MIS Quarterly

SPECIAL ISSUE

INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS[1]

By: **Burcu Bulgurcu**
Sauder School of Business
University of British Columbia
Vancouver, BC V6T 1Z2
CANADA
burcu.bulgurcu@sauder.ubc.ca

Hasan Cavusoglu
Sauder School of Business
University of British Columbia
Vancouver, BC V6T 1Z2
CANADA
hasan.cavusoglu@sauder.ubc.ca

Izak Benbasat
Sauder School of Business
University of British Columbia
Vancouver, BC V6T 1Z2
CANADA
izak.benbasat@sauder.ubc.ca

Abstract

Many organizations recognize that their employees, who are often considered the weakest link in information security, can also be great assets in the effort to reduce risk related to information security. Since employees who comply with the information security rules and regulations of the organization are the key to strengthening information security, understanding compliance behavior is crucial for organizations that want to leverage their human capital.

This research identifies the antecedents of employee compliance with the information security policy (ISP) of an organization. Specifically, we investigate the rationality-based factors that drive an employee to comply with requirements of the ISP with regard to protecting the organization's information and technology resources. Drawing on the theory of planned behavior, we posit that, along with normative belief and self-efficacy, an employee's attitude toward compliance determines intention to comply with the ISP. As a key contribution, we posit that an employee's attitude is influenced by ***benefit of compliance***, ***cost of compliance***, *and* ***cost of noncompliance***, *which are beliefs about the* ***overall assessment of consequences*** *of compliance or noncompliance. We then postulate that these beliefs are shaped by the employee's* ***outcome beliefs*** *concerning the events that follow compliance or noncompliance: benefit of compliance is shaped by* ***intrinsic benefit***, ***safety of resources***, *and* ***rewards***, *while cost of compliance is shaped by* ***work impediment***; *and cost of noncompliance is shaped by* ***intrinsic cost***, ***vulnerability of resources***, *and* ***sanctions***. *We also investigate the impact of* ***information security awareness*** *(ISA) on outcome beliefs and an employee's attitude toward compliance with the ISP.*

Our results show that an employee's intention to comply with the ISP is significantly influenced by attitude, normative beliefs, and self-efficacy to comply. Outcome beliefs significantly affect beliefs about overall assessment of conse-

[1]Mikko Siponen was the accepting senior editor for this paper. Merrill Warkentin served as the associate editor.

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

quences, and they, in turn, significantly affect an employee's attitude. Furthermore, ISA positively affects both attitude and outcome beliefs. As the importance of employees' following their organizations' information security rules and regulations increases, our study sheds light on the role of ISA and compliance-related beliefs in an organization's efforts to encourage compliance.

Keywords: Information security awareness, information security management, compliance, information security policy, behavioral issues of information security, theory of planned behavior

Introduction

Organizations' heavy reliance on information systems (IS) requires them to manage the risks associated with those systems. Today, risks related to information security are a major challenge for many organizations, since these risks may have dire consequences, including corporate liability, loss of credibility, and monetary damage (Cavusoglu, Cavusoglu, and Raghunathan 2004). Ensuring information security has become one of the top managerial priorities in many organizations (Brancheau et al. 1996; Lohmeyer et al. 2002; Ransbotham and Mitra 2009).

To reduce these risks and ensure information security, organizations often rely on technology-based solutions (Ernst & Young 2008; PricewaterhouseCoopers 2008). Although these types of solutions help improve information security (Straub 1990), relying on them exclusively (or excessively) is seldom enough to eliminate the risk (Cavusoglu et al. 2009; Dhillon and Backhouse 2001; Siponen 2005). Empirical and anecdotal evidence indicates that the number of incidents related to information security is increasing (AIRC 2008; Symantec 2009) even as organizations invest more in technology-based solutions. Success in information security can be achieved when organizations invest in both technical and socio-organizational resources.

