European Journal of Information Systems (2016) 25, 231–251

www.palgrave-journals.com/ejis/

EMPIRICAL RESEARCH

Dispositional and situational factors: influences on information security policy violations

Allen C. Johnston[1], Merrill Warkentin[2], Maranda McBride[3] and Lemuria Carter[4]

[1]Department of Management, Information Systems, and Quantitative Methods, School of Business, University of Alabama at Birmingham, Birmingham, U.S.A.; [2]Department of Management and Information Systems, College of Business, Mississippi State University, Mississippi State, MS, U.S.A.; [3]Department of Management, North Carolina A&T State University, Greensboro, U.S.A.; [4]Department of Information Systems, Virginia Commonwealth University, Richmond, U.S.A.

Correspondence: Merrill Warkentin, Department of Management and Information Systems, College of Business, Mississippi State University, 302 McCool Hall, P.O. Box 9581, Mississippi State, MS 39762, U.S.A.
Tel: +(662) 325-1955;
Fax: +(662) 325-8651;
E-mail: m.warkentin@msstate.edu

Received: 18 April 2013
Revised: 30 August 2015
Accepted: 06 September 2015

Abstract
Insiders represent a major threat to the security of an organization's information resources. Previous research has explored the role of dispositional and situational factors in promoting compliant behavior, but these factors have not been studied together. In this study, we use a scenario-based factorial survey approach to identify key dispositional and situational factors that lead to information security policy violation intentions. We obtained 317 observations from a diverse sample of insiders. The results of a general linear mixed model indicate that dispositional factors (particularly two personality meta-traits, Stability and Plasticity) serve as moderators of the relationships between perceptions derived from situational factors and intentions to violate information security policy. This study represents the first information security study to identify the existence of these two meta-traits and their influence on information security policy violation intentions. More importantly, this study provides new knowledge of how insiders translate perceptions into intentions based on their unique personality trait mix.
European Journal of Information Systems (2016) **25**(3), 231–251.
doi:10.1057/ejis.2015.15; published online 23 February 2016

Keywords: information security policy violation; protection motivation theory; general deterrence theory; Big Five personality traits; meta-traits; factorial survey method

Introduction

Employee violations of organizational information security policies, whether intentional or unintentional, are frequently identified as the greatest single threat to organizational information security (Boss *et al*, 2009; Warkentin & Willison, 2009). Indeed, employees are typically called the 'weakest link' in the security environment, as they will often fail to perform specified security behaviors because of an insufficient awareness of policies, low self-efficacy, or carelessness (Hsu *et al*, forthcoming). Recent industry reports (Emm, 2013; Ernst & Young, 2013; Ponemon Institute, 2013; Verizon, 2015) confirm academic research findings, (Warkentin & Willison, 2009) which indicate that insider violations of information security policies continue to be a concern for organizations, especially in contexts in which disgruntled workers engage in various improper acts (Willison & Warkentin, 2013). Technical controls do not effectively prevent motivated insiders from violating information security policies. Thus, organizations employ a range of behavioral controls, including protection motivation appeals or 'fear appeals' (Johnston & Warkentin, 2010; Johnston *et al*, 2015) and sanctions (D'Arcy *et al*, 2009). Furthermore, research indicates that individual differences, such as personality traits, may influence certain insider behaviors (Kajzer *et al*, 2014; Shropshire *et al*, 2015).

When facing decisions about information security, insiders have been shown to behave in response to (1) various perceptions (such as perceptions

of threat and efficacy) and to (2) various extrinsic influences (such as deterrence and fear appeals). The process by which insiders evaluate these factors is, in turn, influenced by the insiders' dispositions and by various situational factors within the environment. Dispositional factors are distinct characteristics that comprise the 'make-up' of each individual and shape his/her core values and beliefs (Hofstede, 1991; Earley *et al*, 1999). These factors, which are relatively stable over time, include personality, propensity to trust, cognitive style, self-esteem, forgetfulness, narcissism, Machiavellianism, psychopathy (Paulhus & Williams, 2002), and other traits. Situational (or contextual) factors, on the other hand, are external – found in the individual's environment – but similarly influence perceptions of external stimuli, including those linked to information security policy compliance (Besnard & Arief, 2004; Workman *et al*, 2008; Lee & Larsen, 2009; Shropshire *et al*, 2015). Situational factors can include policy-compliance-related managerial interventions within an organizational environment and are generally beyond the control of the insider.

Researchers in diverse domains have explored the interactions between dispositional and situational factors (Darley & Batson, 1973; Mischel *et al*, 1973; Wheeler *et al*, 2005); however, information security research has only examined the influence of situational and dispositional factors independently. For example, Kajzer *et al* (2014) found that personality traits impact the effectiveness of security awareness messages. Likewise, Shropshire *et al* (2015) found a link between personality traits and security compliance behaviors. A plethora of information security empirical studies (c.f. Junglas *et al*, 2008; D'Arcy *et al,* 2009; Bulgurcu *et al*, 2010; Johnston & Warkentin, 2010; Johnston *et al,* 2015) have also established the impact of situational factors, such as deterrence measures and fear appeals – yet there has been no scientific investigation of the interaction between dispositional and situational factors in the context of individual responses to security messages, though it has been shown in other domains that dispositional and situational factors interact to influence how an insider will assess and respond in a given information security policy compliance/non-compliance situation.

We assert that the design and administration of situational factors, such as information security communications to insiders (including training protocols and IT-based communications, such as pop-up reminders or electronic 'nudges', Lindqvist, 2012), should be contingent on a set of salient dispositional factors rather than on a 'one-size-fits-all' approach (Wright & Mischel, 1987; Carver & Scheier, 1994; Kammrath *et al*, 2005; Hofmann *et al*, 2008; Warkentin *et al*, 2011; McBride *et al*, 2012). Understanding the interaction between situational and dispositional factors can assist managers in developing controls tailored to particular employee groups to minimize information security policy violations and maximize compliance. Though dispositions, such as personality traits, cannot be easily altered through traditional interventions (situational factors), they can be used to establish empirically tested alternative interventions. By understanding how personality traits influence the downstream impact of security interventions on policy violation intentions, we can tailor these interventions further, establishing, for example, guidelines for designing various information security communications or pop-up reminders. Information security interventions developed using these guidelines can be customized to meet the unique needs of diverse types of insiders and will thus be more effective at influencing their behavior. Our research is designed to provide this knowledge, which can then be used to establish a foundation for the development of customized information security interventions.

In this study, we examined the effects of the interaction between personality traits (which are important dispositional factors) and perceptions of fear appeals and sanctions (two frequently studied situational factors), using a factorial experimental design. Our goal was to identify how one particular set of dispositional factors, namely personality traits, influences the efficacy of various situational factors that are applied in the workplace to influence insider-security-related behaviors. This is an unexplored space in the cognitive progression from situational factor exposure to the intention to violate information security policy, but it is important for understanding, for example, how two people with similar perspectives regarding threat severity and sanction certainty could arrive at different intentions to violate security policy. Previous research has examined the impact of personality traits on individuals' interpretations of situational factors – for example, personal appraisals of communicated threats, coping strategies, sanction severity, and sanction certainty (Self & Rogers, 1990; Janis & Feshbach, 2006; Johnston & Warkentin, 2010; Kajzer *et al*, 2014; Johnston *et al*, 2015). We do not know, however, how personality traits influence the translation of these interpretations and meanings into information security policy compliance or non-compliance intentions. To this extent, we are interested in answering the following question: How do personality traits influence how perspectives, formed from information security interventions, translate to information security policy violation intentions?

The remainder of this paper is organized as follows. The next section provides an overview of the background literature, the research model, and the hypotheses. The following section includes a detailed discussion of our research methodology. Thereafter follows an overview of the data analysis and results, the limitations of the study, and a discussion of the implications for research and practice. Finally, the last section provides a conclusion that synthesizes our findings.

Background literature, research model, and hypotheses

Recent research, found largely within the Information Systems (IS) research community and supported by

theories found in social psychology, criminology, and other related disciplines, has identified a number of factors that influence individuals to either comply with information security policies or violate them. Many of these factors can be classified as either dispositional or situational, with the majority of the factors regarded as perceptions derived from the influence of situational factors, such as warnings about threats or sanctions for non-compliance. For example, in a recent study involving remote insiders of an organization, perceptions of vicarious experience and verbal support derived from social learning situational factors were found to shape insider perceptions of information security policy awareness (Johnston *et al*, 2013). Situational factors, such as social cues from employers and co-workers, were also shown by Warkentin *et al* (2011) to positively influence insider compliance with security and privacy policies. The relationships between these situational factors and the perceptions derived from policy awareness were predicted using social cognitive theory (Bandura, 1977). Other situational factors, such as persuasive messages (Johnston & Warkentin, 2010; Johnston *et al*, 2015) have also been used to invoke perceptions so as to motivate compliance with information security practices, with the latter leveraging protection motivation theory as a theoretical foundation for predicting reactions to the messages.

Various dispositional factors have also been shown to influence security outcomes. However, the research on how dispositional factors interact with situational factors to influence intentions to violate information security policy is limited. On the basis of the extant literature regarding situational and dispositional factors and their influence on violation intentions, we can only speculate as to how these forces may interact to influence violations of information security policy compliance. However, by applying the personality trait theory to this problem, we can begin to understand this interaction.

Extant literature establishes a link between the Big Five personality traits and information security compliance behaviors (Shropshire *et al*, 2015). However, few studies to date have explored the role of all of the Big Five personality traits in the context of information security (Major *et al*, 2006; Shropshire *et al*, 2015) and how these traits may form higher-order groups and interact with situational factors. While situational and dispositional factors are each likely to influence behaviors, such as violations of information security policies, independently of one another, we posit that individuals with certain dispositions are more or less likely to engage in specific risky behaviors based on the circumstances they face (Warkentin *et al*, 2011). Mischel (1968) provided support for this belief when he concluded 'it is evident that the behaviors which are often construed as stable personality trait indicators actually are highly specific and depend on the details of the evoking situations and the response mode employed to measure them' (p. 37). For this reason, the moderating effects of personality meta-traits on the influence of situational factors on policy violation intentions should be explored. Hirsh *et al* (2009) use neuropharmacological trait theory to explore Big Five personality meta-traits, stating that 'not only were the metatraits able to predict behavioral outcomes above and beyond the Big Five, but the hypothesized pattern of negative and positive correlations was also more pronounced at the metatrait level' (p. 1098). Although information security research acknowledges the importance of individual personality traits, few studies have examined the role of meta-traits in this context. Examining the role of meta-traits presents an opportunity for information security researchers and practitioners to develop a more comprehensive understanding of this phenomenon.

In the following subsections, we describe situational and dispositional factors in greater detail and describe the interaction that occurs between these factors that leads to the development of intentions to commit information security policy violations. Individuals respond differently to situational factors (security interventions), forming unique response intentions. Our contention is that personality meta-traits are key to these unique responses and that differentiation can occur *after* situational factor perspectives are derived. In this research, we observed these relationships and interactions and how they shape insider intentions to violate information security policy. Figure 1 depicts this nomological net: the observations involved in this research are denoted with solid lines, and the dashed lines represent informational pathways that are not a part of the current research, but are an important aspect of continuous security intervention design and influence monitoring.

Situational factors

In terms of influencing individual insider behavior, organizations utilize several forms of information security interventions. Two commonly studied situational factors are sanctions and persuasive communications. One powerful tool is the application of formal organizational sanctions – official punishment for non-compliance with information security policies (D'Arcy *et al*, 2009) – as well as informal sanctions, such as personal demonstrations of displeasure or disappointment by others, which may lead to feelings of guilt or shame in the offender. Grounded in deterrence theory, the use of such organizational sanctions relies on the belief that potential offenders are less likely to form rational behavioral intentions to violate social norms or formal rules if they perceive the sanctions to be more severe, more certain, or more swift (Hoffer & Straub, 1989). Persuasive communications, the other main category of situational factors, are designed to influence insiders to adopt secure behaviors that are compliant with organizational polices. These include security training, messages, reminders, electronic 'nudges' (Lindqvist, 2012), and so-called 'fear appeals' (Johnston & Warkentin, 2010; Johnston *et al*, 2015), which are the most studied form of persuasion in IS literature. Both forms of situational factors, along with some of their respective derived perceptions, are represented in Table 1.

