was administered in Finnish, as it was the primary language of all the respondents in our study.

A university in Finland maintains a list of all its graduates who had previously given permission to be contacted by the university in the future. The list is maintained and updated periodically. We used this pool of people as our sample. From this list, we selected people who had work experience and had obtained a master's degree from a university where one of the authors is positioned, which granted us access to this sample. We selected all educational backgrounds, representing all scientific disciplines (medicine, natural science, engineering, business, social science, and educational sciences) except theology, sports science, and law. This resulted in a sample population of nearly 50,000 working graduates. From a population of about 50,000 people, we invited every fiftieth person to take the survey in order to ensure a random selection of respondents. As a result, 898 people were invited to complete the survey. Of these 898 people, 178 took the survey, resulting in a response rate of 19.821%. A reminder was sent by mail, which increased the response rate to 30.512%, $n = 274$ (out of 898) in total. We deem this as a good response rate (keeping in mind that we could not ascertain how many actually received the survey); moreover, the respondents did not receive any financial compensation for taking the survey. Analysis of these two groups, in terms of demographic and descriptive statistics of the constructs, revealed no systematic difference between the early and late

Table 4. Model Fit Statistics

Theory	RMSEA	CFI	TLI	CD
Techniques of neutralization	0.103	0.726	0.687	1.000
Health belief model	0.087	0.864	0.837	1.000
Theory of reasoned action	0.053	0.944	0.956	1.000
Protection motivation theory	0.080	0.875	0.844	1.000
Theory of interpersonal behavior	0.077	0.724	0.798	1.000
Deterrence theory	0.115	0.655	0.607	1.000
Extended protection motivation theory (PMT2)	0.070	0.811	0.789	1.000
Theory of planned behavior	0.097	0.807	0.927	1.000
Theory of self-regulation	0.123	0.805	0.866	0.965
Extended parallel processing model	0.047	0.880	0.868	1.000
Control balance theory (modified)	0.118	0.802	0.849	1.000

RMSEA: Root mean squared error of approximation (should be below .10)
CFI: Comparative fit index (should be above .90)
TLI: Tucker-Lewis index (should be above .90)
CD: Coefficient of determination (should be above .90)

responders. We used this final dataset of 274 respondents for our analysis.

The survey was anonymous: No identifying information of any kind was gathered from the participants in order to ensure that they could not be identified. It was also clearly communicated to the respondents that independent university researchers from a different university would analyze the results of their surveys.

Data Analysis and Results

Convergent and discriminant validities were assessed with STATA's (version STATA/SE 14.1) confirmatory factor analysis (CFA) for each model. Model fit indices for the fully fitted model are reported with each model in Table 4. Convergent validity was supported by large and standardized loadings for all constructs ($p < .001$) and *t*-values that exceeded statistical significance for all models (Gefen et al. 2011). Convergent validity was also supported by calculating the ratio of factor loadings to their respective standard errors, which exceeded |10.0| ($p < .001$) (Marsh and Hocevar 1985). Summary statistics of the constructs are presented in Table 5. We noted that only one correlation was problematically high (Shame and Severity: 0.758). However, this was below the generally accepted high level for correlation, and the variance inflation scores for these constructs were both below the accepted 3.3 level (Kock and Lynn 2012).

Discriminant validity was tested by showing that the measurement model had a significantly better model fit than a competing model with a single latent construct, and that the model fit was better than all other competing models in which pairs of latent constructs were joined. The χ^2 differences between the competing models (see Appendix B for these details) were significantly larger than those of the original model, as also suggested by factor loadings, modification indices, and residuals (Marsh and Hocevar 1985). This process was repeated for each model tested. In summary, these tests confirm the convergent and discriminant validities of the tested theoretical models.

Reliability was assessed by using construct reliability as assessed through Cronbach's α. The majority of measures exceeded 0.70 (see Table 6), suggesting reasonable reliability. Constructs with lower reliability were still maintained in order to assess the various theories. Reliability was also supported because the average variance extracted (Hair et al. 2006) exceeded 0.70 for all factors.

Our test for common method bias showed that it was not a large concern for this sample, as our theoretical models were better fitted to the data than models with a single latent factor, which served as a proxy for common method variance present in the dataset (Gefen et al. 2011). As this single factor did not provide a better fit for the data in comparison to any of the theories, the theoretical model or the saturated model, we posit that common method variance bias was not likely for this sample (see Appendix B for more detail).

We report the following observations regarding the fit of the data from the measurement models, theoretical model, and

Table 5. Descriptive Statistics

Variable	Mean	Std. Dev.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
(1) Intention	3.518	3.145	1.000														
(2) Response efficacy	4.153	0.839	-0.042	1.000													
(3) Habit	3.941	0.729	-0.083	0.146	1.000												
(4) Attitude	1.749	0.890	0.164	-0.195	-0.492	1.000											
(5) Rewards/costs	2.353	1.354	0.064	-0.105	-0.277	0.568	1.000										
(6) Self-efficacy	3.379	0.416	0.055	0.146	-0.013	0.159	0.085	1.000									
(7) Subjective norms	3.726	1.012	-0.175	0.023	0.059	-0.062	-0.058	0.003	1.000								
(8) Perceived behavior control	2.762	0.702	-0.160	0.050	0.088	-0.062	-0.024	0.014	0.556	1.000							
(9) Desire	5.813	0.854	-0.099	-0.009	0.034	-0.008	-0.055	0.012	0.304	0.221	1.000						
(10) Control balance	4.308	0.904	-0.108	0.065	0.048	-0.028	-0.040	0.030	0.527	0.420	0.345	1.000					
(11) Affect	2.410	0.657	0.144	-0.078	-0.066	0.043	0.022	0.011	-0.389	-0.634	-0.285	-0.509	1.000				
(12) Facilitating conditions	3.081	0.770	0.023	-0.049	-0.051	0.000	-0.006	-0.010	-0.283	-0.217	0.084	-0.195	0.165	1.000			
(13) Roles	2.462	1.312	0.142	-0.024	-0.051	0.094	0.050	-0.002	-0.578	-0.586	-0.349	-0.600	0.646	0.173	1.000		
(14) Self-control	2.685	0.666	0.095	-0.060	-0.057	-0.003	-0.060	0.002	-0.355	-0.401	-0.317	-0.566	0.529	0.128	0.625	1.000	
(15) Social factors	2.033	0.589	0.039	-0.046	0.010	-0.007	-0.024	-0.035	-0.091	-0.257	0.037	-0.175	0.389	0.054	0.307	0.246	1.000
(16) Fear	2.533	0.686	-0.074	-0.026	-0.007	0.021	0.023	-0.020	0.065	0.091	-0.020	-0.003	-0.050	-0.014	-0.063	-0.022	-0.043
(17) Defensive avoidance	1.165	0.267	-0.034	0.037	0.045	-0.014	0.021	0.033	-0.016	0.066	-0.010	-0.001	0.007	-0.034	0.005	0.049	0.005
(18) Reactance	3.122	1.438	0.088	0.102	0.043	-0.041	-0.046	-0.042	0.012	-0.049	0.006	-0.006	-0.041	0.043	-0.004	-0.027	-0.032
(19) Severity	4.313	1.045	-0.059	0.300	0.436	-0.587	-0.324	0.087	0.064	0.096	0.015	0.047	-0.053	0.008	-0.069	-0.031	0.001
(20) Vulnerability	4.929	1.280	-0.113	0.282	0.162	-0.460	-0.270	0.018	0.001	0.062	-0.017	0.009	-0.081	-0.013	-0.083	-0.038	-0.006
(21) Shame—certainty	4.882	1.902	-0.030	0.030	0.050	-0.025	0.004	0.073	-0.035	0.004	-0.027	-0.053	0.016	0.044	0.004	0.005	-0.079
(22) Shame—severity	4.881	2.096	0.008	0.055	0.017	0.031	0.011	0.055	-0.071	-0.023	-0.013	-0.061	-0.001	0.052	0.045	0.045	-0.063
(23) Formal—certainty	3.871	2.030	-0.054	-0.026	0.044	0.003	-0.004	0.049	0.009	0.048	0.002	-0.020	0.015	-0.010	-0.012	0.065	-0.005
(24) Formal—severity	1.644	0.565	0.000	-0.001	0.003	0.049	0.035	0.020	-0.063	-0.012	-0.046	-0.067	0.042	0.031	0.038	0.071	-0.032
(25) Informal—certainty	3.704	1.863	-0.054	0.010	0.048	-0.010	0.014	0.037	0.004	0.015	-0.005	-0.032	0.011	0.007	-0.011	0.027	-0.020
(26) Informal—severity	5.346	1.483	-0.007	0.056	0.043	-0.019	0.001	0.068	-0.083	-0.059	-0.017	-0.064	0.031	0.064	0.061	0.052	-0.045
(27) Neutralization condemnation	2.160	1.668	0.083	-0.056	-0.065	0.033	0.018	-0.017	0.036	-0.015	0.007	0.017	-0.024	-0.015	-0.013	-0.035	0.021
(28) Neutralization denial of injury	2.409	1.564	0.114	0.023	-0.005	0.021	0.085	0.043	-0.280	-0.316	-0.519	-0.362	0.459	-0.031	0.425	0.386	0.101
(29) Neutralization higher loyalties	2.589	1.965	0.100	0.021	-0.066	0.035	0.010	-0.023	-0.008	-0.056	0.028	0.013	-0.026	0.001	0.014	0.003	0.011
(30) Neutralization ledger	2.228	1.530	0.112	-0.053	0.001	0.059	0.045	0.005	-0.001	-0.036	0.012	0.022	-0.007	-0.040	0.006	-0.005	0.028
(31) Neutralization necessity	1.882	1.220	0.085	0.019	-0.017	-0.002	-0.021	0.004	-0.003	-0.039	-0.007	0.016	-0.040	0.008	0.011	-0.013	-0.035
(32) Neutralization denial of responsibility	1.748	0.973	0.092	0.015	-0.028	0.010	0.006	0.000	0.009	-0.001	-0.011	0.037	0.003	-0.008	0.023	0.024	-0.052

Table 5. Descriptive Statistics (Continued)

Construct	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
(16) Fear	1.000																
(17) Defensive avoidance	0.214	1.000															
(18) Reactance	-0.230	-0.313	1.000														
(19) Severity	-0.016	0.018	-0.020	1.000													
(20) Vulnerability	-0.017	-0.040	0.020	0.620	1.000												
(21) Shame—certainty	0.335	0.214	-0.245	0.016	0.008	1.000											
(22) Shame— severity	0.339	0.113	-0.152	-0.031	-0.004	0.758	1.000										
(23) Formal punishment certainty	0.440	0.223	-0.212	-0.014	-0.038	0.582	0.577	1.000									
(24) Formal punishment severity	0.406	0.184	-0.213	-0.062	-0.017	0.598	0.684	0.690	1.000								
(25) Informal punishment certainty	0.482	0.252	-0.217	0.009	-0.021	0.665	0.671	0.812	0.670	1.000							
(26) Informal punishment severity	0.241	0.008	-0.052	0.020	0.076	0.630	0.642	0.419	0.556	0.413	1.000						
(27) Neutralization condemnation	-0.190	-0.213	0.319	-0.019	0.028	-0.352	-0.339	-0.286	-0.340	-0.380	-0.155	1.000					
(28) Neutralization denial of injury	-0.009	0.008	0.003	0.027	-0.065	-0.003	-0.009	-0.020	0.035	-0.008	-0.016	-0.008	1.000				
(29) Neutralization higher loyalties	-0.202	-0.378	0.451	-0.059	0.034	-0.368	-0.254	-0.353	-0.329	-0.349	-0.073	0.529	0.012	1.000			
(30) Neutralization ledger	-0.181	-0.237	0.364	-0.057	0.003	-0.318	-0.282	-0.273	-0.266	-0.308	-0.085	0.528	-0.018	0.547	1.000		
(31) Neutralization necessity	-0.302	-0.340	0.453	-0.024	0.047	-0.323	-0.265	-0.380	-0.386	-0.424	-0.072	0.609	-0.002	0.769	0.560	1.000	
(32) Neutralization denial of responsibility	-0.057	-0.223	0.317	-0.012	-0.024	-0.208	-0.224	-0.154	-0.218	-0.135	-0.078	0.354	0.011	0.394	0.417	0.388	1.000

saturated model (see Appendix B) and the model fit statistics for the fully fitted theoretical model (see Table 4). First, only the theory of reasoned action, when fully fitted, seemed to display optimal fit statistics; the rest of the theories indicated that they did not properly fit the data as desired. When comparing these results with the more fully explored results in Appendix B (see Table B1), we can see that, for most of the theories, the fully saturated models had a better fit than the theoretical models, implying that omitted relationships between the theoretical constructs were reducing the fit of the data to the model. We further explored this and performed specification tests[3] for each of the models, using regression analysis, and discovered that each theoretical model, with the exception of TRA, had omitted variables or relationships from the theory.

The majority of all the proposed relationships of the theories received empirical support by our data and models (see Appendix C for a summary of each theoretical model test for the 11 theories). This also provides empirical support that each of the theories is relevant in explaining IS policy violations (at least by our data/models), which is important for the theories that have not yet been used in IS, such as control balance theory, and for those that have only a few empirical studies (e.g., HBM). However, these results should be taken with caution, as our data fit procedures showed that the theories did not fit the data as well as they could have and that missing constructs and relationships were evident in every theory, with the exception of TRA.

Having determined that the majority of the theories are supported by our data, we now turn to the ability of these theories' constructs to explain variance in their dependent variables (summarized in Table 7). We found that the different theories vary in their ability to explain an individual's intention to violate organizational security policies. Namely, we found that the theory of neutralization, health belief model, and rational choice theory/general deterrence theory

[3]Specifically, we used ovtest and linktest, which are specification tests using a Ramsey RESET procedure. See http://www.ats.ucla.edu/stat/stata/webbooks/reg/chapter2/statareg2.htm for more details about these procedures.

Table 6. Construct Reliabilities

Construct	Cronbach's Alpha
Intention	0.976
Response efficacy	0.802
Habit	0.903
Self-efficacy	0.896
Attitude	0.898
Rewards/costs	0.931
Severity	0.826
Vulnerability	0.933
Subjective norms	0.778
Perceived behavioral control	0.618
Desires	0.915
Control (im)balance	0.835
Affect	0.838
Facilitating conditions	0.791
Roles	0.865
Self-control	0.862
Social factors	0.754
Fear	0.871
Defensive avoidance	0.784
Reactance	0.931
Shame—Certainty	0.807
Shame—Severity	0.843
Formal punishment—Certainty	0.832
Formal punishment—Severity	0.939
Informal punishment—Certainty	0.823
Informal punishment—Severity	0.747
Neutralization—Condemnation of the condemners	0.700
Neutralization—Denial of injury	0.983
Neutralization—Appeal to higher loyalties	0.736
Neutralization—Metaphor of the ledger	0.702
Neutralization—Defense of necessity	0.662
Neutralization—Denial of responsibility	0.732

Table 7. Summary of the Explanatory Power of the Tested Theories

Theory	Intention R^2
Theory of neutralization	0.35
Theory of self-regulation	0.48
Health belief model	0.35
Theory of reasoned action	0.47
Protection motivation theory	0.53
Theory of interpersonal behavior	0.59
Deterrence theory	0.38
Extended protection motivation theory (PMT2)	0.60
Theory of planned behavior	0.55
Extended parallel processing model	0.47
Control balance theory	0.52

provide the weakest explanatory power of the theory set. The extended protection motivation theory (PMT2) and the theory of interpersonal behavior are the best explanatory theories within the set.