As the focus on information security shifts toward individual and organizational perspectives, employees' compliance with information security policies (hereafter ISPs) has emerged as a key socio-organizational resource (Boss and Kirsch 2007; Siponen et al. 2007) because employees are often the weakest link in information security (Mitnick and Simon 2002; Warkentin and Willison 2009). Organizations create ISPs to provide employees with guidelines concerning how to ensure information security while they utilize information systems in the course of performing their jobs (Whitman et al. 2001); however, while creating guidelines and policies is an essential starting point, it is not enough to ensure employees' compliance with them. Therefore, an understanding of what factors motivate employees to comply with their organizations' ISPs is central to helping information security managers diagnose the deficiencies in their information security management efforts and in providing them with ways to solve the behavioral issues in information security management.

Recently Pahnila et al. (2007) and Herath and Rao (2009) investigated motivational factors rooted in deterrence theory and protection motivation theory to explain the employees' compliance behavior. Our study aims to extend the knowledge about employee compliance with ISPs by identifying rationality-based factors rooted in the rational choice theory. In so doing, our study addresses three questions.

(1) What are the broad classes of an employee's beliefs about *the overall assessment of consequences* of compliance or noncompliance that influence attitude toward compliance and, in turn, intention to comply with the ISP?

(2) What are an employee's beliefs about the *outcomes* of compliance and noncompliance that influence beliefs about the overall assessment of consequences?

(3) What is the role of information security awareness (ISA) in shaping an employee's beliefs about outcomes and attitude toward compliance?

Drawing on the theory of planned behavior (TPB) (Ajzen 1991), we postulate that an employee's intention to comply with the organization's ISP is influenced by subjective norms, perceived behavioral control, and attitude toward compliance. Building on the TPB, we trace employee attitude toward compliance with the ISP back to its underlying set of compliance-related beliefs, which are rooted in the rational choice theory (RCT). We also investigate the role of information security awareness and postulate that it influences an employee's outcome beliefs as well as attitude toward compliance. We answer the research questions related to the antecedents of an employee's intention to comply with the ISP using data collected through a survey of 464 employees from a diverse set of organizations.

The paper is organized as follows. The next section presents a brief review of the relevant literature and highlights the unique contributions of our work, while the third section lays out the theoretical foundation of the research. We then discuss the research model and develop the hypotheses to be tested, followed by a summary of the research method, and a

description of the data analysis and presentation of the results. Finally, we discuss the findings, their implications, and future research directions.

Literature Review

Previous studies on IS security have highlighted a number of important topics such as IS security effectiveness (Kankanhalli et al. 2003; Straub 1990; Woon and Kankanhalli 2003), security planning and risk management (Soo Hoo 2000; Straub 1998; Straub and Welke 1998), the economics of IS security and evaluation of IS security investments (Cavusoglu, Cavusoglu, and Raghunathan 2004; Cavusoglu, Mishra, and Raghunathan 2004a, 2004b), and the design, development, and alignment of the ISP (Doherty and Fulford 2006; Siponen and Iivari 2006). While these studies have expanded our understanding of IS security from various perspectives, their number is not commensurate with the importance of the subject. IS security research is particularly underrepresented in the leading IS journals (Siponen and Willison 2007).

An emerging research stream on the human perspective of information security focuses on end-user (insider) behaviors and attempts to identify the factors that lead to compliance behavior regarding information security. The current literature recognizes that *insiders*, a term that refers to employees who are authorized to use a particular system or facility (Neumann 1999), may pose a challenge to an organization because their ignorance, mistakes, and deliberate acts can jeopardize information security (Durgin 2007; Lee and Lee 2002; Lee et al. 2003). The vast majority of recent survey reports and anecdotal evidence supports this argument. According to a recent CSI/FBI survey, 64 percent of the respondents reported that some of the losses related to information security they have incurred are due to the actions of insiders (Gordon et al. 2006).