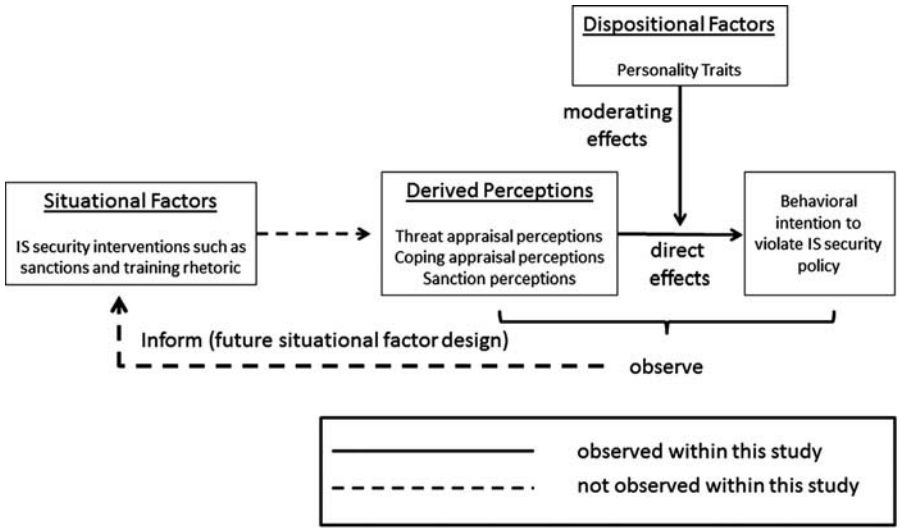

Figure 1 Conceptual model.

Table 1 Situational factors and associated derived perceptions

Situational factor	*Derived perception*	*Definition*
Sanctions	Sanction severity	Perceived harshness of the punishment associated with violating information security policy
	Sanction certainty	Perceived likelihood of being punished if the information security policy is violated
Fear appeals	Threat vulnerability	Perceived likelihood of something negative occurring if the information security policy is violated
	Threat severity	Perceived seriousness of the risk associated with violating IS security policy
	Self-efficacy	Perceived confidence in the ability to comply with information security policy
	Response efficacy	Perceived effectiveness of information security policy
	Response costs	Perceived negative consequences associated with complying with information security policy

Sanctions represent a relatively common situational factor used to generate insider perceptions that align favorably with information security policy prescriptions (Boss *et al*, 2009; D'Arcy *et al*, 2009; Herath & Rao, 2009). Deterrence theory (Akers, 1990; Ehrlich, 1996) suggests that individuals will be discouraged from performing undesirable behavior (e.g., crime, computer abuse, policy violation) if they perceive that there will be punishments or sanctions that are certain and severe. The effective application of deterrence controls presumes that individuals consider the benefits of a policy violation (e.g., convenience of temporarily leaving a workstation without logging off, selecting a weak password that is easy to remember, Zhang *et al*, 2009, avoiding proper patch management, or breaking into a database to steal valuable information) and the costs of such violations (perceived sanction certainty and severity), and elect to engage in non-compliant or criminal behavior. Policies can inform insiders about sanctions, but individuals will cognitively process that information in unique ways.

Another important situational factor is characterized by the communication of threats to insiders along with the recommended protective behaviors associated with these threats. This class of communication is generally referred to as fear appeals. Protection motivation theory suggests that when individuals perceive that they are more vulnerable to security threats and when the threats are more severe, they are more likely to adopt a recommended response to the threat, as long as the individual perceives a sufficient level of self-efficacy, perceived efficacy in the recommended response, and a limited impact on costs associated with the response (Herath & Rao, 2009; Anderson & Agarwal, 2010; Johnston & Warkentin, 2010; Johnston *et al*, 2015). Recent research examining the influence of fear appeals on security policy compliance intentions reveals mostly consistent outcomes. For example, Johnston & Warkentin (2010) as well as Herath & Rao (2009) provide evidence to support the positive influence of perceived threat severity, self-efficacy, and response efficacy on policy compliance outcomes. Herath and Rao also provide support for the negative influence of response cost on compliance outcomes. Anderson & Agarwal (2010) reinforce the impact of perceived security threats and efficacy on intentions to follow security protocols. Each of these studies provides unique perspectives and representations for a threat and the efficacy elements of a fear appeal, but these are ultimately derived from the earlier works of Floyd *et al* (2000) and Maddux & Rogers (1983), from which we model our understanding.

Dispositional factors

Dispositional factors influence how individuals perceive their environment (Hofstede, 1991; Earley *et al*, 1999) and respond to communication interventions (Burke, 1969; Cheney, 1983; Dutta & Vanacker, 2000). One dispositional factor of particular importance is personality type, which remains relatively stable over a person's lifetime (Conley, 1985; Bidjerano & Dai, 2007). Research has found that certain characteristics of a person's personality are linked to a propensity for risk-taking (Zuckerman & Kuhlman, 2000; Nicholson *et al*, 2005; Soane & Chmiel, 2005). Other studies have found that the personality trait that most significantly affects a person's risk-taking behavior may differ based on the type of risk (Gullone & Moore, 2000). Violating security policy can be considered a form of risk-taking behavior because the violator runs the risk of being caught and/or punished. Though one's personality cannot easily be altered through intervention, it can be used to establish empirically tested insider selection and communication intervention strategies as well as other managerial influences on insider behavior. In other words, if we can establish statistically significant relationships between dispositional factors (such as personality traits) and their influence on how individuals respond to situational factors, we can then develop strategies for customizing various information security interventions to meet the unique needs of diverse information security users within the workplace.

One common set of dispositional factors used in IS literature is the Big Five set of personality traits (Lim & Benbasat, 2000; Swickert *et al*, 2002; Engelberg & Sjöberg, 2004; Buchanan *et al*, 2005; Landers & Lounsbury, 2006; Major *et al*, 2006; Karim *et al*, 2009; Barnett *et al*, 2015; Shropshire *et al*, 2015). The five personality traits are described in Table 2. One of the principal benefits of the Big Five model is its inherent generalizability (Goldberg, 1993; Arthur & Graziano, 1996). The Big Five model is not designed to represent a specific theoretical perspective; instead, it is a parsimonious yet comprehensive classification of terms that allow individuals to describe themselves (John & Srivastava, 1999).

In light of the generalizability of this model, we explored literature from diverse fields – accident prevention, organizational safety, and cognitive development – to support our proposed research model. Initial investigations have established linkages between the Big Five personality traits and information security compliance behaviors (Shropshire *et al*, 2015); for instance, preliminary investigations have established that the traits of conscientiousness and agreeableness may be strongly linked with an individual's intention to comply with information security policies and to adopt protective technologies (Major *et al*, 2006; Shropshire *et al*, 2015). However, to date, few studies have explored the role of all of the Big Five personality traits in the context of information security and how these traits may form higher-order groups and interact with situational factors.

Table 2 Dispositional factors – Big Five personality traits (the 'five factor model')

Personality trait	*Trait description*
Openness to experience	'[People scoring high on the openness scale are] characterized by such attributes as open-mindedness, active imagination, preference for variety, and independence of judgment'
Conscientiousness	'People [scoring] high on the conscientiousness scale tend to distinguish themselves for their trustworthiness and their sense of purposefulness and of responsibility. They tend to be strong-willed, task-focused, and achievement-oriented'
Extraversion	'People [scoring] high on the extraversion scale tend to be sociable and assertive, and they prefer to work with other people'
Agreeableness	'People [scoring] high on the agreeableness scale tend to be tolerant, trusting, accepting, and they value and respect other people's beliefs and conventions'
Neuroticism	'People [scoring] high on the [neuroticism] scale tend to experience such negative feelings as emotional instability, embarrassment, guilt, pessimism, and low self-esteem'

Source: Zhang (2006).

Several scholars have argued for the existence of two higher-order, non-orthogonal factors, or broader personality types, that have emerged from a meaningful pattern of correlations among the Big Five traits (Vecchione *et al*, 2011). Digman (1997) was the first to note the existence of two personality meta-traits combining others, labeling them α and β α reflects the common variance among a cluster of agreeableness, conscientiousness, and emotional stability (opposite of neuroticism) traits, while β reflects the common variance among the trait cluster, and consists of extraversion and openness. Since Digman's initial finding, numerous scholars have supported this higher-order structure (Carroll, 2002; DeYoung, 2006), providing additional evidence for the convergence of the Big Five traits with the two broader meta-traits and multiple interpretations of their meaning. Though several studies have criticized the assumption of stable higher-order traits (Ashton *et al*, 2009) or have argued for alternative hierarchical solutions, such as the Big One (Musek, 2007), the two meta-trait solution from Digman (1997) has persevered and continues to be at the heart of meta-trait research.

Combining the findings from reference disciplines about the role of these meta-traits with the empirical results of information security research, it appears that these meta-traits will impact users' intentions to engage in information security policy compliance or in violation behaviors. Specifically, we believe that the personality traits of openness, conscientiousness, extraversion, agreeableness, and neuroticism will uniquely converge as one or more higher-order meta-traits with moderating influence

on how individuals form intentions to violate information security policies from situational factors. We leveraged the established understanding of personality meta-traits to arrive at the following hypotheses.

H1a: *Agreeableness, conscientiousness, and emotional stability (reverse of neuroticism) will emerge as a significant meta-trait (Stability).*

H1b: *Openness and extraversion will emerge as a significant meta-trait (Plasticity).*

Interaction of dispositional and situational factors

An individual's personality meta-traits are dispositional factors that influence how he/she will interpret the message, and, when juxtaposed with perceptions derived from sanction and/or fear appeal situational factors, these meta-traits will influence how an individual will ultimately respond to the message (Connor-Smith & Flachsbart, 2007). The key to predicting the influence of personality meta-traits on responses to situational factors, however, is in how the meta-traits of individuals are interpreted. Different contexts require different interpretations. The security context is no different in this regard, and translating behaviors from a previous context to the security context is critical to a proper interpretation.

One of the more influential interpretations of the two meta-trait proposition by Digman (1997) was proposed by DeYoung (2006), who referred to α as 'Stability' and determined that the shared variance of agreeableness, conscientiousness, and emotional stability appears to reflect an individual's tendency to be risk averse – perceiving and behaving in a manner that avoids environmental threats that may introduce risk and cause emotional strain. Stability has been linked with threat fixation and the avoidance of experiences that may result in detrimental outcomes (Wilt *et al*, 2011). Ellingson *et al* (2001) and Vecchione *et al* (2011) further contend that persons with high levels of these characteristics are more readily influenced by social or normative pressures. Alessandri & Vecchione (2012) also found this meta-trait to be a significant determinant of job performance, likely the result of the individuals' willingness to conform to rules (DeYoung *et al*, 2002) and avoid strain.

DeYoung (2006) referred to β as 'Plasticity' and determined that persons exhibiting high levels of the unique blend of extraversion and openness are less risk averse and more open to engaging their environment and others in ways that yield potential rewards. Plasticity has been linked with the exploration of opportunities that generate positive outcomes (Wilt *et al*, 2011). Persons exhibiting high levels of these characteristics are inclined to act independently when faced with social or normative pressures (Ellingson *et al*, 2001; DeYoung *et al*, 2002; Vecchione *et al*, 2011) and maintain a sense of adventure in how they live their lives (Wilt *et al*, 2011).

In the context of information security policy compliance, we can extrapolate the findings from the extant meta-trait literature to predict how meta-trait characteristics will influence relationships stemming from perspectives derived from situational factors and intentions to violate information security policies. Because of their tendency to be influenced by social or normative pressures, we can reasonably expect fear appeals and deterrence interventions to have a greater impact on individuals that share characteristics consistent with the Stability meta-trait. The result of these interventions should be a reduced likelihood for policy violations. Persons with personalities closely aligned with the Plasticity meta-trait, however, are more risk-inclined than their Stability counterparts. Because of the more independent nature of these individuals, fear appeals and deterrence interventions are less likely to have the desired impact, and so long as the opportunity for rewards exists, policy violation intentions will be more likely.