Unifying the Theories

IS scholars have explained information security behavior by borrowing theories from other disciplines such as criminology and subfields of psychology. Many of these theories and models have concepts that resemble each other. This raises the question of how these theories and models are theoretically and empirically similar or different. The second question is to what extent these rival theories and models can be synthesized into a single model that addresses the limitations of the component models. Attempts to unify theories are called unified models (Venkatesh et al. 2003) or theory integration (Liska et al. 1989). The underlying motives for theory integration are typically concept driven (Liska et al. 1989). Concept-driven investigation examines to what extent the concepts of the underlying theories or models are the same (Liska et al. 1989). Two approaches to carry out the integration exists, namely theory-driven and the empirical-data-driven. The theory-driven approach views theoretical differences as more important than empirical results in determining the unified model. Conversely, the empirical-data-driven approach relies on empirical results to determine the unified model. Both approaches have their strengths and weaknesses. The key strength of the empirical approach is empirical support, which is a potential weakness of the theory-driven approach. In turn, the theory-driven approach has better potential to highlight theoretical differences, which could be important in certain settings but which are not visible in the empirical results in other settings. To summarize, the theory-driven approach is good at highlighting theoretical differences and nuances, while the empirical approach sees empirical similarities as an important qualifier.

Of these approaches, we selected the empirical-data-driven approach for two reasons. First, given that all 11 theories have been developed in totally different contexts than ISS, it is unclear to what extent their different theoretical assumptions are relevant in IS. Given this, second, we prefer empirical rather than theoretical comparisons to test the similarities and differences between the theories. Next, we discuss our approach to theory unification, which is similar to that of Venkatesh et al. (2003).

Combining the Theories: An Empirically Driven Approach

First we performed a factor analysis on all of the previously used items to discover whether several constructs from various theories may be more strongly related, thus enabling us to simplify our model. We deem this an important first step, as several constructs across the various theories have marked similarities. This allowed us to statistically test these similarities, thus also allowing us to reduce the overall complexity of the UMISPC by combining several constructs into a more general construct.

We performed a principal factor analysis of all our measured items, using STATA/SE 14.1. These results were then rotated with a typical orthogonal varimax rotation. The results indicated that the dataset could be better represented with 22 factors (We used the typical cutoff point of retaining all factors with an eigenvector value over 1.00). These 22 factors accounted for 84.45% of all variance in our dataset.

As expected, similar items tended to converge upon factors. Items were mapped on to the factor on which they had the highest loading, assuming at least a loading of .70 was achieved. This resulted in 11 of the 22 factors being removed from further consideration, as no items loaded onto these factors were higher than .70. Our new mapping of items to the retained factors is shown in Table 8. A detailed factor analysis loading is provided in Appendix D. Loadings below the absolute value of .40 were removed in order to clarify the reading of the chart and identify the higher value loadings for the reader.

Proposing the Unified Model of Security Policy Compliance (UMISPC)

Having examined the comparative advantages provided by the various theories, we now turn to the development of a unified theoretical model that is based on the 11 identified and retained factors that emerged from these theories through our data-driven reduction. We employed a hybrid approach in advancing our UMISPC, as we believe that theory should guide how the constructs relate to each other, rather than solely relying on statistical analysis to show us the relationships that exist in the data. We chose this option as it allowed us to preserve the theoretical networks that have been proposed across the theories in the extant literature. Further, theory provides explanations as to why one construct should predict another within our UMISPC

Given the 11 identified factors, our first step was to identify which theory included the majority of these factors in order to identify the relationships with which we should begin in our model. Given that habit, facilitating conditions, and role values were all identified constructs from our data reduction analysis, we built upon the theory of interpersonal behavior (TIB). We thus used TIB as the underlying framework for the

Table 8. Mapping of Items to Identified Factors for UMISPC Validation

Identified Factor	Description in the Study Context	Item	Loading
Factor 1 Role Values	The required ISS policy compliance act is appropriate, justified, and acceptable, keeping in mind the nature of the work and the task the person is performing	percbehcont2	-.7829
		selfcon1	-.7629
		moral1	-.7514
		affect4	.7241
		roles3	.7862
		selfcon2	.8005
		affect1	.8150
		roles2	.8170
		selfcon3	.8751
Factor 2 Punishment	Negative reinforcement that is perceived to be imposed if found to be noncompliant with the ISS policy	formalcert2	.8132
		informalcert1	.7998
		formalcert1	.7966
		formalsev2	.7865
		informalcert3	.7801
		formalcert3	.7268
		informalcert2	.7121
Factor 3 Rewards/Costs	Positive reinforcement that is perceived when in compliance with the ISS policy	respcost5	.7023
		reward3	.7112
		respcost4	.7520
		reward4	.7597
		reward1	.7995
		respcost1	.8287
		respcost2	.8384
Factor 4 Habit	A regular tendency that does not require conscious thought to be compliant with the ISS policy	habit3	.8173
		habit1	.8026
		habit2	.7951
		habit12	.7808
		habit7	.7642
		habit11	.7493
		habit8	.7423
		habit5	.7130
Factor 5 Neutralization	Rationalized thinking that allows one to justify departure from compliance intentions	neutcond3	.7190
		neutloyal1	.7312
		neutinjury3	.7980
Factor 6 Threat	Perceived severity and susceptibility to a perceived potential harm	vulner2	.8555
		vulner3	.8537
		vulner1	.8434
		sever3	.7922
Factor 7 Fear	Negative emotional response to stimuli	fear10	.8625
		fear11	.8462
		fear7	.7598
Factor 8 Response efficacy	The perceived effectiveness of the behavior in mitigating or avoiding the perceived threat	respeff2	.8368
		respeff3	.7230
		respeff4	.7157
Factor 9 Facilitating conditions	The potential of the individual to comply without help from other people	facicond3	.7203
		facicond4	.7735
Factor 10 Reactance	Denying that there is an ISS problem	react4	.7869
		react3	.7808
Factor 11 Intention	The inclination to engage in a specific behavior	intent1	.8728
		intent2	.8809

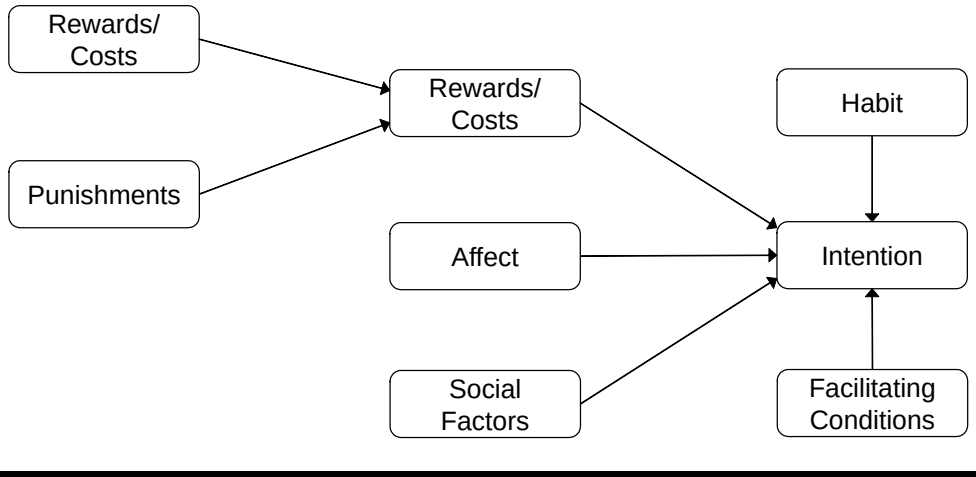


Figure 1. Step 1 of the Unified Model

UMISPC. We present a modified version of TIB as the first step in the formulation of the UMISPC (Figure 1), as it directly includes 5 of the 11 retained factors, as explained below. The relationships between the constructs are based upon those explicated in TIB.

We noted that the majority of the TIB model was included within the 11 retained factors, and we now describe the first exceptions. First, attitude was not a retained factor, and was thus removed from our framework. Instead we directly related the rewards/costs and punishments to intentions. Second, TIB posits that general affect is used in forming intentions; however, within the context of this study, we were concerned with the affective component that would pertain to the intention to engage in security behaviors. Previous research in ISS has highlighted that individuals choose to engage in protective information security behaviors due to a perceived fear felt because of a perceived threat (Boss et al. 2015; Johnston et al. 2015). We thus removed affect and replaced it with the prediction of intention by fear, as proposed in EPPM, PMT, and PMT2, which also posit that fear is produced as an outcome of threat (Rogers 1983). Finally, the original TIB suggests that subjective norms, roles, and self-concept lead to social factors. Instead of social factors, we propose *role values* based on our results, which comprise Factor 1 (Table 8). Our Factor 1 is not a social factor, because the factor does not retain social elements after the results of the factor analysis.[4] We named this new construct "role values," and it is defined in Table 8. A role value refers to the required ISS policy compliance act which is appropriate, justified, and acceptable (cf. moral definitions and self-concept), given the nature of the work and the task the person is performing (cf. roles). We show these adaptations to Step 1 in the next step of our theorizing (Figure 2), where we included two more of the retained factors and removed constructs from TIB that were not retained in our analysis.

The next step included the addition of a route for denying the possible ISS problem (reactance). With the exception of work by Liang and Xue (2009, 2010), ISS research has focused on a single dependent variable within its models; that is, either compliance or noncompliance with ISS policies. As in EPPM and TTAT (Liang and Xue 2009), we proposed that in addition to compliance with ISS policies, reactance should be considered within the same model. It is possible that each of these routes will have different antecedents, and thus it makes sense to consider both routes in the model. Based on EPPM, fear can also be coped with by denying the existence of the possible problem. This extension of the unified information security model (UMISPC), which juxtaposes the dual routes from EPPM with the UMISPC, is shown in Figure 3.

[4]That is to say, social factors (Bergeron et al. 1995) consisted of these items ("With respect to complying with information security procedures, I have to do as the top management of my organization/my colleague/my supervisors thinks"). These were not retained in the factor analysis. Rather, factor analysis suggested a new construct that could be relevant. The construct consists of questions from moral definition (e.g. "How morally wrong would it be to do what the person did in the scenario?") (Siponen et al. 2012), self-concept (e.g., "What Mattila did is consistent with my principles" and "It is acceptable to do what Mattila did") (Gagnon et al. 2003), roles ("What Mattila did fits with his/her work style" and "What Mattila did can be justified due to the nature of Mattila's work") (Bamberg and Schmidt 2003), and affect ("What Mattila did is smart") (Limayem and Hirt 2003).

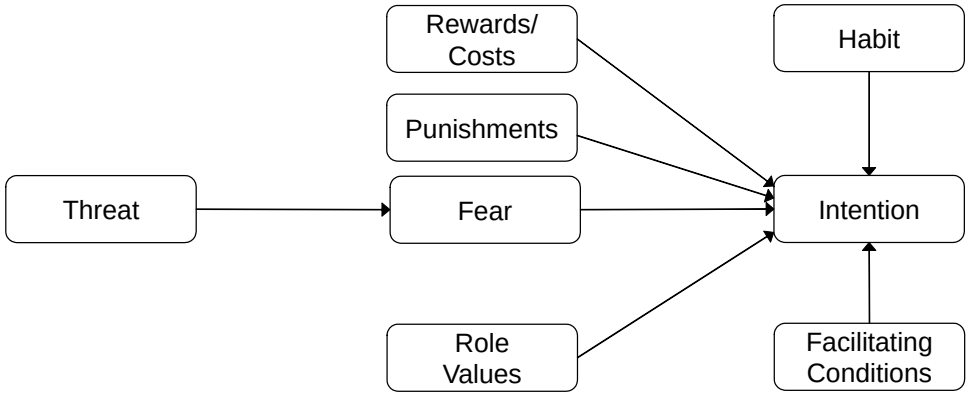


Figure 2. Step 2 of the Unified Model of Information Security Policy Compliance

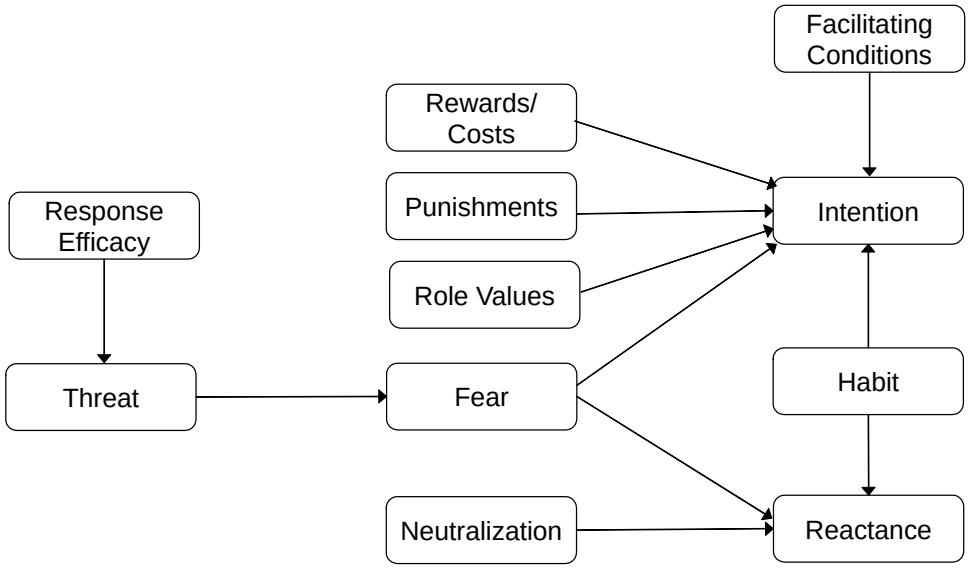


Figure 3. Step 3 of the Unified Model of Information Security Policy Compliance

PMT is based on the notion of fear appeals (Rogers 1975). A fear appeal is a persuasive attempt by a third party to induce the target to engage in a desired behavior that would protect it from some threat (Maloney et al. 2011). According to PMT, the messages used to produce a fear appeal can alter the target's perceptions of their self-efficacy, the efficacy of the desired behavior, and the severity or susceptibility of the threat (Rogers 1975). As the perceived efficacy and threat levels are altered, the individual's attitude toward the intended behavior is also modified through reductions in perceived threat or perceived fear. As our data-driven method did not identify self-efficacy, and severity and susceptibility are subsumed under threat, we included response efficacy as a predictor of threat.