Employees' abuse and misuse of IS resources have been identified in the extant literature as the major information security issue related to insiders, so most of the earlier empirical studies that investigated end-user behaviors assumed that employees simply choose to engage in inappropriate behaviors. Therefore, these studies focused on deterrent and preventative strategies (e.g., sanctions) for reducing IS misuse and computer abuse. For example, Straub and Nance (1990) investigated how to discover computer abuse and discipline perpetrators, suggesting that organizations should punish serious violations to the full extent possible because such punishment would deter other such behavior. In an effort to understand the problems related to information security posed by employees, Willison (2006) focused on computer crime by employees and investigated the relationship between the offender and the context using rational choice and situational crime prevention theories. Willison argued that organizations should focus on the actual behaviors of offenders at various stages of their misuse in order to implement controls (safeguards) that would reduce the employees' ability to misuse the IS at each stage and, in so doing, effectively influence the decision-making processes of their employees. Lee and Lee (2002) proposed a conceptual research model based on deterrence theory and several social theories to explain the influence of organizational factors, information security policy and information awareness programs on preventing computer abuse. Lee et al. (2003) analyzed computer abuse that originates from insiders and outsiders by assessing the role of deterrence and organizational factors and found that enhancement of social bonds through organizational factors (attachment, commitment, involvement, and norm) is an effective mechanism in preventing computer abuse.

Even though most of the information security literature regarding insiders has focused on abusive behavior and has considered employees to be potential information security risks, it has also recognized that employees can help organizations safeguard information and technology resources by performing beneficial acts. To encourage such acts, organizations often put together an ISP that stipulates what roles employees should play. However, the simple existence of these policies does not automatically translate into desirable behaviors because employees may not be motivated to perform the activities required to protect their organization's information and technology resources (Stanton et al. 2005).

Hence, identifying what drives employees' compliance with the roles and responsibilities stipulated in the ISP is central to expanding the literature on information security and to defining where organizations should focus when devising mechanisms to improve their employees' compliance. For example, organizations can tailor persuasive communication to emphasize the important drivers, they can restructure security training and awareness programs to highlight the drivers, or they can use what motivates employees to assess whether ISPs focus on the right motives.

In contrast to many studies that have argued the deterrence effects of sanctions, a few recent studies have focused on the desirable acts of end-users—prescription, rather than proscription—as they relate to information security. Boss and Kirsch (2007) introduced the concept of *mandatoriness*, which has been shown to motivate individuals to take security precautions. While rewards have not been found to be effec-

tive in convincing individuals that security policies are mandatory, specifying policies, evaluating behaviors, and computer self-efficacy have been effective. Later, Boss et al. (2009) showed that mandatoriness mediates the relationship between the control element (specification, evaluation, and reward) and security precautions taken. Pahnila et al. (2007) proposed a theoretical model in which they found that information quality had a significant effect on actual compliance, threat appraisal and facilitating conditions had a significant effect on attitude toward compliance, and sanctions and rewards did not influence intention to comply or actual compliance. In an attempt to understand end-user behaviors in regard to computer technologies that protect data and systems from security-related threats (i.e., protective information technologies), Dinev et al. (2008) posited that cultural differences moderate the strength of such technologies. Myyry et al. (2009) suggested that moral reasoning and employees' values can explain their adherence to information security policies and showed that moral reasoning and values explain employees' adherence to an information security rule prohibiting password sharing. Herath and Rao (2009), drawing on protection motivation theory which was developed to understand how fear appeal motivates health behavior (Rogers 1975, 1983), argued that an employee's attitude toward adopting security technologies and practices is shaped by threat appraisal and coping appraisal processes, in which the employee evaluates the security risks and adopting security technologies and practices as a means to cope with those risks. They also showed that factors rooted in protection motivation theory influence employees' attitudes toward adopting security technologies and practices, but they did not find support for the hypothesis that employee's attitude toward adopting security technologies and practices influences employee's security policy compliance.

While the information security literature has highlighted the deterrent effects of sanctions, organization literature has focused on the role of incentives in encouraging desirable employee conduct (Stajkovic and Luthans 1997). Since employees' adherence to organizational policies is essential to successful organizational functioning (Vardi and Weitz 2004), organizations often deploy instrumental strategies in pursuit of better organizational performance (Huselid 1995). However, an employee's willingness to follow rules may not necessarily be motivated only by such strategies. Although rewards (to encourage desired behavior) and punishments (to discourage undesirable behavior) provide external motivations, an employee's intrinsic desires provide the internal motivation to follow (or not to follow) rules and regulations (Tyler and Blader 2005). We expect that similar motivations exist in the context of ISP compliance.