We believe that these meta-traits produce distinct moderating effects on the relationships stemming from the situational factors and intentions to violate information security policies. On the basis of this belief, we compared our understanding of personality meta-traits and the expected interaction of these meta-traits with situational factors to arrive at the following two sets of hypotheses.

H2a: *The Stability meta-trait will reduce the effect of threat appraisals on intentions to violate IS security policies.*

H2b: *The Stability meta-trait will reduce the effect of coping appraisals on intentions to violate IS security policies.*

H2c: *The Stability meta-trait will reduce the effect of sanction perceptions on intentions to violate IS security policies.*

H3a: *The Plasticity meta-trait will increase the effect of threat appraisals on intentions to violate IS security policies.*

H3b: *The Plasticity meta-trait will increase the effect of coping appraisals on intentions to violate IS security policies.*

H3c: *The Plasticity meta-trait will increase the effect of sanction perceptions on intentions to violate IS security policies.*

The hypotheses pertaining to the situational and dispositional factors are illustrated in the following research model (Figure 2). As indicated, insider intention to violate information security policies is formed by the interaction of perceptions derived from the situational factors of sanctions and fear appeals and the dispositional factor meta-traits emerging from openness, conscientiousness, extraversion, agreeableness, and neuroticism.

Method

To answer the research questions and to test the subsequent research model posed by our study, we applied a scenario-based factorial survey method (Rossi & Nock, 1982). The factorial survey approach is a variant of the vignette design and, through the use of vignettes (or scenarios), is able to provide contextual detail to decision-

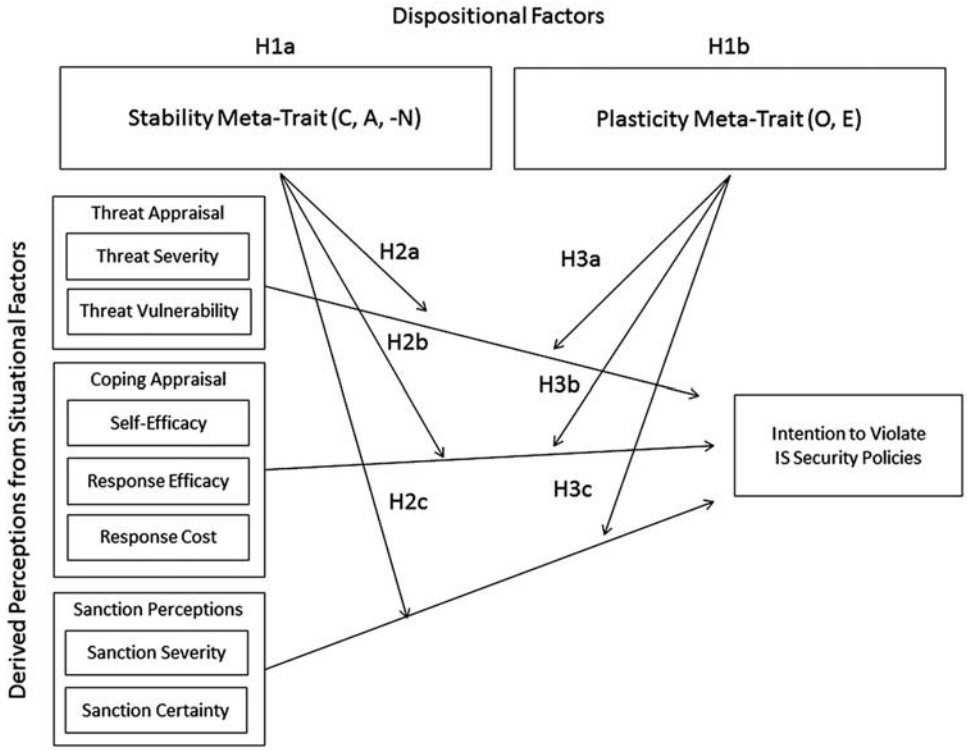

Figure 2 Research model.

making situations and to evenly distribute these details across all participants in the study. By asking participants to read randomly generated vignettes and place themselves in the context of the vignette and in the position of the vignette's primary actor, a reliable and valid measure of perceptions related to the actor's experiences can be obtained and then regressed against dependent outcomes (Jasso, 2006). Used extensively by criminologists, IS researchers, and others exploring deviant behaviors (Barlow *et al*, 2013; Vance *et al*, 2013; Trinkle *et al*, 2014; Vance *et al*, 2015), the factorial survey approach is appropriate for this study, in that it provides a mechanism by which to elicit straightforward responses from participants who might otherwise be subject to social desirability bias (or acquiescence bias), which compels most people to provide socially acceptable answers instead of conceding that they might violate social norms. By placing themselves in the position of fictional vignette characters, the research participants are not reporting personal intentions, but rather how they might respond *if* presented with similar circumstances (Trevino & Victor, 1992). The factorial survey approach is also noted for its ability to reveal the social and individual structures of decision making. Both rationales are important to the successful execution of this study and its ability to fulfill its stated purpose.

Whereas many of these benefits stem from the use of *scenarios*, even when a factorial approach is not pursued, further research rigor is gained from applying the factorial survey approach to data collection. The factorial survey method involves vignette-based experiments in which the participants are presented with one or more versions of a short-story-style vignette. In the vignettes, variable manipulations are embedded within the sentences, which appear in a fixed order and with the sentences relating to the manipulated factors varying randomly across the vignettes (Taylor, 2006), thus 'introducing more realistic complexity' (Lyons, 2008, p. 112). Each vignette was one version of the base scenario, producing a set of scenario versions or types. Developing the individual vignettes in this manner yields 'an almost completely crossed experimental design' (Jasso & Rossi, 1977, p. 642). The random assignment of the factors, which are approximately orthogonal (Rossi & Anderson, 1982; Lyons, 2008), ensures that the levels within the manipulated factors are not correlated with each other, as each has an equal probability of assignment (Shlay *et al*, 2005). Further, the factorial survey method is efficient in that it makes use of statistical sampling to estimate the effect of a factor on a dependent variable without having to test for each combination (Rossi & Anderson, 1982; Jasso, 2006). For our study, six variables were manipulated: self-efficacy, threat vulnerability and severity (combined in one statement), sanction certainty and severity (combined in one statement), and response efficacy.

Sample

We collected the data for this study from an online sample of 242 respondents who met both of the following conditions: (1) have held a job that required the use of a

computer and (2) have held a job where insiders must follow security procedures. The respondents consisted of a group of individuals solicited through a Qualtrics panel selection service (37%), individuals associated with the industry partners of the researchers' academic institutions (44%), and personal contacts of the researchers (19%). Participants were asked to read and respond to the online survey that contained three randomly generated hypothetical vignettes. This should have resulted in 726 observations at the vignette level; however, some respondents did not complete all three vignettes, so the raw dataset included only 595 observations at the vignette level. In terms of the study's participants, 55% were male, with the majority in the 25–34-year age range. Most of the participants had 10–24 years of work experience in diverse industries, with the business services, legal, accounting, and consulting industry, the most popular at 24.8% of the sample. Participant demographic details are shown in Table 3.

Table 3 Survey participants' demographic information

	Percentage
Gender	
Male	55
Female	45
Age	
18–24	5
25–34	41
35–44	26
45–54	19
55 or older	9
Work experience	
Less than 3 years	9
3–9 years	25
10–24 years	40
25 or more years	26
Industry	
Business Services, Legal, Accounting, Consulting, and so on	24.8
Finance, Insurance, and Real Estate	16.8
Manufacturing	14.8
Education	12.1
Health-care Services	8.7
Government – Civilian	6
Information Technology	4
Construction	2
Telecommunications	2
Transportation	1.3
Entertainment	0.7
Electric, Gas, Utilities, and Sanitary Services	0.7
Travel	0.7
Wholesale/Retail	0.7
Other	4.7

Research design and instrumentation

Following a random design factorial survey approach advocated by Rossi & Anderson (1982), we asked each participant to read and respond to an online survey that contained three randomly assigned hypothetical vignettes drawn from a 'vignette universe' of 64 variations of the baseline vignette. Each vignette described a situation in which a company's insider, named Joe, has collected sensitive customer data for his company and wants to take the data home to continue his work. In each vignette, Joe disregards a mandatory password encryption procedure, thus violating an information security policy. We asked respondents to estimate the likelihood or chance that they would duplicate the insider's actions under similar conditions. (See Appendix A for a sample vignette and Appendix B for the constructs manipulated in each vignette version.) After reading each of three randomly assigned vignettes, participants were asked to respond to a series of survey questions, including a four-item manipulation check to ensure that the participant recognized the vignette conditions, a three-item measure of perceived response cost, and a three-item measure of behavioral intention to respond in the same way that Joe did. Also included in the survey, but only asked once of each participant, were demographic items and a 28-item assessment of the Big Five personality traits, which represent the dispositional factors of interest in the present study. (See Appendix C for the Big Five personality traits survey items.)

Dependent variable

As previously mentioned, the dependent variable in this study is the respondent's self-reported intention to violate information security policies (unauthorized removal of sensitive customer information from the workplace, a clear violation of information security policy as described in each vignette). This behavior would be categorized by Guo (2013) as security risk-taking behavior and by Willison & Warkentin (2013) as an internal volitional non-malicious security threat. After reading a vignette in which Joe disregards the security policy and removes the unencrypted information, respondents were asked to estimate the likelihood that they would mirror the insider's actions under similar conditions. The response options ranged on a scale from 1 to 7, with 7 serving as a 'strongly agree' with conducting actions similar to those of Joe. (See Appendix A for elaboration of the instrument's vignette and dependent variable measure.)

Independent variables

A variety of variables served as independent variables associated with the formation of behavioral intention to violate information security policy. The direct determinants of behavioral intention to perpetrate information security policy violations include perceptions of threat severity, threat vulnerability, self-efficacy, response efficacy, response cost, sanction severity, and sanction certainty (see Table 1

for descriptions), derived from the influence of situational factors: sanctions and fear appeals. All of these variables, with the exception of response cost, were randomly manipulated at either high or low levels within each vignette. This represents a Cartesian product of six variables, each with two levels (e.g., threat severity [high/low]×threat vulnerability [high/low]×self-efficacy [high/low]×response efficacy [high/low]×sanction severity [high/low]×sanction certainty [high/low]), resulting in $(2^6) = 64$ unique combinations. Please see Appendix B for the text representing each manipulation (high/low) for each variable.

Pretest

As noted by Piquero *et al* (2000) and, more recently, Siponen &Vance (2010, 2014), vignettes must be designed in such a manner so as to maintain relevance and realism with potential respondents. To ensure realistic vignette design, two controls were embedded into the study. First, as part of the instrument development process before the pilot test, a nine-member panel of experts in research design and instrument development reviewed each vignette and validated the appropriate presence of each independent, dependent, and control variable. The expert review panel also evaluated each generated vignette version to identify unrealistic or logically impossible vignettes for removal from the total universe of potential vignettes. Ultimately, all vignettes were considered realistic and logically possible, maintaining the final universe of vignettes at 64. In addition, the panelists suggested changes to instructions and other wording to improve the clarity of the instrument.

Manipulation check and test for realism

Following each vignette, the participants were also presented with a four-item manipulation check and a three-item realism test. The manipulation check consisted of questions, such as 'How confident was Joe about his ability to complete the password request procedure?' and was intended to ensure that the respondent paid close attention to the important details of the vignette. All four manipulation check questions are shown in Appendix A. The realism questions can also be found in Appendix A (e.g., 'I could imagine a similar vignette taking place at work.'), and were used to assess whether or not the respondent perceived that a vignette such as the one presented could occur in his or her workplace. Manipulation checks and realism items are commonly used in vignette-based research survey instruments that present the participant with hypothetical situations (Keil *et al*, 2000; Barlow *et al*, 2013). If the manipulation checks are not answered correctly, then it can be assumed that the participant did not notice the manipulations within a particular vignette (Sigall & Mills, 1998) and that his or her responses are not based on the appropriate set of vignette conditions. In addition, if the vignette is not considered realistic, then it may be difficult for the participant to imagine him- or herself in that particular situation and provide a rational response to the question.