Finally, we proposed neutralization as an antecedent for denying the possible ISS problem (reactance) using neutralization techniques (Maruna and Copes 2005). The final extensions to our UMISPC, including response efficacy and reactance (from PMT) as well as the inclusion of neutralization, are depicted in Figure 3.

To test the final model (Figure 3), we performed another data collection, drawing from the same sample population but

randomly selecting different respondents than in the first study where we compared the theories.

Study 2: New Data Collection to Test the UMISPC

For Study 2, we used the same pool of 50,000 people as in Study 1, which contained university graduates with graduate degrees from all scientific disciplines (medicine, natural science, engineering, business, social science, and educational sciences), except theology, sports science, and law. However, from the pool of 50,000, we removed those 898 people to whom we had sent Study 1. From this population (49,102), we randomly selected 1,581 working professionals and sent the survey to them. So, although Study 1 and 2 were derived from the same population (50,000), the respondents (sample) in each study were different.

We used three scenarios for data collection. This allowed us to examine whether the unified model held across more than one particular security-related behavior. The three scenarios included the positional role of the main person in the scenario, the security-related policy, and the extent to which the policy was violated. The scenarios were taken from Siponen and Vance (2010). Siponen and Vance (2010, Appendix B) asked ISS managers to report the "most common and significant information security policy violations." The most frequent ISS policy violations reported by 54 ISS managers were insecure USB practices, password issues, and not locking computers (Siponen and Vance 2010, Appendix B). They then developed scenarios based on the most frequent ISS policy violations, which we used. While information security concerns may not be universal across all organizations, Siponen and Vance provided some evidence that their scenarios presented relevant ISS concerns. The scenarios and instrument used for this data collection are described in Appendix A.

We obtained 393 usable responses, resulting in an overall response rate of 24.857% (393 responses out of 1,581). For Scenario 1, the response rate was 25.806% (n = 136/527); for Scenario 2, 25.237% (n = 133/527); and for Scenario 3, 23.529% (n = 124/527). As can be seen, the responses were rather equally distributed per scenario. The survey was anonymous, as no identifying information of any kind was gathered from the participants. It was also clearly communicated to the respondents that university researchers from their alma mater would analyze the results of the surveys. We analyzed the differences between the samples using their demographic information and summarized item scores. No systematic difference was found between the samples.

Data Analysis

Establishing Factorial Validity

Convergent and discriminant validities were assessed with STATA's (version STATA/SE 14.1) confirmatory factor analysis (CFA) for this model. Model fit indices were acceptable (χ^2_{796} = 1665.91; CFI = 0.980; TLI = 0.964; RMSEA = 0.058; SRMR = 0.086; CD = 1.000). Convergent validity was supported by large and standardized loadings for all constructs ($p < .001$) and t-values that exceeded statistical significance for all models. Convergent validity was also supported by calculating the ratio of factor loadings to their respective standard errors, which exceeded |10.0| ($p < .001$) (Gefen et al. 2011; Marsh and Hovecar 1985). Summary statistics of the constructs are presented in Table 9. We noted another large correlation within this dataset (role values and intention: 0.883). This may represent lateral collinearity (Kock and Lynn 2012), demonstrating that the relationship is more a result of shared collinearity between a proposed relationship, inflating the predicted pathway. Following the steps outlined in Kock and Lynn (2012), we created a new model where these constructs were both regressed onto an unrelated construct, which allowed us to classically test their collinearity through the use of variance inflation factors. We found that the VIF score was 1.01, indicating that we could reject the potential for lateral collinearity between role values and intention.

Discriminant validity was tested by showing that the measurement model had a significantly better model fit than a competing model with a single latent construct as well as all other competing models in which pairs of latent constructs were joined. The χ^2 differences between the competing models (omitted for the sake of brevity) were significantly larger than those of the original model, as also suggested by factor loadings, modification indices, and residuals (Marsh and Hocevar 1985). In summary, these tests provided support for convergent and discriminant validities of the tested model. For detailed reports of these validity tests and an analysis for common variance analysis, please see Appendix E.

Reliability was assessed by using the construct reliability as assessed through Cronbach's α. All constructs exceeded the recommended level of 0.70 (see Table 10), suggesting strong reliability. Reliability was also supported because the average variance extracted (Hair et al. 2006) exceeded 0.70 for all factors.

Summary of the Key Results from Study 2

As seen in Figure 4, the majority of the UMISPC is supported, based on the context of our scenarios and our data.

Table 9. Descriptive Statistics

Variable	Mean	Std Dev	1	2	3	4	5	6	7	8	9	10	11
(1) Intention	-0.024	2.984	0.957										
(2) Reactance	-0.014	1.306	0.425	0.901									
(3) Fear	-0.001	1.842	-0.382	-0.304	0.921								
(4) Threat	-0.009	1.469	-0.438	-0.454	0.635	0.923							
(5) Facilitating conditions	0.024	1.851	0.103	-0.026	0.155	0.039	0.902						
(6) Habit	0.004	0.653	-0.435	-0.226	0.175	0.279	-0.195	0.853					
(7) Neutralization	0.025	1.836	0.675	0.544	-0.294	-0.443	0.042	-0.410	0.866				
(8) Role values	0.007	1.571	0.833	0.438	-0.264	-0.393	0.088	-0.370	0.655	0.872			
(9) Punishments	0.034	2.017	-0.235	-0.243	0.334	0.482	0.029	0.259	-0.234	-0.218	0.854		
(10) Rewards/Costs	0.013	1.651	0.329	0.270	-0.238	-0.237	0.068	-0.235	0.378	0.320	-0.078	0.901	
(11) Response efficacy	-0.002	1.249	-0.238	-0.255	0.230	0.341	0.034	0.252	-0.223	-0.205	0.194	-0.120	0.883

Note: The diagonal represents the square root of the Averaged Variance Extracted (AVE) for the respective construct.

Table 10. Construct Reliabilities

Construct	Cronbach's Alpha	Construct	Cronbach's Alpha
Intention	.9783	Reactance	.9095
Fear	.9351	Threat	.9332
Facilitating conditions	.9226	Habit	.9067
Neutralization	.8871	Role values	.8975
Punishments	.8875		

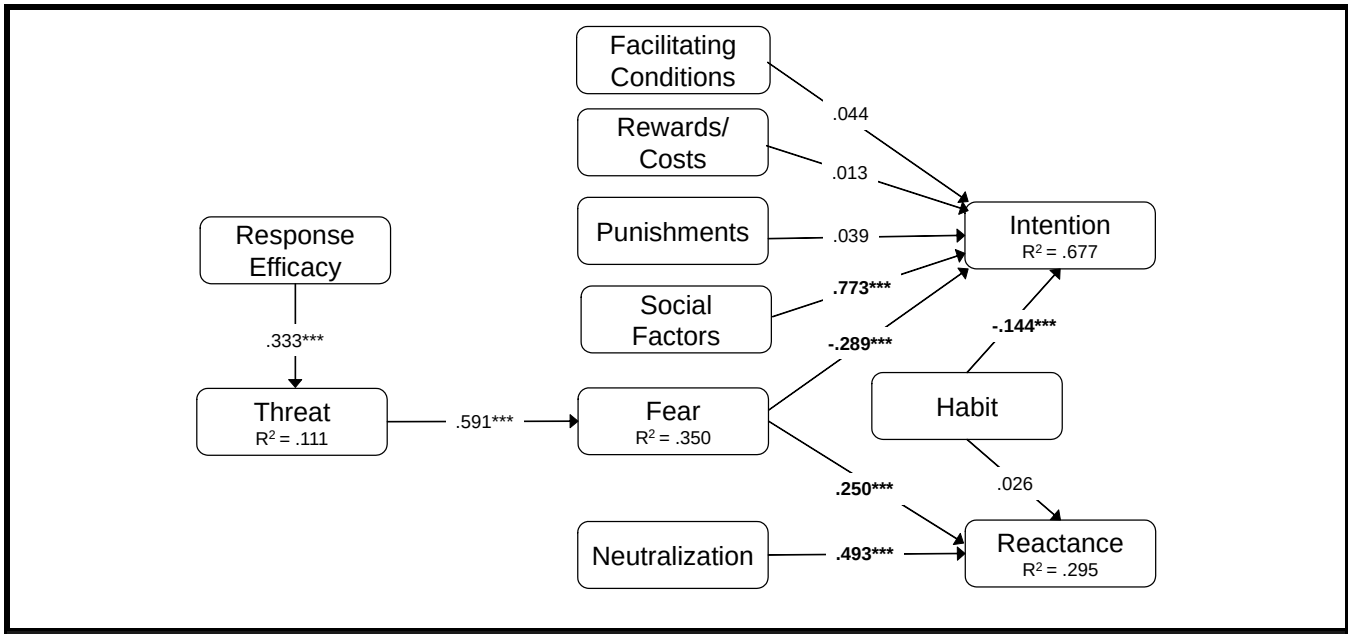


Figure 4. UMISPC Results

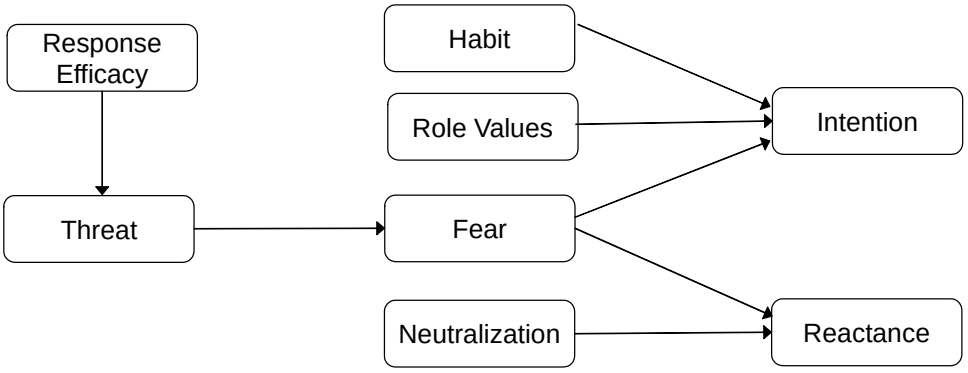


Figure 5. Refined UMISPC

First, we found support for the dual pathways proposed by EPPM, which in our case were (1) intention to comply with ISS policies and (2) reactance (denying the possible ISS problem). We found that the constructs of NoT, fear, habit, and role values were important predictors of the dual outcomes proposed above. We also found that both NoT and fear significantly predicted reactance. The denial of the possible ISS problem was a non-desired behavior in regard to information security, as actual security of information or the system was not increased with this outcome. We further found that fear was predicted by the perceived threat, which in turn was predicted by response efficacy.

We determined that protective behavioral intentions to comply with ISS policies were strongly explained by role values, fear, and habit. Role values had the largest impact on the intention to comply, with both fear and habit detracting from the same intention. We note that, despite previous research, punishments, rewards/costs, and facilitating conditions had no significant impact on the intention construct. Possible reasons for the results will be discussed later in this section.

Given that portions of the proposed UMISPC are not supported, we refined our proposed model to only include the supported pathways for ISS compliance (intentions). This refined UMISPC is shown in Figure 5. We further discuss the importance of these findings for research and practice in the next section.

Discussion

The UMISPC: Current Empirical Support

Our key proposed contribution is the UMISPC. Extant behavioral ISS research has presented several differing theoretical models derived from different disciplines to explain or predict employees' ISS policy violations or associated intentions. The application of theories from different disciplines to ISS policy violations has led to a jungle of different ISS behavioral models. Disentangling this jungle of available models is difficult for two reasons. First, many of these theories and models have concepts that resemble one another, which raises the question of the extent to which the different theories and models are similar. As a case in point, sanctions are studied under deterrence theory (D'Arcy and Hovav 2007; Siponen and Vance 2010), costs under rational choice theory (Vance and Siponen 2012), and constraints under CBT (Tittle 1995). To what extent these theories provide complementary explanations that can be synthesized into one unified theoretical model to complement the possible limitations of the individual models also remains an unexamined issue.

Our data provide some support, within the context of our three scenarios, that the various constructs of the extant (11) theories can be empirically reduced to 11 factors, which still account for over 85% of the original variance. We then relied on the extant theories to explain how these 11 constructs should relate, based on prior research, and proposed a tentative model, called the UMISPC. Following Venkatesh et al. (2003), we collected a new sample and tested this model in Study 2. While the UMISPC received empirical support within the context of the three scenarios, it needs to be further tested, especially across different types of information security behaviors and situations.

Findings, Applicability, and Future Research Needs Per Construct

Next we discuss, construct by construct, which findings we assumed to be generic (across different types of ISS behav-

iors) and which we assumed to be dependent on the type the ISS action. We also outlined issues that future research needs to examine further.

Role values were proposed as a new contract in the previoius section. Based on the empirical analysis, role values were the most important explanation of ISS compliance intentions across our scenarios. We argue that role values are potentially important in ISS, given that ISS policy compliance or violations take place in a work context. To what extent the required ISS acts in the ISS guidelines are regarded as appropriate and justified is linked to the nature of the work the person performs. We speculate that role values may be a generic reason behind different ISS policy compliance behaviors (or intentions thereof). However, this is something that future research that examines role values in different ISS contexts will need to determine.

The **moral beliefs** construct was not retained in the empirical analysis. One moral question was blended with self-concept, roles, and affect, resulting in a new construct we defined as role value. This raises the question of what role moral awareness and judgment with respect to ISS policy violations plays in decisions about whether or not to comply with policies. While information security professionals at organizations, like ISS scholars, may see insecure acts as violations, the burning question is: Do ordinary users or employees see insecure acts as morally as blameworthy as violations of moral norms in the physical world (Leiwo and Heikkuri 1998; Siponen 2001)?

Social factors (TIB's or TRA's subjective norms) were not significant in our model. 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). Social visibility and social unacceptableness may be necessary conditions for social factors or subjective norms to explain ISS policy compliance. Future research should examine to what extent the social nature of the ISS acts are linked to subjective norms and similar social factors.

Deterrents and rewards were not found to be significant within our scenarios. Deterrents, which are among the most examined constructs in ISS behavior (D'Arcy et al. 2009; Harrington 1996; Herath and Rao 2009; Peace et al. 2003; Siponen and Vance 2012; Theoharidou et al. 2005), have enjoyed mixed results (D'Arcy and Herath 2011). We see two explanations for our results. First, it could be that in the context of password sharing, USB practices, and locking computers, sanctions are not used as often. This could explain the lack of deterrent experience (Gibbs 1975). Another potential explanation is role values. In research that reports significant findings regarding sanctions (D'Arcy and Herath 2011), role values are not examined. One potential reason for the insignificance of deterrence constructs is the lack of role values in prior work. Our results regarding deterrence theory before the unification (in Study 1) show a rather weak role of the severity of sanctions, which fades away when role values are added to the UMISPC (in Study 2).