Behavior-related consequences form one's attitude toward the behavior (Fishbein and Ajzen 1975). In our context, an employee's attitude toward compliance is formed when he considers the compliance-related consequences that he will personally experience if he complies (effort, time, etc.) or does not comply (punishment, etc.) with the ISP. Using insights gained from the literature, this study seeks to extend our understanding of an employee's intention to comply by proposing an integrative model to explicate the role of employee beliefs on the intention to comply with an organization's ISP.

Finally, despite the importance of information security awareness, there is a paucity of empirical studies that analyze the impact of information security awareness on information security. Siponen (2000, 2001) conceptually analyzed information security awareness and suggested methods to enhance awareness based on several theoretical perspectives. A few conceptual studies (Furnell et al. 2002; Hentea 2005; Thomson and von Solms 1998) have highlighted the importance of information security awareness education and training, and Puhakainen (2006) proposed a design theory for improving information security awareness campaigns and training. D'Arcy et al. (2009) suggested that organizations can use three security countermeasures—user awareness of security policies; security education, training, and awareness (SETA) programs; and computer monitoring—to reduce user's IS misuse. They showed that users' awareness of countermeasures impacts perceptions on organizational sanctions, which in turn reduces users' IS misuse intention. Still, to the best of our knowledge, the direct and indirect roles of information security awareness on an employee's compliance behavior have not yet been studied. Beyond showing the direct influence of ISA on an employee's attitude toward compliance, we aim to understand the antecedents of compliance by disentangling the relationships between ISA and an employee's outcome beliefs about compliance and noncompliance.

Theoretical Framework

Organizations deploy technological means to protect their information and technology resources, but they also rely on their employees. Employees who use the information and technology resources of their organizations assume certain roles in and are responsible for safeguarding (protecting) those resources, so we are interested in what factors drive an employee to perform those roles and meet their responsibilities. We define *information security policy* as a statement of the roles and responsibilities of the employees to

safeguard the information and technology resources of their organizations. ISP encompasses established rules that address specific security issues by providing instructions to the employees as to what they should do when they interact with the information and technology resources of their organizations (Whitman 2008). Our definition of the ISP is consistent with the extant literature (Boss et al. 2009; D'Arcy et al. 2009; Dhillon 1997; Herath and Rao 2009; Peltier 2004).

Our effort to understand the antecedents of an employee's compliance with the ISP of her organization is undertaken by proposing and testing a model of the factors that influence an employee's intention to comply, based on the theory of planned behavior. Consistent with the TPB, which considers behavioral intention as an indication of an individual's readiness to perform a given behavior, an employee's intention to comply with the requirements of the ISP is used as the dependent variable in the study.

We begin by adopting the three main constructs of the TPB—attitude, subjective norms, and perceived behavioral control—in the ISP compliance context as antecedents of an employee's intention to comply. Then, we add to the model the underlying set of cognitive beliefs, which are rooted in the rational choice theory, as antecedents to attitude. Finally, we investigate the role of information security awareness on an employee's beliefs, as well as its direct impact on attitude. The remainder of this section briefly discusses the TPB and the RCT on which we draw in our model.

The Theory of Planned Behavior

The TPB, an extension of the theory of reasoned action (Ajzen and Fishbein 1980; Fishbein and Ajzen 1975), explains an individual's intention to perform a given behavior. The TPB suggests that the intention to perform various kinds of behaviors can be predicted with high accuracy from attitudes toward the behavior, subjective norms, and perceived behavioral control, and that these intentions, together with perceived behavioral control, account for a considerable amount of variance in the actual behavior (Ajzen 1991). The theory postulates that behavior can be explained by *behavioral beliefs*, *normative beliefs*, and *self-efficacy* as antecedents of attitudes, subjective norms, and perceived behavioral control, respectively. Although these beliefs all influence the intention to perform behaviors, the large majority of the existing literature in the IS field, such as many studies on the technology acceptance model (TAM), has focused most on investigating attitude and its antecedents (behavioral beliefs) because these beliefs can be reshaped by external interventions in the form of objective information concerning information technologies and their design (e.g., Wixom and Todd 2005) to influence those behavioral beliefs and, in turn, improve attitude toward behavior.