The results of this study were obtained from those vignettes in which the participants passed both the realism and manipulation checks. Only responses to vignettes in which all four manipulation checks were answered correctly and the mean realism score was 4 or higher were included in the analysis, as these were the responses that were considered valid for this study. From the study, 595 vignette level responses obtained, 230 were removed because of failures in the manipulation checks, and 48 were removed because of low realism ratings, resulting in 317 usable vignette-level observations from 150 different respondents (participants). The absence of the removed low-realism observations on the Big Five personality traits and behavioral intention to violate security policy did not generate significant differences in the means for these variables. These results are provided in Table 5 of the current study. Also, an ANOVA test to determine whether or not the responses from participants who completed the entire survey differed from those that had responses omitted from failing a manipulation check revealed no significant difference in the dependent variable. An *a priori* power analysis (G*Power3 software) determined that a minimum 211 observations would be required to detect an effect size of 0.25 with a power of 0.95 ($\alpha = 0.05$), given the factors and factor levels provided in this study (Faul *et al*, 2007; Faul *et al*, 2009). The 317 usable responses obtained at the vignette level are therefore more than adequate to meet the desired statistical power. Table 4 provides details as to the representation of each manipulated variable within the 317 vignette level observations.

Data analysis and results

Model estimation followed a generalized form of the standard linear model that accounts for both fixed and random effects (McLean *et al*, 1991). This approach was deemed appropriate because each participant was asked to assess multiple vignettes, and there is the possibility for bias in vignette assessments because of unobserved differences in the participants. By using a linear mixed model procedure,

Table 4 Variable representation

Variable	*High/low manipulation count*	*Representation within acquired vignette-level observations (%)*
Threat Severity	169 (high); 148 (low)	high (53.3%); low (46.7%)
Threat Vulnerability	154 (high); 163 (low)	high (48.6%); low (51.4%)
Self-Efficacy	159 (high); 158 (low)	high (50.2%); low (49.8%)
Response Efficacy	165 (high); 152 (low)	high (52.1%); low (47.9%)
Sanction Severity	167 (high); 150 (low)	high (52.7%); low (47.3%)
Sanction Certainty	175 (high); 142 (low)	high (55.2%); low (44.8%)

however, we were able to control for this fixed individual effect. The general linear mixed model process in SPSS (version 19.0.0) is similar to the PROC MIXED procedure in SAS in that it uses maximum likelihood estimates of variances, thereby accounting for correlation within the data because of repeated measures (i.e., each participant rating three vignettes). This is a significant departure from typical least squares analysis, which does not account for such correlation. Therefore, because we obtained maximum likelihood estimates, the individual effects were controlled for, and we were able to obtain accurate variance estimates.

Control variable model tests

Similar to other vignette-based studies, we included several control variables in our study. These control variables included: (1) scenario type (the version seen by the respondent); (2) manipulation check; (3) realism test; (4) participant source; (5) participant gender; (6) participant age; (7) participant experience; and (8) participant employment industry. Each of these control variables were included in an initial control variable model to determine the extent to which they significantly influence behavioral intention to violate an information security policy. This control variable model establishes baseline fit statistics from which our theoretical models need to improve upon to demonstrate predictive power.

Starting with the full set of eight control variables described above and removing those that are not significant determinants of behavioral intention to violate information security policy, a final control variable model was obtained. By removing the non-significant control variables, we were able to obtain a model with optimum fit statistics. Of the full set of eight control variables, only scenario type was significant and included in the final model. The final control variable model is presented in Table 5 and indicates an Akaike's information criterion (AIC) fit statistic of 958.684 and a Schwarz's Bayesian information criterion (BIC) fit statistic of 973.720. For both AIC and BIC, a lower score indicates better model fit – fewer unnecessary variables in the model. Also, because these scores serve as baseline fit statistics, rival theoretical models should provide lower AIC or BIC fit statistics, thereby indicating an improvement upon the control variable model.

Research model tests

Descriptive statistics for the Big Five personality traits and behavioral intention are shown in Table 6. In addition to depicting the mean and standard deviation values for each of these variables, this table also highlights results that suggest that the removal of observations because of low realism ratings did not significantly impact how the participants rated their personality traits or intentions to violate information security policy. In addition, before testing the hypotheses, we conducted preliminary tests to ensure the reliability and validity of the responses. The results of the Variance Inflation Factor (VIF) analysis indicate that mulitcollinearity is not an issue; the VIF for all variables is less than 3.3 (Diamontopoulous & Siguaw, 2006). We also used the Cronbach's α value to assess the reliability of each scale and conducted a principal components analysis to assess the convergent and discriminant validity of the items. The results indicate that the scales were valid and reliable (Bollen & Lennox, 1991).

Table 5 Control variable model

Effect	β	*Standard error/df*	*t-value*
Intercept	2.678	0.135/305	19.873**
Scenario type	2.178	6.185/238	3.523**
Fit statistics: AIC = 1047.472; BIC = 1058.748			

*$P<0.05$; **$P<0.01$.

Tests of meta-trait existence (tests of H1a and H1b) In order to examine the existence of personality meta-traits in information security policy violations, we first analyzed the Big Five personality traits portion of the survey response data using principal axis factoring (Hirsh *et al*, 2009). As indicated in bold in Table 7, the personality traits of Conscientiousness (*C*), Agreeableness (*A*), and Emotional Stability (*–N*: the opposite of Neuroticism) cluster together, forming one meta-trait, while Openness (*O*) and Extraversion (*E*) cluster together as a second meta-trait. As mentioned earlier, these two meta-traits are referred to as Plasticity and Stability, respectively (DeYoung, 2006), and are different aspects of personality that coexist within individuals. However, their existence within the information security policy compliance context is notable and supports H1a and H1b.

Because individual personality traits are unique and not likely to contribute equally to their respective meta-trait, we treated them as formative constructs. Consequently, we created a composite variable for each meta-trait based on a weighted score for each of its individual personality traits. These weighted scores are generated using a structural equation modeling technique known as partial least squares (PLS) regression and indicate the impact of the individual personality traits. In other words, for each meta-trait, we multiplied each of its significant Big Five traits by their PLS weight and added these to form a composite meta-trait value. These values could then be used as independent variables in the moderating influence analyses, which are described next. The version of PLS software used to provide the weighted values for each personality trait was SmartPLS 2.0.3; a depiction of the PLS model used to obtain the PLS weights for each of the Big Five traits on their respective meta-traits is provided in Appendix F.

Tests of meta-trait moderating influence (tests of H2a-H2c and H3a-H3c) With an established control variable model and an understanding of the existence of two meta-traits, we next examined the direct influence of the

Table 6 Descriptive statistics

Factor	*With low realism ratings (N = 365)*		*Without low realism ratings (N = 317)*		*Significance*	
	Mean	*Standard deviation*	*Mean*	*Standard deviation*	*t-value*	*Significance (2-tailed)*
Openness	4.95	0.92	4.85	0.90	0.908	0.531
Conscientiousness	6.05	0.90	5.92	0.63	0.001	0.232
Extraversion	4.78	1.27	4.87	1.02	0.496	0.620
Agreeableness	5.30	1.31	5.50	0.79	1.400	0.162
Neuroticism	3.72	1.28	3.48	1.15	1.226	0.221
behavioral intention	2.25	1.32	2.31	1.27	0.248	0.804

Table 7 Principal axis factoring results

Factor	*Meta-trait 1: stability*	*Meta-trait 2: plasticity*
Openness (*O*)	–0.103	**0.868**
Conscientiousness (*C*)	**0.591**	0.312
Extraversion (*E*)	0.330	**0.742**
Agreeableness (*A*)	**0.746**	–0.083
Emotional stability (–*N*)	**–0.659**	–0.089

Note: Rotation Method: Varimax with Kaiser Normalization.

perspectives derived from the situational factors and meta-traits on intentions to commit an information security policy violation. The results of this analysis are summarized in Table 8 (on the left) and indicate that, of the situational variables, threat vulnerability, sanction severity, and sanction certainty are significant direct antecedents of policy violation intentions. These findings suggest that the average person is significantly more likely to commit a policy violation when threat vulnerability, sanction severity, and sanction certainty are perceived to be low than if they are perceived to be high. These findings also suggest that the Stability and Plasticity meta-traits in themselves are not sufficient predictors of information security policy violation intentions. For this test, the AIC and BIC fit statistics were 949.572 and 998.438, respectively. Using a likelihood ratio test, we compared this model with the control variable model in terms of either AIC or BIC. The likelihood ratio test yields a test statistic that is distributed as a χ^2 distribution. We then calculated a *P*-value as a measure of this statistic relative to its degrees of freedom (Littell *et al*, 1996; Vance *et al*, 2013) and determined that the fit scores were significantly improved ($P<0.001$), thereby providing significantly better predictability than the control variables model (Carte & Russell, 2003).

Examining the moderating effects of the Stability meta-trait (*C, A, –N*), we obtained improved fit statistics (AIC = 911.037; BIC = 953.037). Using a likelihood ratio test to compare these fit statistics with that of the direct influence model (AIC = 949.572; BIC = 998.438), we found a significant difference between the two models ($P<0.001$). These results, summarized in Table 8, suggest that people who exhibit high degrees of this meta-trait differ from the average person in how they consider a policy violation opportunity. These individuals are significantly more sensitive than the average person to threat vulnerability as well as to both the severity and certainty of sanctions, and are more conservative in their responses. The negative coefficient estimates for the interaction of this meta-trait with threat vulnerability, sanction severity, and sanction certainty suggest that people exhibiting high degrees of this meta-trait are significantly less likely than their peers to commit a policy violation when these elements of threat and deterrence are perceived to be low. In other words, while the average person would commit an information security policy violation when threat vulnerability, sanction severity, and sanction certainty were low, a person whose personality favors the Stability characteristics would be significantly less likely to commit a policy violation given similar perceived circumstances. These significant interaction effects are also illustrated in the given figure in Appendix D.

These results were expected (see H2a and H2c), as the literature suggests that these people are risk averse. As discussed in our support for H2a and H2c, Vecchione *et al* (2011) and Ellingson *et al* (2001) contend that persons with these characteristics are more readily influenced by social or normative pressures. In addition, Alessandri & Vecchione (2012) found this meta-trait to be a significant determinant of job performance, likely the result of the willingness of these individuals to conform to rules (DeYoung *et al*, 2002) and avoid strain.

Examining the moderating effects of the Plasticity meta-trait (*O* and *E*), we see that the fit statistics are an improvement to the direct effects model (AIC = 913.234; BIC = 955.234), suggesting a reasonable model for analysis. A likelihood ratio test of the moderating model's fit statistics to that of the direct influence model (AIC = 949.572; BIC = 998.438) confirms a significant improvement ($P<0.001$) in the moderating effects model over the direct effects model. The significant results of this test are provided in Table 8 and suggest that, for people who exhibit the qualities of this meta-trait, how they assess the threat, efficacy, and deterrence elements of a policy violation opportunity is mostly consistent with others. Where they differ, however, is in how they assess response efficacy and sanction certainty. The average person is more likely to commit a crime if the certainty of sanctions is perceived to be low. The efficacy of their response to a perceived threat is immaterial in forming their policy violation intentions. People exhibiting qualities more