Little research in ISS has explored the effects of **habits** on security-related behaviors, with the exception of Vance et al. (2012). Future research should examine habits in different types of ISS behaviors. One could assume that habits are related to the complexity of ISS actions. Future research also needs to examine the process that leads to an employee becoming a habitual non-complier and determine how bad habits and non-compliance behavior can be changed.

We reported the importance of the **fear** component in understanding compliance intentions. Fear has come to ISS through PMT and fear appeals (Boss et al. 2015; Johnston et al. 2015). While fear is examined in health psychology and linked to the avoidance of health threats (Rogers 1983; Witte et al. 1996), ISS research has been criticized as lacking fear constructs in the PMT applications (Boss et al. 2015). Fear makes sense in health psychology, where the threat refers to serious health threats or "noxious medical examination" (Rogers 1983, p. 156). However, what is debatable is whether the fear of health threat is theoretically the same as the fear of ISS risks. In the case of our fear measures, those measures that reflect fear as an emotion, such as terrifying and afraid, were not retained. Instead, indications of potential threats were retained as fear. Future research should examine to what extent ISS threats really evoke fear. Different types of threats could also affect whether ISS threats evoke fear. For example, it could be that only ISS threats that are viewed as being serious, like concerns that someone will access one's personal bank account, evoke fear.

Finally, the level of technical information security knowledge could also play a role in explaining whether users deny the information security threat (reactance). For example, it is possible that reactance in the context of ISS is not the result of coping with fear but rather users' low levels of technical knowledge about information security, combined with the invisibility of the threat indicators and the certainty in their belief that nothing will happen.

Neutralizations were a significance indicator for reactance; namely, denying the possible ISS problem. We theorize that the neutralization process is not only associated with the three

types of ISS policy violations (sharing passwords, USB practices, and leaving computers unlocked), but is also a generic explanation for reactance or ISS policy violations. We see no theoretical reason for why some types of ISS policy violations would not be justified by employees, but future research can examine this further. However, just as different neutralizations may explain the breaking of different laws (Maruna and Copes 2005), different neutralization techniques can be more important in explaining different types of ISS policy violations. For example, the defense of necessity, such as "I was in a hurry," is more likely to be given for not selecting a new complex password than for locking a computer. This may also explain why not all neutralization techniques loaded on the same factor. Future research can examine how specific neutralizations are connected with the violation types. In criminology, neutralizations are a sign of persisting in the crime and are hence seen as rather stable and hard to overcome (Maruna and Copes 2005). Except for research by Barlow et al. (2013), there is no study that examines how employees' neutralizations can be disabled. As a result, there is a need to examine which persuasion or communication techniques can be used to overcome neutralization-based rationalizations.

Facilitating conditions were insignificant in our model. One explanation for this is that in ISS contexts, users can perform many of the preferred ISS actions, such as avoiding sharing passwords, ensuring secure USBs, or locking computers, without any help. We speculate that facilitating conditions could have different results for more technically challenging ISS actions, such as using encryption to secure email and/or selecting a complex, hard-to-break password. Future research needs to examine this.

Limitations and Boundary Conditions of the UMISPC

Relying on the data-driven approach when specifying the UMISPC requires several trade-offs. First, data reduction methods such as factor analysis produce results that may not be arrived at through a theoretical analysis of the literature. Second, the data-driven approach to arriving at our factors for the unified theory merges assumptions across theories. However, data-driven analysis of the items, their variances, and error terms may show that these constructs are more convergent than divergent when compared to all other constructs from the disparate theories included in the analysis. Relying on the data-driven approach also limits the findings based on the quality of the data used in the analysis. 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. Finally, although our data was only from Finland, there may not be a clear *a priori* theoretical reason why the results would be different in different countries, as none of the 11 theories contain cultural elements. Nevertheless, future research could possibly theorize and examine any cultural differences.

Implications for Practice

Our results highlight the following managerial implications. Given that response efficacy has a significant impact on threat, organizations could consider getting employees to believe that complying with information security procedures (ISP) keeps information security breaches down. They would also need to convey that not only employees but the entire organization could be subject to an information security threat if employees do not comply with the ISP.

Pointing out the threat in terms of its implications for both organizational and employee privacy and security seems to be important, at least based on our results. Information security education and campaigning at organizations should, therefore, include content that specifically relates to the threat, its impact, and the effectiveness of the recommended protective actions in removing the threat.

In the aforementioned introduction of the threat, however, organizations need to exercise care, since too much threat and not enough efficacy may backfire, negatively impacting employees, who may instead react against security awareness and training programs and behave insecurely (reactance). The EPPM explanation for this is arousal of negative emotions and fear in individuals, if the threat is perceived to be significant, leading to reduced intentions to engage in secure behaviors. This reactance can also result from situations in which individuals do not see any indicators of a concrete threat, such as warnings by anti-malware tools, computers slowing down, or program crashes increasing. Indeed, it is easy to believe that no breaches have occurred when there are no observable indicators suggesting that anything has happened. Of course, it is a feature of effective malware or hackers that the malware or hacker is maximally invisible. Actions that make IS incidents visible to employees should be considered.

This study found that punishments and rewards/costs did not significantly impact intentions (Bagozzi 1992), based on our data. Contrary to the notions of PMT (Rogers 1975, 1983) and DT (Gibbs 1975), costs associated with secure behaviors did not positively or negatively impact the intention to engage in those behaviors. Likewise, perceived punishments if an employee were to be caught engaging in insecure behaviors did not significantly increase the intention to behave securely.

A potential explanation for this is the lack of the deterrence effect (Gibbs 1975)—namely, that sanctions are not effective if there are no examples of people who have been caught. Therefore, based on our results, increased monitoring and control efforts would appear to have little impact on whether individuals could be motivated through deterrent mechanisms to comply with security policies, unless there are examples of people getting caught. If there are no examples of punishments, the effect of deterrents is argued to be marginal.

Our results highlight role values as important in explaining employees' compliance with ISS policies. Role values refer to the extent to which the required ISS acts in the ISS guidelines are regarded as appropriate and justified and are linked to the nature of the work the person performs. These results imply the need for ISS regulative actions (e.g., user guidelines or procedures) that match the context of the employees' work and their work tasks. In addition, carefully explaining the need to comply with ISS procedures in employees' specific work is important in ensuring employees' compliance with ISS procedures.

Management should thus rely more on security climate and culture as well as on awareness campaigns that can be used to heighten organizational members' perception of social factors that encourage security compliance.

Our results suggest that NoT has a significant impact on reactance. NoT suggests that individuals rationalize why they would violate the ISP. To address this challenge, one option for organizations is to pose counterarguments in training sessions to make a case that shows how noncompliant behavior has the potential to seriously damage the organization, even if the harm may not be immediately visible. Another thing that could be helpful is to discuss the importance of compliance with ISS procedures compared to other work tasks.

Finally, our results regarding facilitating conditions suggest that avoiding password sharing, using secure USB practices, and logging out of computers are actions that employees can carry out without increasing their technical knowledge or technical support. This may imply that, for similarly easy protective actions, organizations need to provide more persuasive communication than technical support and focus on other factors.

Finally, our results suggest that social factors are insignificant, which is explained by the nature of the three scenarios. Our results imply that social factors may not play a role in ISS actions that are not socially visible, and hence their use for non-visible ISS actions may not be important. However, socially visible ISS actions, such as a clean desk policy or social factors in terms of supervisory pressure, could be used.

Conclusions

ISS behavioral research has produced different competing models based on a variety of theories. This paper first reviewed 11 theories that have served the majority of all previous information security behavior models, namely, (1) the theory of reasoned action, (2) techniques of neutralization, (3) the health belief model, (4) the theory of planned behavior, (5) the theory of interpersonal behavior, (6) the protection motivation theory, (7) the extended protection motivation theory, (8) deterrence theory and RCT, (9) the theory of self-regulation, (10) the extended parallel processing model, and (11) the control balance theory.

Then, we empirically compared these theories with a random sample of working professionals and proposed a tentative, unified model called the unified model of information security policy compliance (UMISPC), using a data-driven approach. This was our first empirical study (Study 1). Finally, we tested the UMISPC with new data collection ($n = 274$), using a different sample from the same population. This was our second empirical study (Study 2).

The contribution of this study is the UMISPC, which is a first step in empirically examining to what extent the available ISS models are empirically similar and to what extent the disparate theories can complement one another. While future research is required to further test the tentative UMISPC, the empirical findings so far support the model, within the three types of ISS policy violations we used to test our model. To what extent the UMISPC can obtain offer support in different ISS contexts (type of violations) will be seen in future research. Such results will show to what extent the UMISPC needs to be contextualized to account for types of ISS policy violations or whether the UMISPC is generalizable beyond the three types of ISS violations we used. Especially, four avenues for future research on the UMISPC are encouraged. First, the UMISPC can be tested in different contexts to determine its boundaries and identify situations in which the UMISPC components fail to explain a phenomenon. Second, the research stream can further extend the UMISPC by adding on additional constructs and moderators in different contexts. Third, future research may find that some of the constructs of the UMISPC may not be relevant in certain ISS contexts. Finally, we hope that our unification research inspires future IS research to further theorize and empirically demonstrate the important differences between rival theories in the ISS context that are not captured by current measures.

Acknowledgments

This research was funded by the Finnish Funding Agency for Innovation, European Regional Development Fund (ERDF), and the Academy of Finland. We thank the SE and the review team for their comments.

References

Ajzen, I. 1985. "From Intentions to Actions: A Theory of Planned Behavior," *Action-Control: From Cognitions to Behavior* (11:), pp. 11-39.

Akers, R. L., Krohn, M. D., Lanza-Kaduce, L., Radosevich, M. 1979. "Social Learning and Deviant Behavior: A Specific Test of a General Theory," *American Sociological Review* (44:4), pp. 636-655.

Ashforth, B. E., and Mael, F. 1989. "Social Identity Theory and the Organization," *Academy of Management Review* (14:1), pp. 20-39.

Ashforth, B. E., Rogers, K. M., and Corley, K. G. 2011. "Identity in Organizations: Exploring Cross-Level Dynamics," *Organization Science* (22:5), pp. 1144-1156.

Bagozzi, R. P. 1992. "The Self-Regulation of Attitudes, Intentions, and Behavior," *Social Psychology Quarterly* (55:2), pp. 178-204.

Bamberg, S., and Schmidt, P. 2003. "Incentives, Morality, or Habit? Predicting Students' Car Use for University Routes with the Models of Ajzen, Schwartz, and Triandis," *Environment and Behavior* (35:2), pp. 264-285.

Bandura, A. 1977. "Self-Efficacy: Toward a Unifying Theory of Behavioral Change," *Psychological Review* (84:2), pp. 191-215.

Barlow, J., Warkentin, M., Ormond, D., and Dennis, A. 2013. "Don't Make Excuses! Discouraging Neutralization to Reduce IT Policy Violation," *Computers & Security* (39:Part B), pp. 145-159.

Baskerville, R., and Siponen, M. T. 2002. "An Information Security Meta-Policy for Emergent Organizations," *Journal of Logistics Information Management* (15:5/6), pp. 337-346.

Becker, G. S. 1974. "Crime and Punishment: An Economic Approach," in *Essays in the Economics of Crime and Punishment*, G. S. Becker and W. M. Landes (eds.), Cambridge, MA: National Bureau of Economic Research, pp. 1-54,.

Becker, M. H. 1974. "The Health Belief Model and Personal Health Behavior," *Health Education Monograph Series* (2:4), pp. 324-508.

Bergeron, F., Raymond, L., Rivard, S., Gara, M.-F. 1995. "Determinants of EIS Use: Testing a Behavioral Model," *Decision Support Systems* (14:2), pp. 131-146.

Boss, S. R., Galletta, D. F., Lowry, P., Moody, G., and Polak P. 2015. "What Do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Behaviors in Users," *MIS Quarterly* (39:4), pp. 837-864,

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R., and 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), pp. 151-164.

Braithwaite, J. 1989. *Crime, Shame and Reintegration*, Cambridge, UK: Cambridge University Press.

Bulgurcu, B., Cavusoglu, H., Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-546.

Curry, T. R. 2005. "Integrating Motivating and Constraining Forces in Deviance Causation: A Test of Causal Chain Hypotheses in Control Balance Theory," *Deviant Behavior* (26:6), pp. 571-599.

D'Arcy, J., and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings," *European Journal of Information Systems* (20:6), pp. 643-658.

D'Arcy, J., Herath, T., and Shoss, M. K. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *Journal of Management Information Systems* (31:2), pp. 285-318.

D'Arcy, J., and Hovav, A. 2007. "Deterring Internal Information Systems Misuse," *Communications of the ACM* (50:10), pp. 113-117.

D'Arcy, J., Hovav, A., and Galletta, D. F. 2009. "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (23:1), pp. 79-98.

Festinger, L. 1957. *A Theory of Cognitive Dissonance*, Stanford, CA: Stanford University Press.

Fishbein, M., and Ajzen, I. 1975. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, Reading, MA: Addison-Wesley.

Floyd, D. L., Prentice-Dunn, S., and Rogers, R. W. 2000. "A Meta-Analysis of Research on Protection Motivation Theory," *Journal of Applied Social Psychology* (30:2), pp. 407-429.

Frattaroli, J. 2006. "Experimental Disclosure and its Moderators: A Meta-Analysis," *Psychological Bulletin* (132:6), pp. 823-865.

Gagnon, M.-P., Godin, G., Gane, C., Fortin, J.-P., Lamothe, L., Reinharz, D., and Cloutier, A. 2003. "An Adaptation of the Theory of Interpersonal Behavior to the Study of Telemedicine Adoption by Physicians," *International Journal of Medical Informatics* (71:2-3), pp. 103-115.

Galletta, D. F., and Polak, P. 2003. "An Empirical Investigation of Antecedents of Internet Abuse in the Workplace," in *Proceedings of the SIG Workshop on Human–Computer Interaction*, pp. 47-51.

Gefen, D., Straub, D. W., and Rigdon, E. E. 2011. "An Update and Extension to Sem Guidelines for Admnistrative and Social Science Research," *MIS Quarterly* (35:2), pp. iii-xiv.

Gibbs, J. P. 1975. *Crime, Punishment, and Deterrence*, New York: Elsevier.

Hair, J. F., Black, B., Babin, B., Anderson, R. E., anTatham. R. L. 2006. *Multivariate Data Analysis* (6th ed.), Upper Saddle River, NJ: Pearson Prentice Hall.