Rational Choice Theory

Rational choice theory is a neo-classical economic approach that offers a theoretical explanation for how individuals make decisions when faced with choices. RCT argues that an individual determines how he will act by balancing the costs and benefits of his options. Because of its parsimonious and elegant explanation, the RCT has been widely applied to the study of individual, social, and economic behaviors in many contexts (McCarthy 2002). Becker (1968), for example, adopted a rational choice perspective in his economic approach to crime and argued that a criminal maximizes his expected benefits from an illicit activity in excess of the expected cost of punishment.

In rational decision making, an individual first recognizes alternative courses of action (Paternoster and Pogarsky 2009) and then contemplates the likely outcomes of each courses of action. Outcomes are states of the world after an action is taken, so an action can lead to various outcomes. Since people have preferences for outcomes, each outcome can be perceived to be associated with a cost or a benefit depending on how much satisfaction the outcome will produce for the individual (McCarthy 2002). Hence, overall assessment of costs and benefits that accrue to the individual from a course of action are shaped by the individual's perception of potential outcomes associated with that course of action. Finally, the individual balances his overall assessments of costs and benefits of courses of action to determine the best alternative.

The RCT, while shown to be useful in explaining behaviors in many contexts, is not exempt from criticisms. McCarthy (2002) argued that most criticisms of RCT stem from confusion about its key concepts, premises, and predictions. First, rationality means one's choices are harmonious with his preferences (MacCarthy 2002; Paternoster and Pogarsky 2009). Since an individual's preferences are influenced by his individual *perception* of costs and benefits (Becker 1993), the costs and benefits of alternative courses of action are subjective, reflecting the preference structure of the decision maker. A decision based on his assessment of costs and benefits will be consistent with his preferences and, therefore, rational. Second, RCT recognizes that there is a vast array of costs and benefits, many of which may not necessarily be monetary (Paternoster and Pogarsky 2009; Paternoster and Simpson 1996). While a particular decision maker may focus only on materialistic interest during the appraisal, diverse interests,

such as cultural, social, psychological, or emotional interests, may also be considered according to the theory (McCarthy 2002). Third, RCT does not fail to explain "expressive" offenses that occur in "the heat of the moment." McCarthy argued that anger, jealousy, rage, hatred, and a host of other emotional states are forces (motives) that influence the decision maker's appraisal of the costs and benefits of courses of action. Emotional states are not independent of preferences (Damasio 1994; Elster 1999): while the assessment of costs and benefits in the heat of the moment might be markedly different than that made at other times, RCT argues that the behavior is based on that assessment.

Research Model and Hypotheses

Based on the TPB, we propose a research model that explains an employee's intention to comply with the ISP (Figure 1).

We first trace an employee's *attitude toward compliance* with the ISP back to that attitude's underlying foundation of cognitive beliefs related to compliance. An employee's beliefs that performing or not performing the compliance behavior will lead to certain consequences (i.e., costs and benefits) are the determinants of her attitude toward compliance behavior. Consistent with the RCT, we define these as *beliefs about overall assessment of consequences* of compliance and noncompliance. Next, consistent with rational decision making (Paternoster and Pogarsky 2009), we postulate that these beliefs about overall assessment of consequences are influenced by an employee's *beliefs about outcomes of compliance and noncompliance*. Beliefs about outcomes are beliefs that certain events will follow from performing (or not performing) a certain compliance behavior. Further, based on expectancy value theory (Fishbein and Ajzen 1975), we postulate how beliefs about overall assessment of consequences influence an employee's attitude toward compliance.