Table 8 Meta-trait influence results

Dimension and level	*Stability meta-trait (C, A, –N)*						*Plasticity meta-trait (O, E)*					
	Direct influence model			*Moderating influence model*			*Direct influence model*			*Moderating influence model*		
	β	*Standard error/df*	*t-value*	*β*	*Standard error/df*	*t-value*	*β*	*Standard error/df*	*t-value*	*β*	*Standard error/df*	*t-value*
Scenario type (version)	5.910	1.031/231	0.573 n.s.	9.556	8.633/237	0.111 n.s.	5.910	1.031/231	0.573 n.s.	8.868	6.917/234	1.282 n.s.
Self-efficacy[a]	–0.079	0.133/233	–0.596 n.s.	–1.853	0.814/229	–2.278*	–0.079	0.133/233	–0.596 n.s.	0.281	0.901/230	0.312 n.s.
Response efficacy[b]	0.023	0.100/231	0.234 n.s.	1.161	0.788/226	1.474 n.s.	0.023	0.100/231	0.234 n.s.	–1.279	0.656/229	–1.951 n.s.
Threat severity[c]	0.017	0.104/227	0.160 n.s.	0.508	0.819/237	0.621 n.s.	0.017	0.104/227	0.160 n.s.	0.158	0.668/230	0.237 n.s.
Threat vulnerability[d]	0.279	0.103/223	2.708**	1.211	0.893/253	1.355 n.s.	0.279	0.103/223	2.708**	1.003	0.697/241	1.438 n.s.
Sanction severity[e]	0.545	0.137/237	3.960**	–0.700	0.845/238	–0.829 n.s.	0.545	0.137/237	3.960**	–0.603	0.828/237	–0.729 n.s.
Sanction certainty[f]	0.323	0.140/236	2.304*	1.018	0.794/218	1.281 n.s.	0.323	0.140/236	2.304*	0.050	0.883/233	0.057 n.s.
Response costs	–0.029	0.049/221	–0.596 n.s.	–0.410	0.334/285	–1.226 n.s.	–0.029	0.049/221	–0.596 n.s.	0.203	0.305/276	0.668 n.s.
Stability (*C, A, –N*)	0.281	0.286/152	0.982 n.s.	–0.645	1.127/300	–0.573 n.s.	0.281	0.286/152	0.982 n.s.	0.275	0.286/151	0.963 n.s.
Plasticity (*O, E*)	–0.165	0.161/148	–1.023 n.s.	–0.174	0.159/149	–1.091 n.s.	–0.165	0.161/148	–1.023 n.s.	–0.469	0.677/315	–0.693 n.s.
Stability (*C, A, –N*)*scenario type (version)	—	—	—	2.606	4.259/228	0.612 n.s.	—	—	—	–0.639	0.085/280	–0.750 n.s.
Stability (*C, A, –N*)*self-efficacy[a]	—	—	—	–0.058	0.327/220	–0.180 n.s.	—	—	—	–0.105	0.253/231	–0.414 n.s.
Stability (*C, A, –N*)*response efficacy[b]	—	—	—	0.022	0.042/219	0.525 n.s.	—	—	—	0.363	0.182/228	1.993*
Stability (*C, A, –N*)*threat severity[c]	—	—	—	0.002	0.044/227	0.065 n.s.	—	—	—	–0.336	0.186/231	–0.180 n.s.
Stability (*C, A, –N*)*threat vulnerability[d]	—	—	—	–0.114	0.043/219	–2.648**	—	—	—	–0.194	193/242	–1.001 n.s.
Stability (*C, A, –N*)*sanction severity[e]	—	—	—	–0.241	0.057/235	–4.163**	—	—	—	0.320	0.231/239	1.383 n.s.
Stability (*C, A, –N*)*sanction certainty[f]	—	—	—	–0.135	0.060/236	–2.241*	—	—	—	0.089	0.039/239	2.277*
Stability (*C, A, –N*)*response costs	—	—	—	–0.012	0.021/314	–0.565 n.s.	—	—	—	–0.008	0.013/311	–0.622 n.s.
Intercept	1.781	0.836/183	2.129*	1.906	0.664/149	2.868*	1.781	0.836/183	2.129*	2.761	0.569/148	4.850**
Observations		*N* = 317			*N* = 317			*N* = 317			*N* = 317	
Fit statistics	AIC = 949.572; BIC = 998.438			AIC = 911.037; BIC = 953.037			AIC = 949.572; BIC = 998.438			AIC = 913.234; BIC = 955.234		

[a]Reference level: high self-efficacy.
[b]Reference level: high response efficacy.
[c]Reference level: high threat severity.
[d]Reference level: high threat vulnerability.
[e]Reference level: high sanction severity.
[f]Reference level: high sanction certainty.
*$P<0.05$; **$P<0.01$; n.s. = not significant.

consistent with the Plasticity meta-trait, however, respond differently. If a policy violation could potentially yield rewards, these people are less likely to be deterred and significantly more likely than their peers to follow through with a policy violation, even if they perceive response efficacy and sanction certainty to be high. This finding supports H3b and H3c and is consistent with what some scholars (DeYoung, 2006) have said about people whose personalities are dominant toward this meta-trait – they are less risk averse and more open to engaging in activities that potentially yield rewards. These significant interaction effects are also illustrated in the given figure in Appendix E.

Examining the moderating effects of both meta-traits, Stability (*C, A, –N*) and Plasticity (*O, E*), within the same model, we see that the fit statistics are an improvement to the direct effects model (AIC = 918.225; BIC = 960.004), suggesting a reasonable model for analysis. A likelihood ratio test to compare the moderating model's fit statistics with the direct influence model (AIC = 949.572; BIC = 998.438) confirms a significant improvement ($P<0.01$). For presentation parsimony, only the significant moderating results of this test are provided in Table 9. The results confirm those of the independent meta-trait moderating effect tests, that people who exhibit strong Stability meta-trait characteristics are less likely than the average person to commit an information security policy violation when threat vulnerability, sanction severity, and sanction certainty are low, while people who exhibit strong Plasticity meta-trait characteristics are more likely than the average person to commit an information security violation, even if they perceive high degrees of both response efficacy and sanction certainty.

Discussion

Our study has examined the impact of *dispositional* and *situational* factors on intentions to violate an information security policy. Others have suggested that these factors may not operate in a vacuum, but rather, may interact with each other. However, a search of the literature uncovered no studies that explore this interaction. Hence, using personality traits to represent dispositional factors and using protection motivation and general deterrence factors to represent situational factors, we conducted an exploratory study to assess how information security policy violation intentions are formed from the interaction of dispositional and situational factors. More specifically, we wanted to understand the role that personality traits play in the translation of the perspectives invoked by information security interventions into information security policy violation intentions.

The results of our factorial survey indicate that dispositional and situational factors interact in security settings. In particular, two meta-traits – Stability and Plasticity – were shown to have an impact on one's intention to violate an information security policy. For insiders for whom the Stability meta-trait is the prevailing trait, conscientiousness, agreeableness, and emotional stability (opposite of neuroticism) are dominant. Within the context of information security policy compliance, we find that persons with personalities exhibiting a strong Stability meta-trait are found to be more risk-averse and may avoid actions that place them at risk for threat and sanction-related consequences. From the results of this study, we contend that the reason for this is believed to be tied to their desire to conform with others and with the safety of stable environments. On the other hand, insiders with a strong Plasticity meta-trait are characterized primarily by the dominant openness and extraversion traits. These insiders are more likely to take risks when compared with their peers, but seemingly only in situations in which a clear benefit is possible from the added risk. These important findings demonstrate the efficacy of using personality meta-traits as indicators in the investigation of insider behaviors within the context of information security policy violation.

Contributions to research and theory

Our findings contribute to the theoretical perspective on the important phenomenon of employee violations of

Table 9 Combined stability (*C, A, –N*) and plasticity (*O, E*) moderating influence results

Dimension and level	*Direct influence model*			*Moderating influence model*		
	β	*Standard error/df*	*t-value*	*β*	*Standard error/df*	*t-value*
Stability (*C, A, –N*)*threat vulnerability[a]	—	—	—	–0.112	0.049/219	–2.623**
Stability (*C, A, –N*)*sanction severity[b]	—	—	—	–0.190	0.049/235	–3.066**
Stability (*C, A, –N*)*sanction certainty[c]	—	—	—	–0.117	0.090/236	–2.180*
Plasticity (*O, E*)*response efficacy[d]	—	—	—	0.322	0.180/228	1.962*
Plasticity (*O, E*)*sanction certainty[c]	—	—	—	0.189	0.061/239	2.410*
Intercept	1.781	0.836/183	2.129*	2.730	0.527/148	4.439**
Observations		*N* = 317			*N* = 317	
Fit statistics		AIC = 949.572; BIC = 998.438			AIC = 918.225; BIC = 960.004	

[a]Reference level: high threat vulnerability.
[b]Reference level: high sanction severity.
[c]Reference level: high sanction certainty.
[d]Reference level: high response efficacy.
Note: * $p < 0.05$; ** $p < 0.01$; n.s. = not significant.

information security policies and have several implications for future research. First, ours is the first study to demonstrate the significant influence of personality meta-traits on information security policy violation intentions, opening the door for further investigation into this important insight. The literature describing personality meta-traits is relatively immature, but within the information security literature, it has been non-existent. Kajzer *et al* (2014) and Shropshire *et al* (2015), for instance, established that personality traits are important in terms of how security awareness messages are received and in shaping security compliance behaviors, respectively. But no study to date has moved to the meta-level of examination, a level of study supported within multiple other contexts (Carroll, 2002; DeYoung, 2006). By demonstrating the existence of two higher-order personality type factors, our study increases the preliminary understanding of the role of personality traits in information security and provides the first evidence for personality meta-traits as significant elements of the compliance equation.

Second, this study is the first to interpret meta-traits into the information security context. The literature that has examined the existence and role of personality meta-traits, specifically Digman's (1997) two meta-trait proposition, has elucidated the importance of understanding how the two meta-traits are interpreted within different contexts (Connor-Smith & Flachsbart, 2007). Once we determined the two meta-trait solution was present within the information security policy violation context, the interpretation and labeling of those meta-traits were important components in the process of outcome prediction. This interpretation also establishes the foundation for future research in this context. Future scholarship should continue to explore the role of meta-traits within this context and further refine the interpretations of our research results.

Finally, our results are the first to show how dispositional factors in general, and personality meta-traits in particular, influence the translation of perspectives derived from situational factors into information security policy violation intentions. Previous research has presented several perspectives on how dispositional factors, including personality traits, influence how individuals interpret situational factors – that is, how they receive and process factors such as fear appeals and sanctions (Self & Rogers, 1990; Janis & Feshbach, 2006; Johnston & Warkentin, 2010; Kajzer *et al*, 2014; Johnston *et al*, 2015). This study extends this research by being the first to demonstrate how dispositional factors may influence how these interpretations are ultimately translated into information security policy compliance or non-compliance intentions. Our findings from this study provide rationale for why insiders, when in agreement on the severity of a threat or on the imminence of sanctions, for instance, arrive at different intentions for information security policy violation. Perhaps more importantly, this study sheds light on an underserved area in our search to understand the cognitive progression from perspective development to behavioral action. Future research is still needed, however, to refine this initial understanding.

Contributions to and implications for practice

On the basis of our findings, we posit that customized information security interventions (situational factors) may be more effective at preventing security policy violations than generic interventions. An organization that does not provide a nuanced approach to information security is less likely to achieve its goal of insider compliance with information security policies. Customization of information security interventions should be based on the profiles of the two meta-traits determined by this research (i.e., Plasticity and Stability) to influence information security policy violation intentions (see Figure 1). For example, the results of our research study indicate that response efficacy and sanction certainty, even when perceived to be at high levels, may not effectively deter policy violation intentions by insiders with strong Plasticity tendencies. Therefore, to appeal to these insiders, fear appeals should emphasize the threat elements, and sanction interventions should focus primarily on the sanction severity rhetoric. Because insiders who exhibit high degrees of the Stability meta-trait are more likely to avoid risk overall, information security interventions directed at them can focus less on the severity of sanctions and more on the vulnerability to threats and the certainty of sanctions. More broadly, our work confirms and extends the premise that 'one size does *not* fit all' when it comes to communicating arguments for information security policy compliance to insiders. Employers are advised to leverage individual differences, including personality types, when tailoring persuasive messages to their staff. However, the organizational justice literature regarding security contexts (Willison & Warkentin, 2009; Posey *et al*, 2011; Warkentin *et al*, 2011) indicates that differential treatment of employees can be viewed negatively and can have undesirable effects on behaviors (Posey *et al*, 2011); thus, employers must be mindful, when tailoring these messages for diverse personality types, that the procedures used to reward or punish employees as well as the methods for assessing employee performance (Hsu *et al*, forthcoming) must be designed to be fair and consistent to avoid perceptions of procedural justice (Willison & Warkentin, 2013). In other words, persuasive communications can be differential, but other controls (such as the use of sanctions) must be seen as fair and equitable.