Harrington, S. J. 1996. "The Effect of Codes and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *MIS Quarterly* (20:3), pp. 257-278.

Hirschheim, R., Klein, H. K., and Lyytinen, K. 1995. *Information Systems Development and Data Modelling: Conceptual and Philosophical Foundations*, Cambridge, UK: Cambridge University Press.

Herath, T., and Rao, H. R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:1), pp. 106-125.

Janz, N. K., and Becker, M. H. 1984. "The Health Belief Model: A Decade Later," *Health Education & Behavior* (11:1), pp. 1-47.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.

Johnston, A. C., Warkentin, M., and Siponen, M. 2015. "An Enhanced Fear Appeal Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric," *MIS Quarterly* (39:1), pp. 113-134.

Kock, N., and Lynn, G. S. 2012. "Lateral Collinearity and Misleading Results in Variance-Based SEM: An Illustration and Recommendations," *Journal of the Association for Information Systems* (13:7), Article 2.

Laudan, L. 1978. *Progress and its Problems: Towards a Theory of Scientific Growth*, Berkeley, CA: University of California Press.

Lee, S. M., Lee, S.-G., and Yoo, S. 2004. "An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories," *Information & Management* (41:6), pp. 707-718.

Leiwo, J., and Heikkuri, S. 1998. "An Analysis of Ethics as Foundation of Information Security in Distributed Systems," in *Proceedings of the 31st Hawaii International Conference on Systems Sciences*, Los Alamitos, CA: IEEE Computer Society Press.

Leone, L., Perugini, M., and Ercolani, A. P. 1999. "A Comparison of Three Models of Attitude–Behavior Relationships in the Studying Behavior Domain," *European Journal of Social Psychology* (29:2-3), pp. 161-189.

Liang, H., and Xue, Y. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly* (33:1), pp. 71-90.

Liang, H., and Xue, Y. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems* (11:7), pp. 394-413.

Limayem, M., and Hirt, S. G. 2003. "Force of Habit and Information Systems Usage: Theory and Initial Validation," *Journal of the Association for Information Systems* (4:1), pp. 65-97.

Liska, A. E., Krohn, M. D., and Messner, S. F. 1989. "Strategies and Requisites for Theoretical Integration in the Study of Crime and Deviance," in *Theoretical Integration in the Study of Deviance and Crime: Problems and Prospects*, S. F. Messner, M. D. Krohn, A. E. Liska (eds.), Albany, NY: SUNY Press, pp. 1-20.

Lowry, P. B., and Moody, G. D. 2015. "Proposing the Control Reactance Compliance Model (CRCM) to Explain Opposing Motivations to Comply with Organizational Information Security Policies," *Information Systems Journal* (25:50, pp. 433-463.

Maddux, J. E., and Rogers, R. W. 1983. "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change," *Journal of Experimental Social Psychology* (19:5), pp. 469-479.

Maloney, E. K., Lapinski, M. K., and Witte, K. 2011. "Fear Appeals and Persuasion: A Review and Update of the Extended Parallel Process Model," *Social and Personality Psychology Compass* (5:4), pp. 206-219.

Marsh, H. W., and Hocevar, D. 1985. "Application of Confirmatory Factor Analysis to the Study of Self-Concept: First- and Higher Order Factor Models and Their Invariance Across Groups," *Psychological Bulletin* (97), pp. 362-582.

Maruna, S., and Copes, H. 2005. "What Have We Learned from Five Decades of Neutralization Research?," *Crime and Justice* (32), pp. 221-320.

Mishra, S., and Dhillon, G. 2006. "Information Systems Security Governance Research: A Behavioral Perspective," in *Proceedings of the 1st Annual Symposium on Information Assurance, Academic Track of the 9th Annual 2006 NYS Cyber Security Conference*, New York, pp. 18-26.

Ng, B.-Y., Kankanhalli, A., and Xu, Y. 2009. "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems* (46:4), pp. 815-825.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior Towards IS Security Policy Compliance," in *Proceedings of 40th Annual Hawaii International Conference on System Sciences*, Los Alamitos, CA: IEEE Computer Society Press.

Paternoster, R. 2010. "How Much We Really Know about Criminal Deterrence?," *Journal of Criminal Law and Criminology* (100:3), pp. 765-824.

Paternoster, R., and Simpson, S. 1996. "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime," *Law & Society Review* (30:3), pp. 549-584.

Peace, A. G., Galletta, D. F., and Thong, J. Y. 2003. "Software Piracy in the Workplace: A Model and Empirical Test," *Journal of Management Information Systems* (20:1), pp. 153-177.

Pee, L. G., Woon, I. M. Y., and Kankanhalli, A. 2008. "Explaining Non-Work-Related Computing in the Workplace: A Comparison of Alternative Models," *Information & Management* (45:2), pp. 120-130.

Pogarsky, G. 2004. "Projected Offending and Implications for Heterotypic Continuity," *Criminology* (42:1), pp. 111-135.

Puhakainen, P., and Siponen, M. 2010. "Improving Employee's Compliance through IS Security Training: An Action Research Study," *MIS Quarterly* (34:4), pp. 757-778.

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

Rogers, R. W. 1983. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation," in *Social Psychophysiology*, J. Cacioppo and R. E. Petty (eds.), New York: Guilford, pp. 153-176.

Sheppard, B. H., Hartwick, J., and Warshaw, P. R. 1988. "The Theory of Reasoned Action: A Meta-Analysis of Past Research with Recommendations for Modifications and Future Research," *Journal of Consumer Research* (15:12), pp. 325-343.

Siponen, M. 2001. "On the Role of Human Morality in Information System Security: From the Problems of Descriptivism to Non-descriptive Foundations," in *Social Responsibility in the Information Age: Issues and Controversies*, G. Dillon (ed.), Hershey, PA: Idea Group Publishing, pp. 239-254.

Siponen, M. 2005. "Analysis of Modern IS Security Development Approaches: Towards the Next Generation of Social and Adaptable ISS Methods," *Information and Organization* (15:4), pp. 339-375.

Siponen, M., Karjalainen, M., and Sarker, S. 2010. "Unearthing Social Mechanisms that Lead Employees to Violate IS Security

Procedures: An Inductive Study," in *Proceedings of Dewald Roode Workshop on Information Systems Security Research, IFIP Working Group 8.11/11.13*, B. Molyneux and A. Vance (eds.) (https://ifip.byu.edu/ifip2010.html).

Siponen, M., Mahmood, M. A., and Pahnila, S. 2014. "Employees' Adherence to Information Security Policies: An Exploratory Field Study," *Information & Management* (51:2), pp. 217-224.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-502.

Siponen, M., and Vance, T. 2014. "Examining the Phenomenon of Deliberate IS Security Policy Violations: A Call and Guidelines for Research," *European Journal of Information Systems* (23:3), pp. 289-305.

Siponen, M., Vance, T., and Willison, R. 2012. "New Insights into the Problem of Software Piracy: The Effects of Neutralization, Shame, and Moral Beliefs," *Information & Management* (49:7), pp. 334-341.

Straub, D. W. 1990. "Effective IS Security," *Information Systems Research* (1:3), pp. 255-276.

Straub, D., Goodman, S., and Baskerville, R. 2008. "Framing the Information Security Process in Modern Society," in *Information Security: Policy, Processes, and Practices*, D. W. Straub, S. Goodman, R. Baskerville (edsl), Armonk, NY: M. E. Sharpe Inc., pp. 5-12.

Sykes, G. M., and Matza, D. 1957. "Techniques of Neutralization: A Theory of Delinquency," *American Sociological Review* (22:6), pp. 664-670.

Teh, P.-L., Ahmed, P. K., and D'Arcy, J. 2015. "What Drives Information Security Policy Violations among Banking Employees? Insights from Neutralization and Social Exchange Theory," *Journal of Global Information Management* (23:1), pp. 44-64.

Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E. 2005. "The Insider Threat to Information Systems and the Effectiveness of ISO17799," *Computers & Security* (24:6), pp. 472-484.

Tittle, C. R. 1995. *Control Balance: Toward a General Theory of Deviance*, Boulder, CO: Westview Press.

Triandis, H. 1977. *Interpersonal Behavior*, Pacific Grove, CA: Brooks/Cole Publishing Company.

Vance, T., and Siponen, M. 2012. "IS Security Policy Violations: A Rational Choice Perspective," *Journal of Organizational and End User Computing* (24:1), pp. 21-41.

Vance, T., Siponen, M., and Pahnila, S. 2012. "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49:2), pp. 190-198.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), pp. 425-478.

Venkatesh, V., Thong, J. Y. L., and Xin, X. 2012. "Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology" *MIS Quarterly* (36:1), pp. 157-178.

Verplanken, B. 2006. "Beyond Frequency: Habit as Mental Construct," *British Journal of Social Psychology* (45:3), pp. 639-656.

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18:2), pp. 101-105.

Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly*, (37:1), pp. 1-20.

Witte, K. 1992. "Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model," *Communication Monographs* (59:4), pp. 329-349.

Witte, K., Cameron, K. A., McKeon, J. K., and Berkowitz, J. M. 1996. "Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale," *Journal of Health Communications* (1:4), pp. 317-341.

About the Authors

Gregory D. Moody (Ph.D., University of Pittsburgh; Ph.D., University of Oulu) is currently an assistant professor in the Management, Entrepreneurship and Technology Department in the Lee Business School at the University of Nevada, Las Vegas, and director of the Graduate MIS program. He has published in *Information Systems Research, MIS Quqrterly, Journal of Management Information Systems, Journal of the AIS, European Journal of Information Systems,*and other journals. His interests include IS security and privacy, e-business (electronic markets, trust) and human–computer interaction (Web site browsing, entertainment). He is currently an associate editor and managing editor for *Information Systems Journal* and *AIS Transactions on Human–Computer Interaction*, THCI, an officer in SIGHCI.

Mikko Siponen is full professor of Information Systems. He has served as vice head of department, head of department and a director of a research center. His degrees include Doctor of Social Sciences, majoring in Philosophy; M.Sc. in Software Engineering; Lic.Phil. in Information Processing Sciences; and Ph.D. in Information Systems. He has received over 10 million EUR of research funding from corporations and numerous other funding bodies. In addition to leading industry-funded projects, Mikko has been a PI on projects for the Academy of Finland, the EU, and the Finnish Funding Agency for Innovation. He has published 48 articles in journals such as *MIS Quarterly*, *Information Systems Research*, and *Journal of the Association for Information Systems*.

Seppo Pahnila received his Ph.D. in Information Processing Science from the University of Oulu, Finland, where he holds an adjunct professorship in Information Processing Science. His current interests are information systems security, information systems security policy and personalized information systems. He has published in such journals as *European Journal of Information Systems, Information & Management, Communications of the ACM, IEEE Computer*, and *Pacific Asia Journal of the Association for Information Systems*.

MIS Quarterly

RESEARCH ARTICLE

TOWARD A UNIFIED MODEL OF INFORMATION SECURITY POLICY COMPLIANCE

Gregory D. Moody
University of Nevada, Las Vegas, 4505 S. Maryland Parkway,
Las Vegas, NV 89154 U.S.A. {gregory.moody@unlv.edu}

Mikko Siponen
Faculty of Information Technology, University of Jyväskylä, P.O. Box 35,
FI-40014 Jyväskylä FINLAND {mikko.t.siponen@jyu.fi}

Seppo Pahnila
Faculty of Information Technology and Electrical Engineering, University of Oulu, P.O. Box 8000,
FI-90014 Oulu FINLAND {seppo.pahnila@oulu.fi}

Appendix A

Instruments

Scenarios (Siponen and Vance 2010)

Note that all scenarios were altered to use one common last name, Mattila. Further, this survey was distributed in Finnish, and Finnish does not have gendered pronouns (e.g., her/his or he/she); everything is referred to with a non-gendered pronoun.

USB Drive

Mattila is a mid-level manager in a medium-sized business where he has worked for several years. Mattila is currently working on a sales report that requires the analysis of the company's customer database, which contains sensitive financial and purchase history information. Because of the sensitive nature of the corporate data, the company has a strict policy prohibiting the copy of corporate data to unencrypted media, such as USB drives. However, Mattila will travel for several days and would like to analyze the corporate database on the road. Mattila expects that copying the data to the USB drive and taking it on the road could save the company a lot of time and money.

Workstation Logout

Mattila is a mid-level manager in a medium-sized company where he was recently hired. His department uses an inventory procurement software application program to allow only authorized employees to make inventory purchases. The company has a firm policy that employees must log out of or lock their computer workstation when not using it. Mattila expects that keeping his user account logged-in could save him and coworkers time in ordering inventory.

Passwords

Mattila is a low-level manager in a small company where he was recently hired. His company has a strong policy that each computer workstation must be password protected and that passwords are not to be shared. However, Mattila is on a business trip and one of his coworkers needs a file on his computer. Mattila expects that sharing his password could save his coworker a lot of time and effort.

Note: Unless noted, all items are measured on a typical seven-point Likert scale from strongly disagree to strongly agree.

Miscellaneous Questions

1. What is your current age?
2. What is your gender?
3. How many years of work experience do you have?
4. How realistic do you think the above scenario is?
5. Do you think this scenario is realistic? Why or why not?

Intention (Piquero and Piquero 2006)

1. What is the chance that you would do what Mattila did in the described scenario?
2. I would act in the same way as Mattila did if I were in the same situation.

Protection Motivation Theory (Milne et al. 2000; Woon et al. 2005)

Perceived Severity

1. An information security breach in my organization would be a serious problem for me.
2. An information security breach in my organization would be a serious problem for my organization.
3. If I were to do what Mattila did, there would be a serious information security problem for my organization.
4. If I were to do what Mattila did, a serious information security problem would result.

Perceived Vulnerability

1. I would be subjected to an information security threat if I were to do what Mattila did.
2. My organization would be subjected to an information security threat if I were to do what Mattila did.
3. An information security problem would occur if I were to do what Mattila did.

Response Efficacy

1. Complying with information security procedures in our organization keeps information security breaches down.
2. If I were to comply with information security procedures, IS security breaches would be scarce.
3. If I were to do the opposite to what Mattila did, it would keep IS security breaches down.
4. If I were to do the opposite to what Mattila did, IS security breaches would be minimal.

Self-Efficacy

1. I can comply with information security procedures by myself.
2. I can use information security measures if someone tells me what to do as I go along.
3. Doing the opposite of what Mattila did would be difficult for me to do.
4. Doing the opposite of what Mattila did would be easy for me to do.

Response Cost (Woon et al. 2005)

1. Complying with information security procedures would be time consuming.
2. Complying with information security procedures would take work time.
3. Doing the opposite of what Mattila did would be time consuming.
4. Complying with information security procedures makes my work more difficult.
5. Complying with information security procedures inconveniences my work.
6. There are too many overheads associated with complying with information security procedures.
7. Complying with information security procedures would require considerable investment of effort other than time.