The research model also highlights the role of information security awareness in an employee's compliance or noncompliance with the ISP. The objective of creating information security awareness is to make employees cognizant of risks related to information security and to educate them about their roles and responsibilities concerning those risks. Based on the role of background factors in the TPB described by Ajzen and Albarracin (2007), we posit that information security awareness influences an employee's beliefs about outcomes. Further, based on Rogers (2003), we posit that information security awareness also directly influences an employee's attitude toward compliance with the ISP.

Figure 1 presents our conceptual model, and the following sections discuss the operationalization of constructs and the formation of our hypotheses.

Constructs from the Theory of Planned Behavior

Table 1 provides definitions of the TPB constructs in the model and their sources. In line with the existing literature, we posit that an employee's intention to comply with the requirements of the organization's ISP is associated with attitude toward compliance, normative beliefs, and self-efficacy. Self-efficacy is used instead of perceived behavioral control in our model because the latter essentially measures the same latent construct as self-efficacy (Fishbein 2007) and it originates from self-efficacy theory (Bandura 1977). Our use of self-efficacy is consistent with the literature (Fishbein and Cappella 2006; Fishbein and Yzer 2003; Giles et al. 2004; Yi and Hwang 2003).

Based on extant literature that has investigated relationships among TPB constructs, we form the following hypotheses in the context of ISP compliance:

Hypothesis 1: An employee's attitude toward compliance with the organization's ISP positively affects intention to comply with the requirements of the ISP.

Hypothesis 2: An employee's normative beliefs about compliance with the organization's ISP positively affects intention to comply with the requirements of the ISP.

Hypothesis 3: An employee's self-efficacy in complying with the organization's ISP positively affects intention to comply with the requirements of the ISP.

Beliefs about Overall Assessment of Consequences

While we argue that an employee's attitude toward compliance, subjective norms, and perceived behavioral control influence intention to comply with the ISP, we focus on understanding the antecedents of an employee's attitude toward compliance. The extant literature has argued that an employee's attitude toward performing a given behavior is related to his beliefs about behavior-related consequences (Ajzen 1991; Fishbein 2007; Fishbein and Ajzen 1975), and we use the RCT to identify those compliance-related conse-

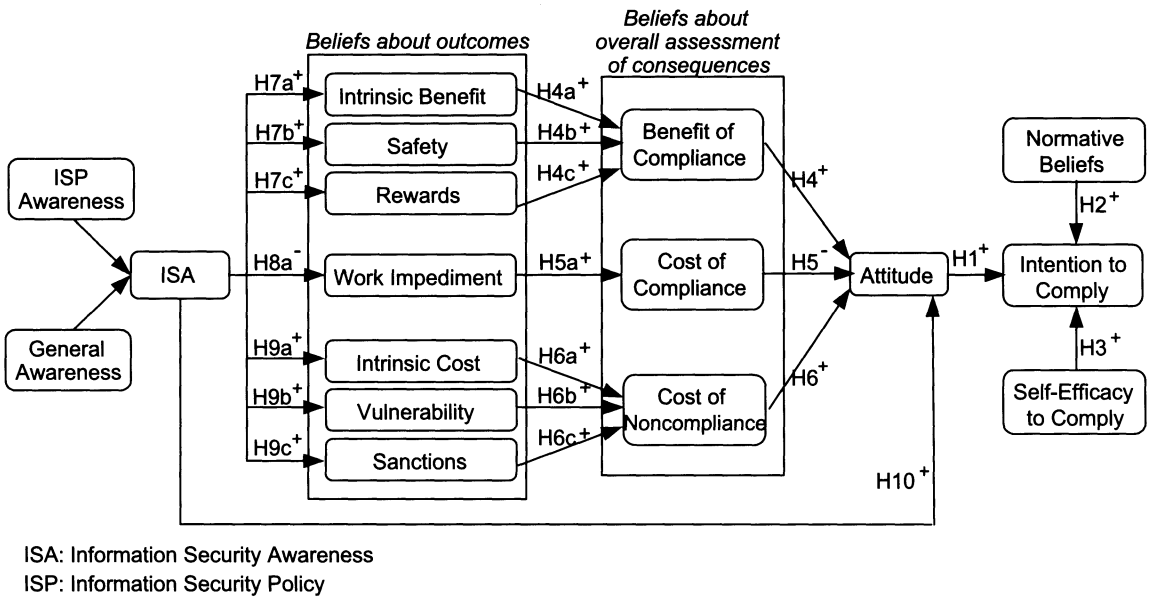

Figure 1. A Proposed Model of the Antecedents of ISP Compliance

Table 1. Definitions and Sources of Constructs Taken from the Theory of Planned Behavior