Limitations and future research

Several limitations of our work point to exciting opportunities for future research. First, in our study, we measured the intention to violate a security policy. While the factorial survey design enables us to overcome some of the weaknesses of survey-based research, future studies should also explore actual security behaviors (Warkentin *et al*, 2012). Second, our research model incorporates many of the fundamental individual differences that impact compliance behavior; however, the model is not exhaustive. There are numerous situational and dispositional factors that may impact intention to comply with an

information security policy. For instance, future studies could incorporate both formal and informal sanctions into the proposed model. In addition, we only assessed a single type of information security policy violation. Non-compliance with information security policies by failing to encrypt data removed from the workplace is only one of many possible violation behaviors (Guo, 2013; Willison & Warkentin, 2013). To some extent, the choice of one behavior limits the generalizability of the findings to other security misbehaviors. However, given the large number of manipulations included in the study, adding multiple violations was not feasible. Hence, future research should utilize diverse methods, such as action research or design science, to explore the impact of these meta-traits on additional security misbehaviors.

Finally, one of criticisms of scenario-based designs is that subjects are asked to assess how they would respond in given fictitious situations. If the situation is perceived as unrealistic, it is difficult for the subject to envision it or him/herself within it. For that reason, it is a tradition of researchers employing the factorial survey design to control for realism in scenario construction (Piquero *et al*, 2000; Barlow *et al*, 2013; Siponen & Vance, 2014; Vance *et al*, 2015). Furthermore, because we are 'setting' the levels of the perceptions derived from situational factors (e.g., sanction severity, self-efficacy, etc.), it is important for the subjects to believe that those levels are realistic for a given scenario. Otherwise, their reported intentions to violate information security policies could be confounded and not attributable to their meta-trait disposition. A common technique among factorial survey designs is to include the full sample of data, including all of the records formerly excluded because of low realism scores, and control for realism. This is less attractive for our study, however, given that we are establishing the levels of perceptions from the situational factors, while most factorial survey studies let those vary by respondent.

Conclusion

Our study integrates situational and dispositional factors into a comprehensive model of information security policy violation intentions. The results confirm that individuals with different dispositional factors indeed react differently to similar situational factors in the context of security-related behaviors. In other words, individuals are not the same; insiders respond to information security interventions differently. Now there is data to show that this differentiation even exists after the perspectives derived from information security interventions have been formed and is because of differences in personality profiles, which are explained by personality meta-traits. Our findings establish the foundation for further explorations of the impact of dispositional factors on insiders' interpretations of managerial communications about information security policies and procedures.

Acknowledgements

This study was funded by a grant from the Institute of Homeland Security Solutions (IHSS) as part of their Cyber Security Test Bed project. IHSS is a federally funded collaborative initiative that coordinates its research activities with the U. S. Department of Homeland Security's Human Factors/Behavioral Sciences Division. An earlier version of this research was presented at the IFIP WG 8.11/11.13 Dewald Roode Workshop on Information Security Research. The authors also thank the anonymous reviewers for their insightful recommendations on earlier versions of this manuscript.

About the authors

Dr. Allen C. Johnston is an Associate Professor and the Director of the MS MIS program in the Collat School of Business at the University of Alabama at Birmingham. His research has been in the area of information assurance and computer security and can be found in *MIS Quarterly, European Journal of Information Systems, Journal of the Association for Information Systems*, and *CACM*.

Dr. Merrill Warkentin is a Professor of MIS and the Drew Allen Endowed Fellow in the College of Business at Mississippi State University. His primary research focus is in behavioral IS security issues. His research has appeared in such journals as *MIS Quarterly, European Journal of Information Systems, Journal of the Association for Information Systems, Decision Sciences, Information Systems Journal*, and others.

Dr. Maranda McBride is an Associate Professor of Management in the School of Business and Economics at North Carolina Agricultural and Technical State University. Her research is in the area of Human Machine Systems Engineering. Results of her research have been published in the *International Journal of Industrial Ergonomics, Ergonomics, Applied Ergonomics*, and *Human Factors*.

Dr. Lemuria Carter is an Associate Professor and the Chair of Information Systems at Virginia Commonwealth University. Her research interests include technology adoption, e-government, cybersecurity, and online trust. She has published in several top-tier journals, including the *Journal of Strategic Information Systems, Information Systems Journal, Journal of the Association for Information Systems*, and the *DATA BASE for Advances in Information Systems*.

References

AKERS R (1990) Rational choice, deterrence, and social learning theory in criminology: the path not taken. *The Journal of Criminal Law and Criminology* **81(3)**, 653–676.

ALESSANDRI G and VECCHIONE M (2012) The higher-order factors of the big five as predictors of job performance. *Personality and Individual Differences* **53(6)**, 779–784.

ANDERSON C and AGARWAL R (2010) Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly* **34**(**3**), 613–643.

ARTHUR W and GRAZIANO W (1996) The five-factor model, conscientiousness, and driving accident involvement. *Journal of Personality* **64**(**3**), 594–618.

ASHTON MC, LEE K, GOLDBERG LR and DEVRIES RE (2009) Higher-order factors of personality: do they exist? *Personality and Social Psychology Review* **13**(**2**), 79–91.

BANDURA A (1977) Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review* **84**(**2**), 191–215.

BARLOW JB, WARKENTIN M, ORMOND D and DENNIS AR (2013) Don't make excuses! Discourage neutralization to reduce IT policy violation. *Computers & Security* **39**(**B**), 145–159.

BARNETT T, PEARSON AW, PEARSON R and KELLERMANNS FW (2015) Five-factor model personality traits as predictors of perceived and actual usage of technology. *European Journal of Information Systems* **24**(**4**), 374–390.

BESNARD D and ARIEF B (2004) Computer security impaired by legitimate users. *Computers & Security* **23**(**3**), 253–264.

BIDJERANO T and DAI DY (2007) The relationship between the big-five model of personality and self-regulated learning strategies. *Science Direct* **17**(**1**), 69–81.

BOLLEN K and LENNOX R (1991) Conventional wisdom on measurement: a structural equation perspective. *Psychological Bulletin* **110**(**2**), 305.

BOSS S, KIRSCH LJ, ANGERMEIER I, SHINGLER RA and BOSS W (2009) If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems* **18**(**18**), 151–164.

BUCHANAN T, JOHNSON JA and GOLDBERG LR (2005) Implementing a five-factor personality inventory for use on the internet. *European Journal of Psychological Assessment* **21**(**2**), 115–127.

BULGURCU B, CAVUSOGLU H and BENBASAT I (2010) Information security compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* **34**(**3**), 523–548.

BURKE K (1969) *A Rhetoric of Motives*. University of California Press, Berkeley, CA.

CARROLL JB (2002) The five factor personality model: how complete and satisfactory is it? In *The Role of Constructs in Psychological and Educational Measurement* (BRAUN HI, JACKSON DN and WILEY DE, Eds), pp 91–126, Routledge Publisher, London.

CARTE T and RUSSELL C (2003) In pursuit of moderation: nine common errors and their solutions. *MIS Quarterly* **27**(**3**), 479–502.

CARVER C and SCHEIER M (1994) Situational coping and coping dispositions in a stressful transaction. *Journal of Personality and Social Psychology* **66**(**1**), 184–195.

CHENEY G (1983) The rhetoric of identification and the study of organizational communication. *Quarterly Journal of Speech* **69**(**2**), 143–158.

CONLEY JJ (1985) Longitudinal stability of personality traits: a multitrait-multimethod-multioccasion analysis. *Journal of Personality and Social Psychology* **49**(**5**), 1266–1282.

CONNOR-SMITH JK and FLACHSBART C (2007) Relations between personality and coping: a meta-analysis. *Journal of Personality and Social Psychology* **93**(**6**), 1080–1107.

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

DARLEY JM and BATSON D (1973) 'From Jerusalem to Jericho': a study of situational and dispositional variables in helping behavior. *Journal of Personality and Social Psychology* **27**(**1**), 100–108.

DEYOUNG CG (2006) Higher-order factors of the big five in a multi-informant sample. *Journal of Personality and Social Psychology* **91**(**6**), 1138–1151.

DEYOUNG CG, PETERSON JB and HIGGINS DM (2002) Higher-order factors of the big five predict conformity: are there neuroses of health? *Personality and Individual Differences* **33**(**4**), 533–552.

DIAMANTOPOULOS A and SIGUAW JA (2006) Formative versus reflective indicators in organizational measure development: a comparison and empirical illustration. *British Journal of Management* **17**(**4**), 263–282.

DIGMAN JM (1997) Higher-order factors of the big five. *Journal of Personality and Social Psychology* **73**(**6**), 1246–1256.

DUTTA MJ and VANACKER B (2000) Effects of personality on persuasive appeals in health communication. *Advances in Consumer Research* **27**(**1**), 119–124.

EARLEY P, GIBSON CB and CHEN CC (1999) How did I do? versus how did we do? Cultural contrasts of performance feedback use and self-efficacy. *Journal of Cross-Cultural Psychology* **30**(**5**), 594–619.

EHRLICH I (1996) Crime, punishment, and the market for offenses. *Journal of Economic Perspectives* **10**(**1**), 43–67.

ELLINGSON JE, SMITH DB and SACKETT PR (2001) Investigating the influence of social desirability on personality factor structure. *Journal of Applied Psychology* **86**(**1**), 122–133.

EMM D (2013) The threat landscape: A practical guide from the Kaspersky lab experts. [WWW document] http://media.kaspersky.com/en/business-security/kaspersky-threat-landscape-it-online-security-guide.pdf (accessed 17 November 2014).

ENGELBERG E and SJÖBERG L (2004) Internet use, social skills, and adjustment. *Cyber Psychology & Behavior* **7**(**1**), 41–47.

ERNST & YOUNG (2013) Under cyber attack: EY's global information security survey 2013. [WWW document] http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf (accessed 17 November 2014).

FAUL F, ERDFELDER E, LANG A-G and BUCHNER A (2007) G*Power 3: a flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods* **39**(**2**), 175–191.

FAUL F, ERDFELDER E, LANG A-G and BUCHNER A (2009) Statistical power analyses using G*Power 3.1: tests for correlation and regression analyses. *Behavior Research Methods* **41**(**4**), 1149–1160.

FLOYD DL, PRENTICE-DUNN S and ROGERS RW (2000) A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology* **30**(**2**), 407–429.

GOLDBERG LR (1993) The structure of phenotypic personality traits. *American Psychologist* **48**(**1**), 26–34.

GULLONE E and MOORE S (2000) Adolescent risk-taking and the five-factor model of personality. *Journal of Adolescence* **23**(**4**), 393–407.

GUO KH (2013) Security-related behavior in using information systems in the workplace: a review and synthesis. *Computers & Security* **32**(**February**), 242–251.

HERATH R and RAO HR (2009) Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems* **18**(**2**), 106–125.

HIRSH JB, DEYOUNG CG and PETERSON JB (2009) Metatraits of the big five differentially predict engagement and restraint of behavior. *Journal of Personality* **77**(**4**), 1085–1102.

HOFFER JA and STRAUB DW (1989) The 9-to-5 underground: are you policing computer crimes. *Sloan Management Review* **30**(**4**), 35–43.

HOFMANN W, GSCHWENDNER T, FRIESE M, WIERS R and SHMITT M (2008) Working memory capacity and self-regulatory behavior: toward an individual differences perspective on behavior determination by automatic versus controlled processes. *Journal of Personality and Social Psychology* **95**(**4**), 962–977.

HOFSTEDE G (1991) *Work-Related Values, Software of the Mind*. McGraw-Hill, UK, Berkshire.

HSU JS-C, SHIH S-P, HUNG YW and LOWRY PB (forthcoming) The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research.*

JANIS IL and FESHBACH S (2006) Personality differences associated with responsiveness to fear-arousing communications. *Journal of Personality* **23**(**2**), 154–166.

JASSO G and ROSSI PH (1977) Distributive justice and earned income. *American Sociological Review* **42**(**4**), 639–651.

JASSO G (2006) Factorial survey methods for studying beliefs and judgments. *Sociological Methods & Research* **34**(**3**), 334–423.

JOHN OP and SRIVASTAVA S (1999) The big-five trait taxonomy: history, measurement, and theoretical perspectives. In *Handbook of Personality: Theory and Research* (PERVIN LA and JOHN OP, Eds), Guilford Press, New York.

JOHNSTON AC and WARKENTIN M (2010) Fear appeals and information security behaviors: an empirical study. *MIS Quarterly* **34**(**3**), 549–566.