Rewards (Abraham et al. 1994)

1. If I were to do what Mattila did, I would save time.
2. If I were to do what Mattila did, I would save work time.
3. Not complying with information security procedures saves work time.

Habit (Verplanken and Orbell 2003)

1. Complying with information security procedures is something I do frequently.
2. Complying with information security procedures is something I do automatically.
3. Complying with information security procedures is something I do without having to consciously remember.
4. Complying with information security procedures is something that makes me feel weird if I do not do it.
5. Complying with information security procedures is something I do without thinking.
6. Complying with information security procedures is something that would require effort not to do it.
7. Complying with information security procedures is something that belongs to my (daily, weekly, monthly) routine.
8. Complying with information security procedures is something I start doing before I realize I'm doing it.
9. Complying with information security procedures is something I would find hard not to do.
10. Complying with information security procedures is something I have no need to think about doing.
11. Complying with information security procedures is something that's typically "me."
12. Complying with information security procedures is something I have been doing for a long time.

Attitude (Triandis 1977)

The scales for these items are anchored with the words listed below.

If I were to do what Mattila did it would be a very:

(a) bad idea-good idea
(b) foolish idea-wise idea
(c) unpleasant idea-pleasant idea
(d) negative idea-positive idea

Subjective Norm (Johnston and Warkentin 2010)

1. I believe that top management in my organization thinks I should do what Mattila did.
2. I believe that my immediate supervisor in my organization thinks I should do what Mattila did.
3. I believe that coworkers in my organization think I should do what Mattila did.
4. I believe that the security staff in my organization thinks I should do what Mattila did.

Perceived Behavioral Control (Ajzen 2002)

1. If you were to do as Mattila did, how much would you feel like you were in charge of the situation?
2. If you were Mattila, how much would you feel able to not do as he did?
3. If you were Mattila, how much would you feel you were in control?

Desire (Kanfer and Ackerman 1989)

1. I want to comply with the organization's security procedures.
2. My desire to comply with the organization's security procedures can be defined as something that is very important to me.

Costs/Benefits (McClenahan et al. 2007)

1. Mattila's behavior against the security procedures cause harm to the organization.
2. Mattila's behavior against the security procedures weakens the organization's security.
3. Mattila's behavior against the security procedures increases the vulnerability of the organization.

Facilitating Conditions (Bamberg and Schmidt 2003)

1. I am too busy to comply with information security procedures.
2. I have enough knowledge to follow information security procedures.
3. I need more guidance from my superiors with work-related information security policies.
4. I need more guidance from the IT/information security personnel regarding information security issues related to my work.
5. Support is available if I experience difficulties in complying with information security procedures.

Affect (Limayem and Hirt 2003)

1. What Mattila did is smart.
2. What Mattila did is enjoyable.
3. What Mattila did is boring.
4. What Mattila did is pleasant.

Roles (Bamberg and Schmidt 2003)

1. What Mattila did is compatible with his/her work.
2. What Mattila did fits with his/her work style.
3. What Mattila did can be justified due to the nature of Mattila's work.

Self-Concept (Gagnon et al. 2003)

1. I would feel guilty if I did what Mattila did.
2. What Mattila did is consistent with my principles.
3. It is acceptable to do what Mattila did.

Social Factors (Bergeron et al. 1995)

1. With respect to complying with information security procedures, I have to do as the top management of my organization thinks.
2. With respect to complying with information security procedures, I have to do as my colleagues think.
3. With respect to complying with information security procedures, I have to do as my superiors think.

Formal – Certainty (Siponen and Vance 2010)

1. What is the chance that you would be formally sanctioned (punished) if management learned that you had violated company information security policies?
2. I would receive corporate sanctions if I violated company information security procedures.
3. What is the chance that you would be warned if management learned you had violated company information security procedures?

Formal – Severity (Siponen and Vance 2010)

1. How much of a problem would it create in your life if you were warned for doing what Mattila did?
2. I would receive severe corporate sanctions if I violated company information security procedures.
3. How much of a problem would it create in your life if you were formally sanctioned for doing what Mattila did?

Informal – Certainty (Siponen and Vance 2010)

1. How likely is it that you would lose the respect and good opinion of your business associates for violating company information security procedures?
2. How likely is it that you would jeopardize your promotion prospects if management learned that you had violated company information security procedures?
3. How likely is it that you would lose the respect and good opinion of your manager for violating company information security policies?

Informal – Severity (Siponen and Vance 2010)

1. How much of a problem would it create in your life if you jeopardized your future job promotion prospects for doing what Mattila did?
2. How much of a problem would it create in your life if you lost the respect and good opinion of your business associates for violating company information security procedures?
3. How much of a problem would it create in your life if you lost the respect of your managers for violating company information security procedures?

Moral Definitions (Vance and Siponen 2012)

1. How morally wrong would it be to do what the person did in the scenario?
2. Is it morally right to violate company information security procedures?
3. I feel that violating company information security procedures is wrong.

Neutralization Techniques (Vance and Siponen 2010)

Condemnation of the Condemners

1. It is not as wrong to violate company information security procedures that are unreasonable.
2. It is not as wrong to violate company information security procedures that require too much time to comply with.
3. It is not as wrong to violate company information security procedures that are too restrictive.

Denial of Injury

1. It is OK to violate company information security procedures if no harm is done.
2. It is OK to violate company information security procedures if no damage is done to the company.
3. It is OK to violate company information security procedures if no one gets hurt.

Metaphor of the Ledger

1. I feel my general adherence to company information security procedures compensates for occasionally violating a policy.
2. I feel my good job performance compensates for occasionally violating information security procedures.
3. I feel my hard work in the company compensates for occasionally violating an information security procedure.

Appeal to Higher Loyalties

1. It is alright to violate company information security procedures to get a job done.
2. It is alright to violate company information security procedures if you get your work done.
3. It is alright to violate company information security policies if you complete the task given by management.

Defense of Necessity

1. It is alright to violate company information security procedures under circumstances where it seems like you have little other choice.
2. It is alright to violate company information security procedures when you are under a tight deadline.
3. It is alright to violate company information security procedures when you are in a hurry.

Denial of Responsibility

1. It is OK to violate company information security policies if you aren't sure what the policy is.
2. It is OK to violate company information security procedures if the security procedures are not advertised.
3. It is OK to violate company an information security procedure if you don't understand it.

Shame (Siponen and Vance 2010)

Certainty

1. I would be ashamed if business associates knew that I had violated company information security procedures.
2. How likely is it that you would be ashamed if others knew that you had violated company information security procedures?
3. How likely is it that you would be ashamed if managers knew that you had violated company information security procedures?

Severity

1. How much of a problem would it be if you felt ashamed that business associates knew you had violated company information security procedures?
2. How much of a problem would it be if you felt ashamed that others knew you had violated company information security procedures?
3. How much of a problem would it be if you felt ashamed that managers knew you had violated company information security procedures?

Reactance (Adapted from Witte et al. 1996)

To what degree do you

1. Think that the potential problems resulting from acting like Mattila did are realistic?
2. Feel that problems resulting from acting like Mattila did would not apply to you?
3. Feel that problems resulting from acting like Mattila did are overly exaggerated?
4. Think that problems resulting from acting like Mattila did are overstated?

Fear (Adapted from Osman et al. 1994)

1. Any problems that result from acting like Mattila did will never go away.
2. Something terrible will happen if I do what Mattila did.
3. Though doing what Mattila did is potentially harmful, I am going to be OK.
4. I am afraid of what may happen if I do what Mattila did.
5. Any problems that result from acting like Mattila did will go away with time.
6. Doing as Mattila did could cause a serious problem.
7. My computer might be compromised if I did what Mattila did.

8. Doing what Mattila did is terrifying.
9. I am afraid of doing what Mattila did.
10. My computer might become unusable if I did what Mattila did.
11. My computer might become slower if I did what Mattila did.

Defense Avoidance (Adapted from Witte et al. 1996)

When I first read the scenario about Mattila, my first instinct was to

1. "Want to"/"not want to" think about the problems that may result from acting like Mattila did.
2. "Want to"/"not want to" do something to prevent my computer from suffering any problems that would result if I were to act like Mattila did.

Self-Control (Curry 2005)

1. I often act on the spur of the moment without stopping to think.
2. I often do whatever brings me pleasure here and now, even at the cost of some distant goal.
3. I am more concerned with what happens to me in the short run than in the long run.
4. I will try to get things I want even when I know it's causing problems for other people.

Control Balance (Curry 2005; Tittle 1995, 2005)

Please indicate how much control (given the definition of control above) you assert and experience in the following:

1. Friendships in general
2. People you tend to hang out with
3. Relationships with significant others
4. Other people (such as neighbors, or solicitors)
5. Relationships with family members
6. Recreational activities
7. Physical body (such as avoiding or regulating illness or fatigue, or maintaining your appearance)
8. Physical environment (such as the ability to control heat, cold, regularity of food, or cleanliness)
9. Society as a whole
10. Job/place of employment
11. Salary/pay-scale
12. Workload
13. Time at work

Appendix B

Validation and Analysis Details for Analysis of Eleven Theories Used in Previous IS Behavioral Security Research

Table B1 describes the results of our measurement model and validity tests. To perform these tests, we first assess the measurement model for each theory; this is reported in the respective column. Second, as part of the test for validity and as a check for common method variance, we load all of the items on to one latent construct. Next, we create the pathways between the latent constructs, as prescribed by the theory. Finally, we report the X^2 for the saturated model, which represents all potential relationships between the latent constructs in the model.

To demonstrate that the theory has sound validity, we would expect to see that the theoretical model (Column 3) would be associated with the lowest X^2. Likewise, to demonstrate that common method variance is not a likely problem for the dataset, we would want to see that the data are better fitted, as demonstrated by a lower X^2, for the theoretical model than for the model with one latent construct (Column 2).

Column 1 is used to assess the fit of the items to the measurement model itself and is an indication of convergent and divergent validity. Ideally, it would be expected that the data would fit better to the theoretical model in Column 3. Further, the inclusion of the X^2 in Column 4 is a test to verify whether the theory is the best fit model or whether additional relationships that are not predicted in the theory better fit the data, indicating some missing relationships beyond the theory.

Table B1. Results of Tests of Data Fitness for Each Theory, Using X^2

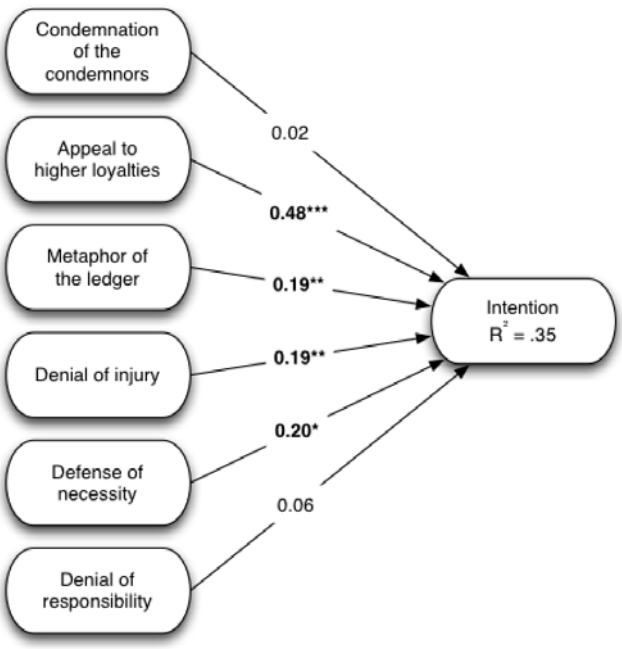
Theory	—1—	—2—	—3—	—4—
Neutralization techniques	495.89	266.34	235.09	394.07
Theory of self-regulation	452.98	238.36	112.20	94.92
Health belief model	844.12	2184.66	756.61	428.28
Theory of reasoned action	314.31	429.82	120.84	134.86
Protection motivation theory	1600.53	1255.67	720.77	545.36
Theory of interpersonal behavior	3442.23	6492.93	1773.46	1842.36
Deterrence theory	769.60	661.01	700.21	203.52
Extended protection motivation theory (PMT2)	1501.09	2334.81	1345.29	934.31
Theory of planned behavior	578.23	1036.81	393.93	269.09
Extended parallel processing model	1245.32	1741.10	816.54	622.78
Control balance theory	396.19	1217.96	364.84	191.69

1 – Measurement model
2 – Single latent construct model
3 – Theoretical model
4 – Saturated model
Note: This table does not report on every single latent construct combination that could be provided for each theory, for the sake of brevity.

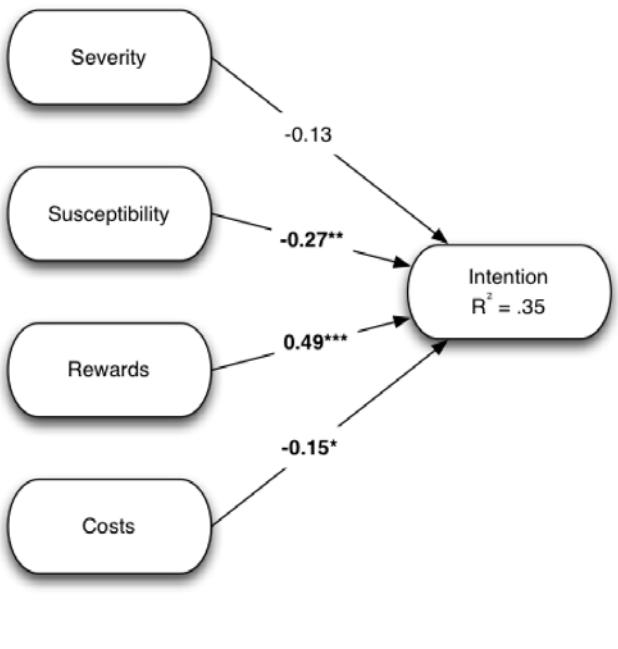
Appendix C

Results of Theory Model Tests

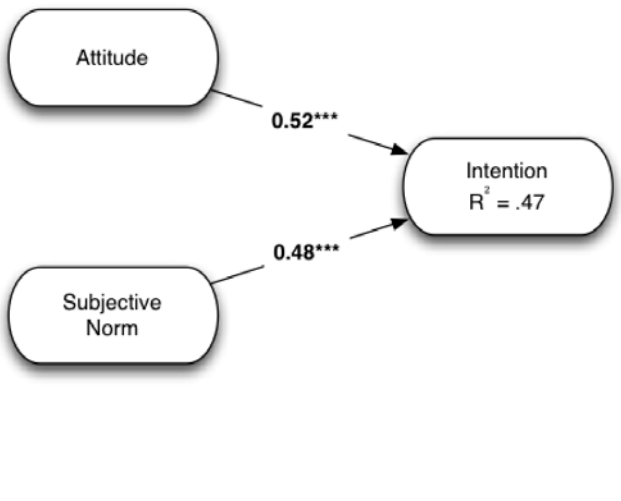
The results of each theory are presented in chronological order of publication. These results are based on CB-SEM analyses, using STATA/SE 14.1.