Construct	Definition	Sources
Attitude toward compliance with the ISP	The degree to which the performance of the compliance behavior is positively valued.	Theory of Planned Behavior (Ajzen 1991; Fishbein and Ajzen 1975)
Normative beliefs	An employee's perceived social pressure about compliance with the requirements of the ISP caused by behavioral expectations of such important referents as executives, colleagues, and managers.	Social Bond Theory (Hirschi 1969; Theory of Planned Behavior (Ajzen 1991; Fishbein and Ajzen 1975)
Self-efficacy to comply	An employee's judgment of personal skills, knowledge, or competency about fulfilling the requirements of the ISP.	Social Cognitive Theory (Bandura 1977, 1992, 1997)
Intention to comply	An employee's intention to protect the information and technology resources of the organization from potential security breaches.	Theory of Planned Behavior (Ajzen 1991; Fishbein and Ajzen 1975)

quences. RCT focuses on the consequences of alternative courses of action (McCarthy 2002; Paternoster and Pogarsky 2009). In our context, an employee's alternative courses are compliance and noncompliance. Since the ISP stipulates an employee's role and responsibilities in protecting the information and technology resources of the organization, compliance with the ISP is *not* a *passive* event. Thus, when an employee contemplates complying with what is prescribed in the ISP, he considers the costs or effort of doing so (for example, changing the password every other month). He also considers the benefits of complying (e.g., personal gain from complying with the ISP). On the other hand, while noncompliance is a passive event, an employee still has to consider its consequences. Therefore, in keeping with RCT, we posit that beliefs about overall assessment of consequences consist of three *key* distinct beliefs: (1) perceived benefit of compliance, (2) perceived cost of compliance, and (3) perceived cost of noncompliance. We define *perceived benefit of compliance* as the overall expected favorable consequences to an employee for complying with the requirements of the ISP. *Perceived cost of compliance* is the overall expected unfavorable consequences for complying, and *perceived cost of non-*

compliance is the overall expected unfavorable consequences for noncompliance.

Based on the TPB, we posit that an employee's beliefs about overall assessment of consequences will influence attitude toward complying with the requirements of the ISP. Drawing on the expectancy-value theory of attitude (Fishbein and Ajzen 1975), it is possible to determine whether an employee's beliefs about overall assessment of consequences will positively or negatively influence attitude toward compliance. According to the expectancy-value theory, an individual learns to favor behaviors believed to have desirable consequences and not to favor those with undesirable consequences. Accordingly, in our context, we argue that, if an employee perceives that benefits are derived from compliance or disadvantage from noncompliance, or that less effort is expended for compliance, a favorable attitude toward compliance is formed. This proposition is in line with the finding that compliance behavior is positively associated with the reaction to the behavior that is captured as personal benefit in the case of compliance with organizational policy and personal damage in the case of noncompliance (Tyler and Blader 2005). Further, in the security context, the more costly it is to perform security requirements in terms of time and effort, the less likely it is that employees will perform those requirements (PricewaterhouseCoopers 2008). Therefore, we propose the following hypotheses for the antecedents of the attitude toward compliance behavior.

Hypothesis 4: An employee's perceived benefit of compliance positively affects attitude toward complying with the requirements of the ISP.

Hypothesis 5: An employee's perceived cost of compliance negatively affects attitude toward complying with the requirements of the ISP.

Hypothesis 6: An employee's perceived cost of noncompliance positively affects attitude toward complying with the requirements of the ISP.