JOHNSTON AC, WECH B and JACK E (2013) Engaging remote employees: the moderating role of 'remote' status in determining employee information security policy awareness. *Journal of Organizational and End User Computing* **25**(**1**), 1–23.

JOHNSTON AC, WARKENTIN M and SIPONEN M (2015) An enhanced fear appeal framework: leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly* **39**(**1**), 113–134.

JUNGLAS IA, JOHNSON NA and SPITZMÜLLER C (2008) Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems* **17**(**4**), 387–402.

KAJZER M, D'ARCY J, CROWELL CR, STRIEGEL A and VAN BRUGGEN D (2014) An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers & Security* **43**(**June**), 65–76.

KAMMRATH L, MENDOZA-DENTON R and MISCHEL W (2005) Incorporating if … then … personality signatures in person perception: beyond the person – situation dichotomy. *Journal of Personality and Social Psychology* **88**(**4**), 605–618.

KARIM NSA, ZAMZURI NHA and NOR YM (2009) Exploring the relationship between Internet ethics in university students and the big five model of personality. *Computers & Education* **53**(**1**), 86–93.

KEIL M, TAN BCY, WEI K-K, SAARINEN T, TUUNAINEN V and WASSANAAR A (2000) A cross-cultural study on escalation of commitment behavior in software projects. *MIS Quarterly* **24**(**2**), 299–325.

LANDERS RN and LOUNSBURY JW (2006) An investigation of big five and narrow personality traits in relation to internet usage. *Computers in Human Behavior* **22**(**2**), 283–293.

LEE Y and LARSEN KR (2009) Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems* **18**(**2**), 177–187.

LIM KH and BENBASAT I (2000) The effect of multimedia on perceived equivocality and perceived usefulness of information systems. *MIS Quarterly* **24**(**3**), 449–471.

LINDQVIST J (2012) Nudging people. WINLAB, Dept. of ECE, Rutgers University Presentation at the NSF/DIMACS Workshop for Aspiring PIs in Secure and Trustworthy Cyberspace, Raleigh, NC. 15 October. [WWW document] http://dimacs.rutgers.edu/Workshops/Aspiring/program.html (accessed 29 November 2012).

LITTELL R, MILLIKEN G, STROUP W and WOLFINGER R (1996) *SAS Systems for Mixed Models*. SAS Institute, Cary, NC.

LYONS CJ (2008) Individual perceptions and the social construction of hate crimes: a factorial survey. *The Social Science Journal* **45**(**1**), 107–131.

MADDUX JE and ROGERS RW (1983) Protection motivation and self-efficacy: a revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology* **19**(**5**), 469–479.

MAJOR DA, TURNER JE and FLETCHER TD (2006) Linking proactive personality and the big five to motivation to learn and development activity. *Journal of Applied Psychology* **91**(**4**), 927–935.

MCBRIDE M, CARTER L and WARKENTIN M (2012) One size doesn't fit all: cybersecurity training should be customized. Technical Report, Institute for Homeland Security Solutions. [WWW document] http://sites.duke.edu/ihss/files/2011/12/CyberSecurity_2page-summary_mcbride-2012. pdf (accessed 25 June 2014).

MCLEAN R, SANDERS W and STROUP W (1991) A unified approach to mixed linear models. *The American Statistician* **45**(**1**), 54–64.

MISCHEL W (1968) *Personality and Assessment*. John Wiley & Sons, Hoboken, NJ.

MISCHEL W, EBBESEN EB and ZEISS AR (1973) Selective attention to the self: situational and dispositional determinants. *Journal of Personality and Social Psychology* **27**(**1**), 129–142.

MUSEK J (2007) A general factor of personality: evidence for the big one in the five-factor model. *Journal of Research in Personality* **41**(**6**), 1213–1233.

NICHOLSON N, SOANE E, FENTON-O'CREEVY M and WILLMAN P (2005) Personality and domain-specific risk taking. *Journal of Risk Research* **8**(**2**), 157–176.

PAULHUS DL and WILLIAMS KM (2002) The dark triad of personality: narcissism, machiavellianism, and psychopathy. *Journal of Research in Personality* **36**(**6**), 556–563.

PIQUERO AR, MACINTOSH R and HICKMAN M (2000) Does self-control affect survey response? Applying exploratory, confirmatory, and item response theory analysis to Grasmick *et al*'s self-control scale. *Criminology* **38**(**3**), 897–930.

PONEMON INSTITUTE (2013) 2014 state of endpoint risk. [WWW document] http://www.lumension.com/Lumension/media/graphics/Resources/2014-state-of-the-endpoint/2014-State-of-the-Endpoint-Whitepaper-Lumension.pdf (accessed 17 November 2014).

POSEY C, BENNETT RJ, ROBERTS TL and LOWRY PB (2011) When computer monitoring backfires: privacy invasions and organizational injustice as precursors to computer abuse. *Journal of Information Systems Security* **7**(**1**), 24–47.

ROSSI PH and ANDERSON AB (1982) The factorial survey approach: an introduction. In *Measuring Social Judgments: The Factorial Survey Approach* (ROSSI PH and NOCK SL, Eds), pp 15–67, Sage, Beverly Hills, CA.

ROSSI PH and NOCK SL (1982) *Measuring Social Judgments: The Factorial Survey Approach*. Sage Publications, Beverly Hills.

SELF CA and ROGERS RW (1990) Coping with threats to health: effects of persuasive appeals on depressed, normal, and antisocial personalities. *Journal of Behavioral Medicine* **13**(**4**), 343–357.

SHLAY AB, TRAN H, WEINRAUB M and HARMON M (2005) Teasing apart the child care conundrum: a factorial survey analysis of perceptions of child care quality, fair market price and willingness to pay by low-income, African American parents. *Early Childhood Research Quarterly* **20**(**4**), 393–413.

SHROPSHIRE J, WARKENTIN M and SHARMA S (2015) Personality, attitudes, and intentions: predicting initial adoption of information security behavior. *Computers & Security* **29**(**March**), 177–191.

SIGALL H and MILLS J (1998) Measures of independent variables and mediators are useful in social psychological experiments: but are they necessary? *Personality and Social Psychology Review* **2**(**3**), 218–226.

SIPONEN M and VANCE A (2010) Neutralization: new Insights into the problem of employee information systems security policy violations. *MIS Quarterly* **34**(**3**), 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**), 289–305.

SOANE E and CHMIEL N (2005) Are risk preferences consistent? The influence of decision domain and personality. *Personality and Individual Differences* **38**(**8**), 1781–1791.

SWICKERT RJ, HITTNER JB, HARRIS JL and HERRING JA (2002) Relationships among internet use, personality, and social support. *Computers in Human Behavior* **18**(**4**), 437–451.

TAYLOR BJ (2006) Factorial surveys: using vignettes to study professional judgement. *British Journal of Social Work* **36**(**7**), 1187–1207.

TREVINO L and VICTOR B (1992) Peer reporting of unethical behavior: a social context perspective. *Academy of Management Journal* **35**(**1**), 38–64.

TRINKLE BS, CROSSLER RE and WARKENTIN M (2014) I'm game, are you? Reducing real-world security threats by managing employee activity in virtual environments. *Journal of Information Systems* **28**(**2**), 307–327.

VANCE A, LOWRY PB and EGGETT D (2013) Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems* **29**(**4**), 263–290.

VANCE A, LOWRY PB and EGGETT D (2015) Increasing accountability through user-interface design artifacts: a new approach to address the problem of access-policy violations. *MIS Quarterly* **39**(**2**), 345–366.

VECCHIONE M, ALESSANDRI G, BARBARANELLI C and CAPRARA G (2011) Higher-order factors of the big five and basic values: empirical and theoretical relations. *British Journal of Psychology* **102**(**3**), 478–498.

VERIZON (2015) Verizon data breach investigation report. [WWW document] http://www.verizonenterprise.com/DBIR/ (accessed 7 June 2015).

WARKENTIN M, CARTER L and MCBRIDE ME (2011) Exploring the role of individual employee characteristics and personality on employee compliance with cyber security policies. Paper presented at the International Federation of Information Processing (IFIP) Dewald Roode Workshop on Information Systems Security Research, Blacksburg, VA.

WARKENTIN M, JOHNSTON AC and SHROPSHIRE J (2011) The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems* **20**(**3**), 267–284.

WARKENTIN M, STRAUB D and MALIMAGE K (2012) Measuring secure behavior: a research commentary. In *Proceedings of the 7th Annual Symposium on Information Assurance*, pp. 1–8, Albany, NY. [WWW document] http://www.albany.edu/iasymposium/proceedings/2012/5-Warkentin_Straub&Malimage.pdf (accessed 15 October 2015).

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

WARKENTIN M, WILLISON R and JOHNSTON AC (2011) The role of perceptions of organizational injustice and techniques of neutralization in forming computer abuse intentions. In *Proceedings of the 17th Americas Conference on Information Systems (AMCIS)*, pp 1–8, Detroit, MI, August, [WWW document] http://aisel.aisnet.org/amcis2011_submissions/318/.

WHEELER SC, PETTY R and BIZER G (2005) Self-schema matching and attitude change: situational and dispositional determinants of message elaboration. *Journal of Consumer Research* **31(4)**, 787–797.

WILLISON R and WARKENTIN M (2009) Motivations for employee computer crime: understanding and addressing workplace disgruntlement through the application of organisational justice. In *Proceedings of the International Federation of Information Processing (IFIP) International Workshop on Information Systems Security Research* (VANCE A. Ed), pp 127–144, Cape Town, South Africa, May.

WILLISON R and WARKENTIN M (2013) Beyond deterrence: an expanded view of employee computer abuse. *MIS Quarterly* **37(1)**, 1–20.

WILT J, OLSON BD and MCADAMS DP (2011) Higher-order factors of the big five predict exploration and threat in life stories. *Journal of Research in Personality* **45(6)**, 613–621.

WORKMAN M, BOMMER WH and STRAUB D (2008) Security lapses and the omission of information security measures: a threat control model and empirical test. *Computers in Human Behavior* **24(6)**, 2799–2816.

WRIGHT J and MISCHEL W (1987) A conditional approach to dispositional constructs: the local predictability of social behavior. *Journal of Personality and Social Psychology* **53(6)**, 1159–1177.

ZHANG L (2006) Thinking styles and the big five personality traits revisited. *Personality and Individual Differences* **40(6)**, 1177–1187.

ZHANG J, LUO X, AKKALADEVI S and ZIEGELMAYER J (2009) Improving multiple-password recall: an empirical study. *European Journal of Information Systems* **18(2)**, 165–176.

ZUCKERMAN M and KUHLMAN DM (2000) Personality and risk-taking: common bisocial factors. *Journal of Personality* **68(6)**, 999–1029.

Appendix A

Sample vignette (plus items that follow each vignette)

Joe has just collected sensitive customer data for his company, and he wants to take that data home to continue his work. He knows his company requires that he request a password to be issued and applied to all data before taking it out of the office on a USB drive so that it cannot be accessed by an unauthorized individual. Joe has completed the password request procedure before, so he is confident he can do it again easily. Joe believes that without the password, it is not likely that unauthorized people will see the data, but if they do, nothing bad will happen. Joe believes that the password procedure is effective and prevents unauthorized people from seeing the data. Regardless, the password procedure takes several minutes, and he needs to leave now, so he skips the procedure. Joe believes his chances of being caught are low, but if caught, the punishment would be minimal.

Please select an answer for the following items as they relate to the vignette.

How confident was Joe about his ability to complete the password request procedure?

a He was confident he could do it again easily.
b He was not confident he could do it again easily.

What did Joe believe about the threat of other people seeing the data?

c He believed it was not likely they would see the data, but if they did, nothing bad would happen.
d He believed it was not likely they would see the data, but if they did, they may alter or misuse it.
e He believed it was likely they would see the data, but if they did, nothing bad would happen.
f He believed it was likely they would see the data, and if they did, they may alter or misuse it.

What did Joe believe about the effectiveness of the password procedure?

g He believes that the password procedure is effective and prevents unauthorized people from seeing the data.
h He believes that the password procedure is not effective and does not prevent unauthorized people from seeing the data.