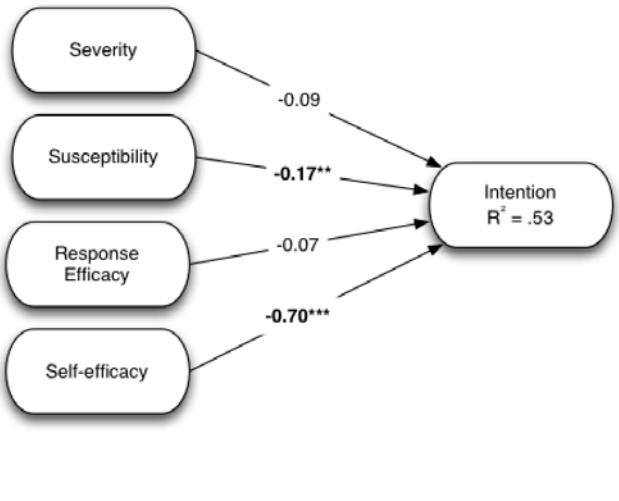
Neutralization Techniques



Health Belief Model

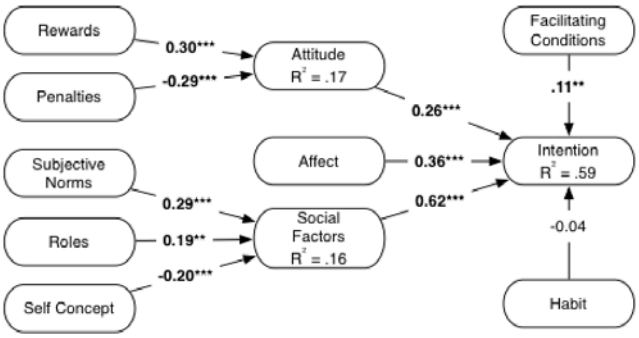


Theory of Reasoned Action

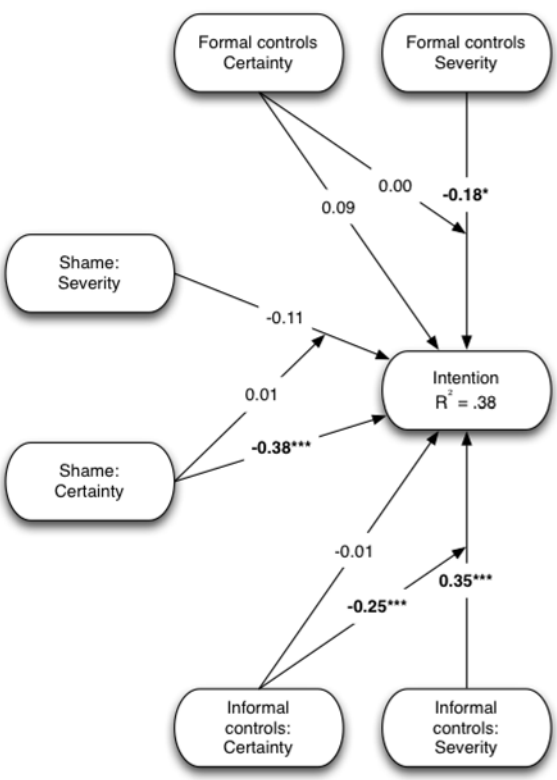


Protection Motivation Theory

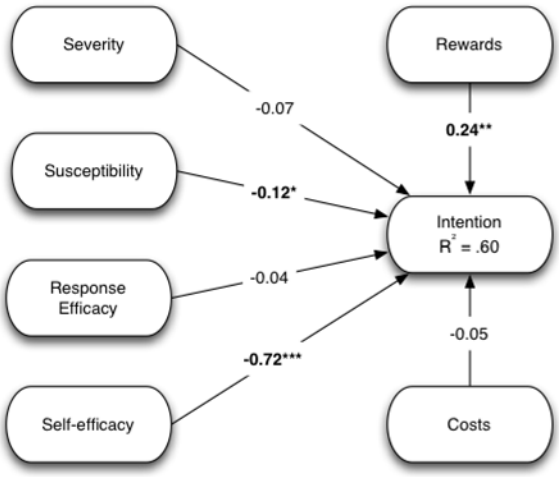
Figure C1. Results of Model Theory Tests



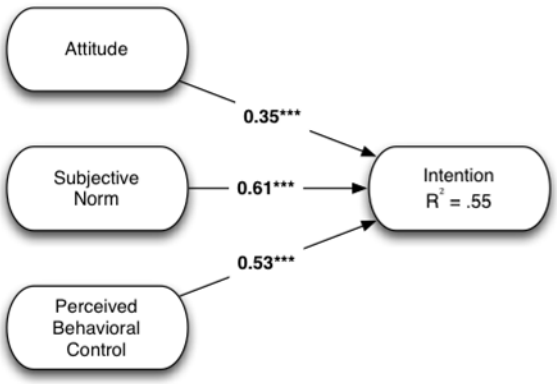
Theory of Interpersonal Behavior



Deterrence Theory

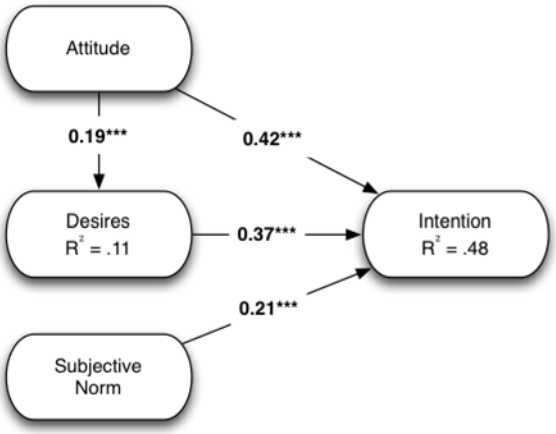


Extended Protection Motivation Theory

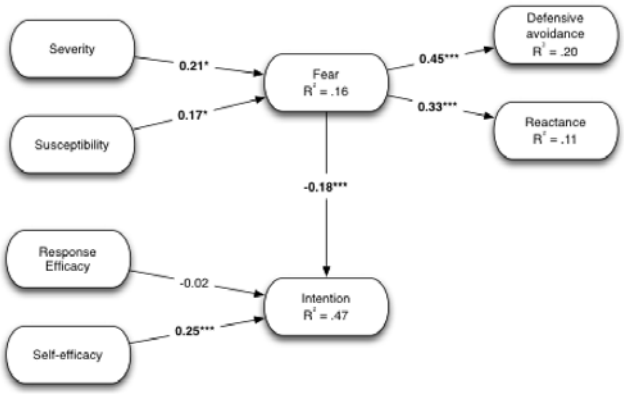


Theory of Planned Behavior

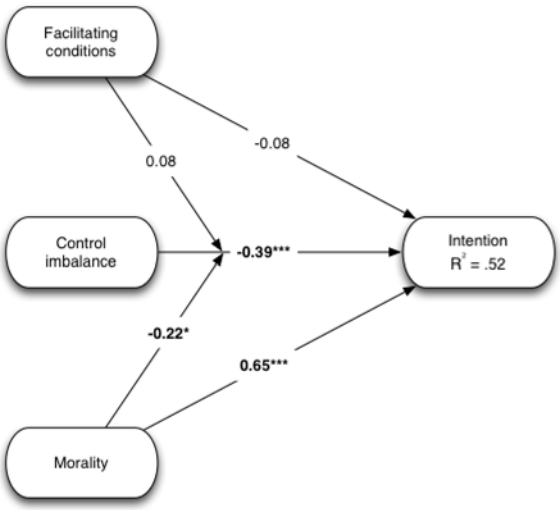
Figure C1. Results of Model Theory Tests (Continued)



Theory of Self-Regulation



Extended Parallel Processing Model



Modified Control Balance Theory

Figure C1. Results of Model Theory Tests (Continued)

Appendix D

Analysis Details for Data Reduction Analysis for UMISPC

Item Mapping for UMISPC

Table D1 show the results of the exploratory factor analysis we conducted to determine the factors needed to develop the UMISPC. Only loadings with absolute values above 0.40 were displayed to make it easier to see moderate to high loading items.

Table D1. Results from Exploratory Factor Analysis of All Items from Study 1

Item	Factor1		Factor3	Factor4	Factor5	Factor6	Factor7	Factor8
Q1Intent1	0.5322	0.4535						
Q2Intent2	0.5514	0.4809						
Q3Sever1						0.5084		
Q4Sever2						0.5687		
Q5Sever3						0.6831		
Q6Vulner1						0.6550		
Q7Vulner2						0.8079		
Q8Vulner3						0.8019		
Q9RespEffi1								
Q10RespEffi2								
Q11RespEffi3								
Q12RespEffi4								
Q13SelfEffi1								
Q14SelfEffi5								
Q15SelfEffi2								
Q16SelfEffi3								
Q17SelfEffi4								
Q18Responsecost1			0.8074					
Q19Responsecost2			0.7311					
Q20Responsecost4			0.7403					
Q21Responsecost5			0.6846					
Q22Rewards/Costs1			0.6540					
Q23Rewards/Costs2			0.6285					
Q24Rewards/Costs3			0.5630					
Q25Rewards1			0.8169					
Q26Rewards2			0.8349					
Q27Rewards3			0.7513					
Q29Rewards4			0.6941					
Q31Habit1				0.7587				
Q32Habit10				0.7635				
Q33Habit11				0.7759				
Q34Habit12				0.5634				
Q35Habit2				0.6172				

Table D1. Results from Exploratory Factor Analysis of All Items from Study 1 (Continued)

Item	Factor1		Factor3	Factor4	Factor5	Factor6	Factor7	Factor8
Q36Habit3				0.4613				
Q37Habit4				0.7488				
Q38Habit5				0.6078				
Q39Habit6				0.5768				
Q40Habit7								
Q41Habit8				0.7505				
Q42Habit9				0.7372				
Q43Atti1						-0.4250		
Q43Atti2								
Q43Atti3								
Q43Atti4								
Q44Subnorm1	-0.4233							
Q45Subnorm2								
Q46Subnorm3	-0.5712							
Q47Subnorm4								
Q49PercBehCont1								
Q50PercBehCont2	-0.6449							
Q51PercBehCont3								
Q52Desire1	-0.5234							
Q53Desire2	-0.5292							
Q54CostBenefits1	-0.6151							
Q55CostBenefits2	-0.4990							
Q56CostBenefits3	-0.5454							
Q57FacCon1								
Q58FacCon2								
Q59FacCon3								
Q60FacCon4								
Q61FacCon5								
Q62Affect1	0.7398							
Q63Affect2	0.6698							
Q64Affect3	-0.7604							
Q65Affect4	0.7658							
Q66Roles1	0.7551							
Q67Roles2	0.7529							
Q68Roles3	0.7294							
Q69SelfCon1	-0.7164							
Q70SelfCon2	0.7460							
Q71SelfCon3	0.8250							
Q72NeutCondB	0.5133							
Q73SocialFact1								
Q75SocialFact2								
Q76SocialFact3								

Table D1. Results from Exploratory Factor Analysis of All Items from Study 1 (Continued)

Item	Factor1		Factor3	Factor4	Factor5	Factor6	Factor7	Factor8
Q77NeutLoyB	0.6585							
Q78NeutLedgC	0.6479							
Q79NeutInjA	0.6106							
Q80NeutInjB	0.6340							
Q81ShameSevC	-0.4544							
Q82ShameCertA	-0.5447							
Q83MoralA	-0.7466							
Q84FormSevA								
Q85FormCertC					0.6566			
Q86NeutNecB		0.6143						
Q87InformCertB					0.6754			
Q88InformSevA							0.4720	
Q89NeutRespB		0.5273						
Q90NeutLedgA		0.6037						
Q91NeutRespA								
Q92FormCertA					0.7821			
Q93ShameSevA					0.4172		0.6880	
Q94InformSevC							0.7212	
Q95MoralB		0.4760						
Q96ShameCertB							0.6560	
Q97FormSevC							0.6207	
Q98NeutCondC		0.6988						
Q99InformCertC					0.6925			
Q100NeutLoyC		0.6546						
Q101InformSevB							0.7309	
Q102NeutCondA		0.6734						
Q103InformCertA					0.6375		0.4147	
Q104NeutLedgB		0.6670						
Q105MoralC		-0.4122						
Q106NeutNecC		0.6433						
Q107ShameSevB							0.7717	
Q108NeutInjC		0.8300						
Q109FormCertB					0.8468			
Q110NeutLoyA		0.8097						
Q111FormSevB					0.7893			
Q112NeutNecA		0.7179						
Q113ShameCertC					0.4027		0.6931	
Q114Fear2					0.4844			
Q115Fear3		0.5360						
Q116Fear4								
Q117Fear5		0.4509						
Q118Fear6								

Table D1. Results from Exploratory Factor Analysis of All Items from Study 1 (Continued)

Item	Factor1		Factor3	Factor4	Factor5	Factor6	Factor7	Factor8
Q119Fear7								0.7379
Q120Fear8								
Q121Fear9		0.5360						
Q122Fear10								0.9334
Q123Fear11								0.8710
Q124aDefenceAvoid1								
Q124bDefenceAvoid2								
Q125aReactance1								
Q125bReactance2								
Q125cReactance3		0.4631						
Q125dReactance4		0.4689						
Q126NeutRespC		0.4237						

Note: All factor loadings < |.40| have been suppressed from the output.

Table D1. Results from Exploratory Factor Analysis of All Items from Study 1 (Continued)

Item	Factor 9	Factor10	Factor1 1	Factor1 2	Factor1 3	Factor1 4	Factor1 5	Factor1 6
Q1Intent								
Q2Intent								
Q3Sever1								
Q4Sever2								
Q5Sever3								
Q6Vulner1								
Q7Vulner2								
Q8Vulner3								
Q9RespEffi1								0.7268
Q10RespEffi2								0.7657
Q11RespEffi3				0.9469				
Q12RespEffi4				0.7751				
Q13SelfEffi1								
Q14SelfEffi5							0.9860	
Q15SelfEffi2							0.6517	
Q16SelfEffi3								
Q17SelfEffi4								
Q18Responsecost1								
Q19Responsecost2								
Q20Responsecost4								
Q21Responsecost5								
Q22Rewards/Costs1								
Q23Rewards/Costs2								

Table D1. Results from Exploratory Factor Analysis of All Items from Study 1 (Continued)

Item	Factor 9	Factor10	Factor11	Factor12	Factor13	Factor14	Factor15	Factor16
Q24Rewards/Costs3								
Q25Rewards1								
Q26Rewards2								
Q27Rewards3								
Q29Rewards4								
Q31Habit1								
Q32Habit10								
Q33Habit11								
Q34Habit12								
Q35Habit2								
Q36Habit3								
Q37Habit4								
Q38Habit5								
Q39Habit6								
Q40Habit7								
Q41Habit8								
Q42Habit9								
Q43Atti1		0.4259						
Q43Atti2		0.4982						
Q43Atti3		0.6877						
Q43Atti4		0.7946						
Q44Subnorm1			0.4826					
Q45Subnorm2			0.4202					
Q46Subnorm3								
Q47Subnorm4			0.4830					
Q49PerchBehCont1								
Q50PerchBehCont2								
Q51PerchBehCont3								
Q52Desire1								
Q53Desire2								
Q54CostBenefits1			0.4058					
Q55CostBenefits2			0.4840					
Q56CostBenefits3			0.4611					
Q57FacCon1								
Q58FacCon2	-0.6061							
Q59FacCon3	0.8458							
Q60FacCon4	0.8822							
Q61FacCon5	-0.4555							
Q62Affect1								
Q63Affect2								
Q64Affect3								
Q65Affect4								

Table D1. Results from Exploratory Factor Analysis of All Items from Study 1 (Continued)

Item	Factor 9	Factor10	Factor11	Factor12	Factor13	Factor14	Factor15	Factor16
Q66Roles1								
Q67Roles2								
Q68Roles3								
Q69SelfCon1								
Q70SelfCon2								
Q71SelfCon3								
Q72NeutCondB								
Q73SocialFact1								
Q75SocialFact2								
Q76SocialFact3								
Q77NeutLoyB								
Q78NeutLedgC								
Q79NeutInjA								
Q80NeutInjB								
Q81ShameSevC					0.6755			
Q82ShameCertA					0.6273			
Q83MoralA								
Q84FormSevA								
Q85FormCertC								
Q86NeutNecB								
Q87InformCertB								
Q88InformSevA								
Q89NeutRespB								
Q90NeutLedgA								
Q91NeutRespA								
Q92FormCertA								
Q93ShameSevA								
Q94InformSevC								
Q95MoralB								
Q96ShameCeertB								
Q97FormSevC								
Q98NeutCondC								
Q99InformCertC								
Q100NeutLoyC								
Q101InformSevB								
Q102NeutCondA								
Q103InformCertA								
Q104NeutLedgB								
Q105MoralC								
Q106NeutNecC								
Q107ShameSevB								
Q108NeutInjC								

Table D1. Results from Exploratory Factor Analysis of All Items from Study 1 (Continued)

Item	Factor 9	Factor10	Factor11	Factor12	Factor13	Factor14	Factor15	Factor16
Q110NeutLoyA								
Q111FormSevB								
Q112NeutNecA								
Q113ShameCertC								
Q114Fear2								
Q115Fear3								
Q116Fear4								
Q117Fear5								
Q118Fear6								
Q119Fear7								
Q120Fear8								
Q121Fear9								
Q122Fear10								
Q123Fear11								
Q124_aDefenceAvoid1								
Q124_bDefenceAvoid2								
Q125aReactance1								
Q125bReactance2								
Q125cReactance3						0.7595		
Q125dReactance4						0.7908		
Q126NeutReespC								

Appendix E

Validation and Analysis Details for UMISPC

Table E1 summarizes the model validation of the measurement model for UMISPC. All item loadings were significant at the $p < .0001$ level. Table E2 summarizes further validation procedures for this model. Namely, it verifies that the data fit, based on X^2, of the measurement model is improved by moving to the theoretical model. We also verify that the fitted model is more fit to the data than the saturated model of UMISPC, which provides assurance of no misspecification errors and indicates that our model is not lacking any relationships or constructs. Finally, comparing the model fit with a model that has all items loaded on to one latent construct in order to test for the common method bias shows a strong lack of support for that bias, indicating that method bias is not likely present in our sample.

Table E1. Item Loadings for UMISPC Validation

Identified Factor	Item	Loading
Social factors	roles2	.857
	roles3	.784
	moral1	.812
	affect1	.911
	affect4	.786
	selfcon1	.889
	selfcon2	.752
	selfcon3	.833
	percbehcont2	.866
Punishment	formalcert1	.755
	formalcert2	.959
	formalcert3	.796
	formalsev2	.904
	informalcert1	.781
	informalcert2	.753
	informalcert3	.743
Rewards/Costs	respcost1	.858
	respcost2	.818
	respcost4	.780
	respcost5	.892
	reward1	.881
	reward3	.700
	reward4	.701
Habit	habit1	.785
	habit2	.800
	habit3	.762
	habit5	.849
	habit7	.799
	habit8	.783
	habit11	.862
	habit12	.847
Neutralization	neutcond3	.791
	neutloyal1	.916
	neutinjury3	.811

Table E1. Item Loadings for UMISPC Validation

Identified Factor	Item	Loading
Threat	vulner1	.884
	vulner2	.894
	vulner3	.908
	sever3	.854
Fear	fear7	.858
	fear10	.969
	fear11	.943
Response efficacy	respeff2	.836
	respeff3	.861
	respeff4	.861
Facilitating conditions	facicond3	.798
	facicond4	.859
Reactance	react3	.842
	react4	.994
Intention	intent1	.958
	intent2	.982

Table E2. Item Loadings for UMISPC Validation

Measurement Model	Single Latent Factor Model (CM Bias Model)	Theoretical Model	Fully Saturated Model
2524.99	6594.95	1665.91	1985.50

Appendix F

Strengths and Weaknesses of Different Measurement Approaches

These approaches have different strengths and potential weaknesses regarding *specifying violation type*, *allowing capturing context*, *intimidation concern*, *capturing current behavior*, and *capturing future intention* (Table 3). Besides the fact that both can be used to specify the type of violation (or insecure act), the scenario approach allows presentation of the context. The scenario approach presents a scenario that describes a case and context where the scenario character typically violates a law, norm, or policy (Pogarsky 2004; Siponen and Vance 2010). Describing the context is difficult, if not impossible, with typical survey statements capturing actual behavior like "I select an easy-to-break password" or "I lock my computer." Including context can have two benefits. First, it puts respondents in a specific situation where the insecure act is committed (Pogarsky 2004). Besides specifying and clarifying the situation, this is believed to have the potential to increase realism (D'Arcy et al. 2009; Hu et al. 2011; Pogarsky 2004). Second, one can vary the contextual information in the scenario (Siponen and Vance 2014). Importantly, context can explain the results, too (Dudwick et al. 2006). Scenarios allow examination of the extent to which the model (or its independent variables) holds for different IS security violation types when the contexts of the violations are different. If the model can explain the different violation types (or insecure acts), but the relationships are also significant with different context descriptions, then this provides further evidence that the model is applicable in explaining various insecure acts and that the contexts do not explain the results.

The behavior statement approach is a good choice if there is a theoretical reason to avoid any contextual information. For example, let us assume that scholars used the scenario approach and the same model and received different results for different scenarios, and it is believed that the context could explain the results. Then, one could try avoiding the entire context and including behavior questions such as "I lock my computer" and so on. This could help to determine if the context characteristics, rather than the different insecure types, influence the different results. We did not have this concern and we preferred to have a context to increase realism and to see if the results hold with the different scenarios (with different contexts) (Siponen and Vance 2014).

Intimidation concern is another reason to use scenarios in our case. When it comes to self-report studies, the scenario approach has been reported as the most commonly used technique for examining ethically sensitive acts in business ethics (O'Fallon and Butterfield 2005) and illegal acts in criminology (Pogarsky 2004). In these fields, it is believed that in the scenario setting, respondents are in a less threatened position to admit such an act, because scenarios describe third-person behavior (Trevino 1992; Pogarsky 2004). Fisher (1993) reports that indirect questioning reduces social desirability bias, compared with questions that ask the persons to report their own current behavior. A number of IS security scholars note the decreased intimation concern as a key reason for using the scenario approach (Barlow et al. 2013; D'Arcy et al. 2009; Guo et al. 2011; Hu et al. 2011; Siponen and Vance 2010).

The last issue is *capturing current behavior* versus *capturing prospective behavior intention*. The behavior approach captures current or retrospective self-reported behavior, while the scenario approach captures prospective self-reporting behavior (Pogarsky 2004) (Table 3). The self-report behavior captures current behavior or retrospective behavior without giving context (Pogarsky 2004). The scenario approach poses subjects with a hypothetical situation, followed by a question asking the likelihood that they would behave in the same way under similar circumstances (Paternoster and Simpson 1996; Pogarsky 2004). Therefore, scenario-based self-report captures "the prospective behavior" intention (Pogarsky 2004). The weakness of self-reported current or retrospective behavior is the link between current and future behavior, because it provides no evidence of future behavior (Pogarsky 2004). Similarly, the concern in prospective scenario-based measures is whether "how individuals intend to behave" in future translates to actual future behavior (Pogarsky 2004 p. 114). Available evidence suggests that self-reported scenario responses to projected rule violations correspond to actual rule violations in the future (Pogarsky 2004). Rogers (1983) notes that "protection motivation is best measured by behavioral intention" (p. 172). This makes sense if the focus is on prospective behavior.

References

Abraham, C. S., Sheeran, P., Abrams, D., and Spears, R. 1994. "Exploring Teenagers' Adaptive and Maladaptive Thinking in Relation to the Threat of HIV Infection," *Psychology & Health*, (9:4), pp. 253-272.

Ajzen, I. 2002. "Residual Effects of Past on Later Behavior: Habituation and Reasoned Action Perspectives," *Personality and Social Psychology Review* (6:2), pp. 107-122.

Bamberg, S., and Schmidt, P. 2003. "Incentives, Morality, or Habit? Predicting Students' Car Use for University Routes with the Models of Ajzen, Schwartz, and Triandis," *Environment and Behavior* (35:2), pp. 264-285.

Barlow, J., Warkentin, M., Ormond, D., and Dennis, A. 2013. "Don't Make Excuses! Discouraging Neutralization to Reduce IT Policy Violation," *Computers & Security* (39:Part B), pp. 145-159.

Bergeron, F., Raymond, L., Rivard, S., Gara, M.-F. 1995. "Determinants of EIS Use: Testing a Behavioral Model," *Decision Support Systems* (14:2), pp. 131-146.

Curry, T. R. 2005. "Integrating Motivating and Constraining Forces in Deviance Causation: A Test of Causal Chain Hypotheses in Control Balance Theory," *Deviant Behavior* (26:6), pp. 571-599.

D'Arcy, J., Hovav, A., and Galletta, D. F. 2009. "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (23:1), pp. 79-98.

Dudwick, N., Kuehnast, K., Jones, V. N., and Woolcock, M. 2006. "Analyzing Social Capital in Context: A Guide to Using Qualitative Methods and Data," Stock No. 37260, The International Bank for Reconstruction and Development, The World Bank, Washington, DC.

Fisher, R. J. 1993. "Social Desirability Bias and the Validity of Indirect Questioning. Journal of Consumer Research, 20(2): 303-315.

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.

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

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.

Kanfer, R., and Ackerman, P. L. 1989. "Motivation and Cognitive Abilities: An Integrative/Aptitude-Treatment Interaction Approach to Skill Acquisition," *Journal of Applied Psychology* (74:4), pp. 657-690.

Limayem, M., and Hirt, S. G. 2003. "Force of Habit and Information Systems Usage: Theory and Initial Validation," *Journal of the Association for Information Systems* (4:1), pp. 65-97.

Gagnon, M.-P., Godin, G., Gane, C., Fortin, J.-P., Lamothe, L., Reinharz, D., and Cloutier, A. 2003. "An Adaptation of the Theory of Interpersonal Behavior to the Study of Telemedicine Adoption by Physicians," *International Journal of Medical Informatics* (71:2-3), pp. 103-115.

McClenahan, C., Shevlin, M., Adamson, G., Bennett, C., and O'Neill, B. 2007. "Testicular Self-Examination: A Test of the Health Belief Model and the Theory of Planned Behavior," *Health Education Research* (22:2), pp. 272-284.

Milne, S., Sheeran, P., and 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), pp. 106-143.

O'Fallon, M., and Butterfield, K. 2005. "A Review of the Empirical Ethical Decision-Making Literature: 1996–2003," *Journal of Business Ethics* (59:4), pp. 375-413.

Osman, A., Barrios, F. X., Osman, J. R., Schneekloth, R., and Troutman, J. A. 1994. "The Pain Anxiety Symptoms Scale: Psychometric Properties in a Community Sample," *Journal of Behavioral Medicine* (17:5), pp. 511-522.

Paternoster, R., and Simpson, S. 1996. "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime," *Law & Society Review* (30:3), pp. 549-584.

Piquero, N. L., and Piquero, A. R. 2006. "Control Balance and Exploitative Corporate Crime," *Criminology* (44:2), pp. 397-430.

Pogarsky, G. 2004. "Projected Offending and Implications for Heterotypic Continuity," *Criminology* (42:1), pp. 111-135.

Rogers, R. W. 1983. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation," in *Social Psychophysiology*, J. Cacioppo and R. E. Petty (eds.), New York: Guilford, pp. 153-176.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-502.

Siponen, M., and 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), pp. 289-305.

Tittle, C. R. 1995. *Control Balance: Toward a General Theory of Deviance*, Boulder, CO: Westview Press.

Tittle, C. R. 1997. "Thoughts Stimulated by Braithwaite's Analysis of Control Balance Theory," *Theoretical Criminology* (1:1), pp. 99-110.

Trevino, L. K. 1992. "Experimental Approaches to Studying Ethical–Unethical Behavior in Organizations," *Business Ethics Quarterly* (2:2), pp. 121-136.

Triandis, H. 1977. *Interpersonal Behavior*, Pacific Grove, CA: Brooks/Cole Publishing Company.

Vance, T., and Siponen, M. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-502.

Vance, T., and Siponen, M. 2012. "IS Security Policy Violations: A Rational Choice Perspective," *Journal of Organizational and End User Computing* (24:1), pp. 21-41.

Verplanken, B., and Orbell, S. 2003. "Reflections on Past Behavior: A Self-Report Index of Habit Strength," *Journal of Applied Social Psychology* (33:6), pp. 1313-1330.

Witte, K., Cameron, K. A., McKeon, J. K., and Berkowitz, J. M. 1996. "Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale," *Journal of Health Communications* (1:4), pp. 317-341.

Woon, I. M. Y., Tan, G.-W., and Low, R. 2005. "A Protection Motivation Theory Approach to Home Wireless Security," in *Proceedings of the 26th International Conference on Information Systems*, D. Avison, D. Galletta, and J. I. DeGross (eds.), Las Vegas, NV, December 11-14, pp. 367-380.