What did Joe think about the punishment for his actions?

i Joe thought that it was unlikely he would be punished, and if so, the punishment would not be severe.
j Joe thought that it was unlikely he would be punished, but if he was, the punishment would be severe.
k Joe thought that it was likely he would be punished, but the punishment would not be severe.
l Joe thought that it was likely he would be punished, and the punishment would be severe.

	SD						*SA*
In this situation, I would do the same as Joe	1	2	3	4	5	6	7
The password request procedure takes a long time	1	2	3	4	5	6	7
The above vignette is a realistic one	1	2	3	4	5	6	7
If I were Joe, I would have also skipped the procedure	1	2	3	4	5	6	7
The password procedure does not take long	1	2	3	4	5	6	7
I could imagine a similar vignette taking place at work	1	2	3	4	5	6	7
I think I would do what Joe did if this happened to me	1	2	3	4	5	6	7
The situation could occur at work	1	2	3	4	5	6	7
The password procedure will take too much time	1	2	3	4	5	6	7

Note: SD = Strongly disagree, SA = Strongly agree.

Appendix B

Constructs manipulated in the vignettes (scenario versions)

Below are the statements associated with the various levels of each of the situational factors manipulated in the vignettes. The levels are shown in parentheses.

Self-efficacy levels

- Joe has completed the password request procedure before, but he is not confident he can do it again easily – (low)
- Joe has completed the password request procedure before, so he is confident he can do it again easily – (high)

Threat vulnerability and severity

- Joe believes that, without the password, it is not likely that unauthorized people will see the data, but if they do, nothing bad will happen – (low/low)
- Joe believes that, without the password, it is not likely that unauthorized people will see the data, but if they do, they may alter or misuse it – (low/high)
- Joe believes that, without the password, it is likely that unauthorized people will see the data, but if they do, nothing bad will happen – (high/low)
- Joe believes that, without the password, it is likely that unauthorized people will see the data and if they do, they may alter or misuse it – (high/high)

Sanction certainty and severity

- Joe believes his chances of being caught are low, but if caught, the punishment would be minimal – (low/low)
- Joe believes his chances of being caught are low, but if caught, the punishment would be severe – (low/high)
- Joe believes his chances of being caught are high, and if caught, the punishment would be minimal – (high/low)
- Joe believes his chances of being caught are high, and if caught, the punishment would be severe – (high/high)

Response efficacy

- Joe believes that the password procedure is not effective and does not prevent unauthorized people from seeing the data – (low)
- Joe believes that the password procedure is effective and prevents unauthorized people from seeing the data – (high)

Appendix C

Five factor (Big Five) survey

Please choose a number for each statement to indicate the extent to which you agree or disagree with that statement by selecting 1 to 7 where 1 means you Strongly Disagree with the statement and 7 means you Strongly Agree with the statement.

I see myself as someone who …

Extraversion

1. Is outgoing, sociable.
2. Is talkative.
3. Has an assertive personality.
4. Generates a lot of enthusiasm.
5. Is full of energy.

Agreeableness

1. Is considerate and kind to almost everyone.
2. Likes to cooperate with others.
3. Is helpful and unselfish with others.
4. Has a forgiving nature.
5. Is generally trusting.

Conscientiousness

1. Does a thorough job.
2. Does things efficiently.
3. Makes plans and follows through with them.
4. Is a reliable worker.
5. Perseveres until the task is finished.

Neuroticism

1. Can be moody.
2. Is depressed, blue.
3. Gets nervous easily.
4. Can be tense.
5. Worries a lot.

Openness

1. Is inventive.
2. Is original, comes up with new ideas.
3. Values artistic, esthetic experiences.
4. Has an active imagination.
5. Likes to reflect, play with ideas.
6. Is sophisticated in art, music, or literature.
7. Is ingenious, a deep thinker.
8. Is curious about many different things.

Appendix D

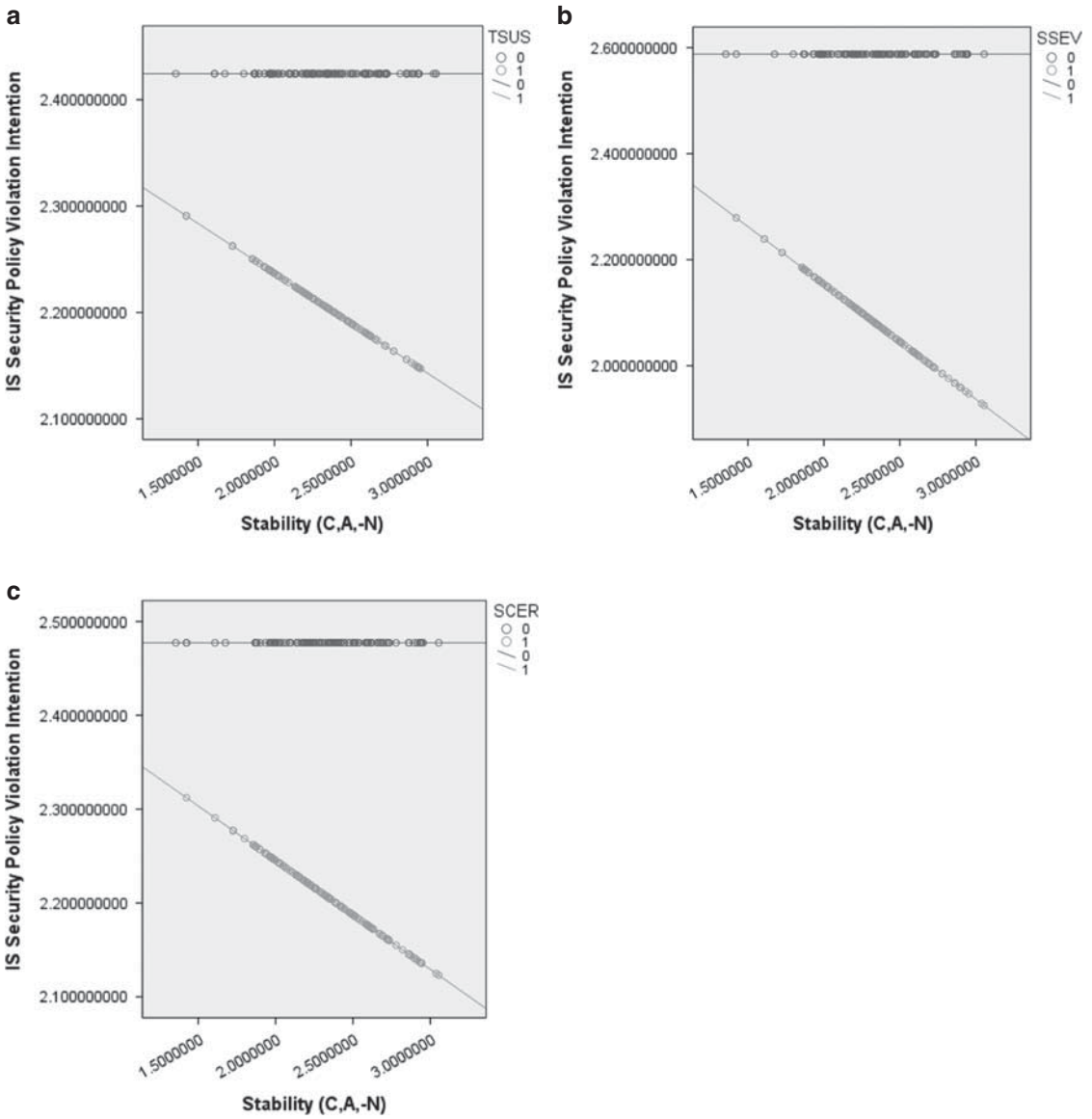

Figure D1 'Stability' meta-trait (C,A,–N) moderating influence plots. (a) Stability*Threat Vulnerability (TSUS) Plot; (b) Stability*Sanction Severity (SSEV) Plot; (c) Stability*Sanction Certainty (SCER) Plot.
Note: These plots depict a negative moderating effect of Stability on threat vulnerability, sanction severity, and sanction certainity. These plots suggest that as one's personality becomes more strongly aligned with the Stability meta-trait, he or she will be less likely than their less Stability oriented counterparts to form information security policy violation intentions when perceiving high degrees of threat vulnerability (TSUS=1), sanction severity (SSEV=1), or sanction certainty (SCER=1).

Appendix E

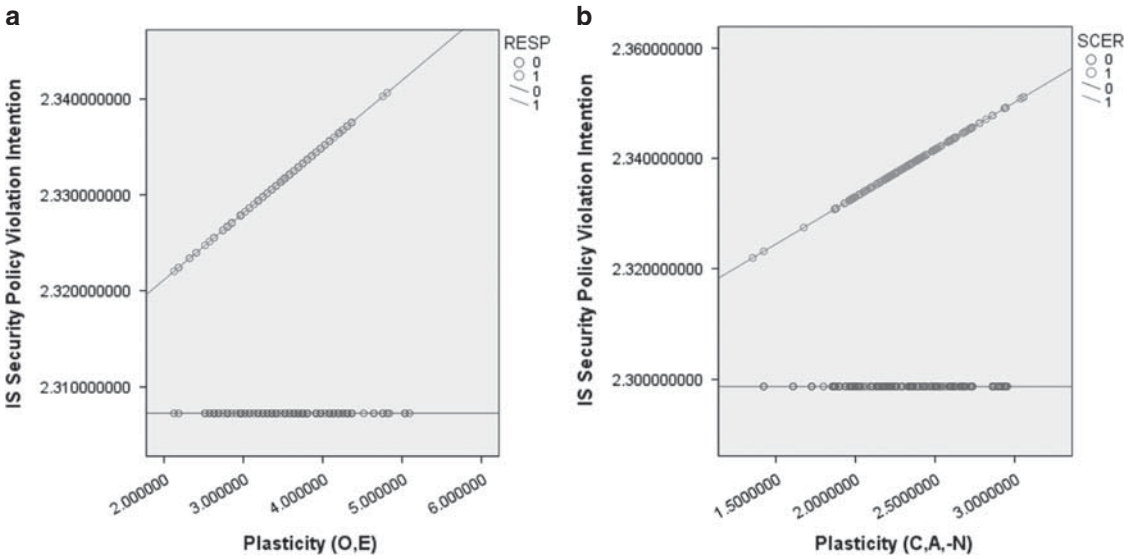

Figure E1 'Plasticity' meta-trait (O, E) moderating influence plots. (a) Plasticity*Response Efficacy (RESP) Plot; (b) Plasticity*Sanction Certainty Plot.
Note: These plots depict a positive moderating effect of Plasticity on response efficacy and sanction certainty. These plots suggest that as one's personality becomes more strongly aligned with the Plasticity meta-trait, he or she will be more likely than their less Plasticity-oriented counterparts to form information security policy violation intentions when perceiving high degrees of response efficacy (RESP=1) or sanction certainty (SCER=1).

Appendix F

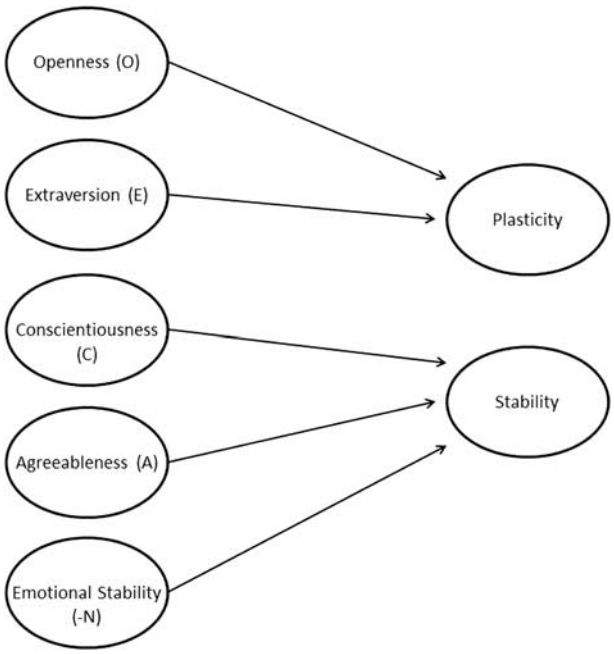

Figure F1 PLS model for obtaining Big Five PLS weights.