Drivers of Beliefs about Overall Assessment of Consequences

While we argue that beliefs about overall assessment of consequences are determinants of an employee's attitude toward compliance, we also need to describe how an employee forms those beliefs. Consistent with rational decision making, we posit that overall assessment of consequences that accrue to the individual from compliance (or noncompliance) is influenced by the individual's perception of potential outcomes associated with compliance and noncompliance. In our context, outcomes are events/things that are likely to happen after performing (or not performing) compliance behavior. Tolman (1932) argued that people learn "expectations," which are beliefs that an event is associated with (or follows from) some other event. In the context of compliance, for example, an employee might believe that, if he complies with the ISP, he will receive favorable personal mention in his performance assessment, so the event that follows compliance is "personal mention." Since the events that follow from performing or not performing compliance behavior have cost/benefit implications for the employee, his beliefs about such events will serve as a foundation or basis for his beliefs about overall assessment of consequences. Therefore, we define *beliefs about outcomes* as one's beliefs that some events will follow from performing (or not performing) the compliance behavior, so we postulate that an employee forms beliefs of overall assessment of compliance-related consequences by processing beliefs about outcomes.

While beliefs about outcomes characterize perceptions of future events that will develop as a result of compliance or noncompliance, beliefs about overall assessment of compliance-related consequences characterize individuals' aggregate *evaluations* of those events. Hence, beliefs about overall assessment of consequences are the results of a cognitive processing of beliefs about outcomes. The relationship between beliefs is recognized in the literature; for example, Fishbein and Ajzen (1975, ch. 5) described the inference process through which a belief is formed from other beliefs, and O'Grady (2002, p. 98) described an epistemic ascent process in which higher-level beliefs are inferentially justified by relating them to basic beliefs. By relating the belief about overall assessment of consequences to the beliefs about outcomes, our model provides guidance to information security practitioners about what outcomes can be manipulated to influence employees' compliance behavior.

In order to identify employees' outcome beliefs about compliance, we conducted an extensive review of relevant academic/practitioner literature. In most criminology literature, sanctions are viewed as an important instrument with which to deter inappropriate behaviors such as tax evasion (Klepper and Nagin 1989a, 1989b), juvenile delinquency (Paternoster 1989), corporate crime (Paternoster and Simpson 1996), disobedience of regulatory laws (Elffers et al. 2003), and general illegal conduct (Wright et al. 2004). Since individuals are believed to be amenable to sanction-based threats, the punishment-as-deterrence doctrine has been widely accepted by policymakers and the general public (Liska and Steven 1999). Similarly, the use of sanctions for not following rules has also been argued as important in corporate settings (Tyler and Blader 2005). Drawing on the extant

literature, we postulate that *sanction* is one of the outcome beliefs related to compliance.

The organization literature also highlights the importance of incentives as an instrument with which to encourage desired behavior (Huselid 1995), so we suggest that *rewards* are another outcome belief related to compliance. Further, while rewards and punishments provide external motivations, it is well recognized that employee's intrinsic values provide internal motivations to follow rules and regulations (Tyler and Blader 2005). As such, we posit that *intrinsic cost* (guilt, embarrassment, shame, and stress) is an outcome belief about noncompliance behavior and that *intrinsic benefit* (contentment, satisfaction, accomplishment, and fulfillment) is an outcome belief about performing the compliance behavior.

Previous studies have also found that ensuring information security may interfere with the primary or strategic goals of the business (Pahnila et al. 2007; West 2008), such that, if an employee complies with the ISP, her business functioning may be impeded since compliance requires her to perform certain activities. We postulate that *work impediment* is another outcome belief about performing the compliance behavior.

Beyond the outcome beliefs that were proposed based on the literature, our study identifies two other factors that an employee would consider in the context of ISP compliance: safety and vulnerability. If an employee chooses not to comply with the ISP, those resources that he uses remain vulnerable to information security risks, so *vulnerability* is an important state that follows from an employee's noncompliance with the ISP. However, if an employee performs what is prescribed in the ISP, he contributes to the protection of the organization's information and technology resources, so *safety* is an important state that follows from an employee's compliance with the ISP.

In summary, we conceptualize that there are seven outcome beliefs related to compliance that provide the foundation for beliefs about consequences: sanctions, rewards, intrinsic cost, intrinsic benefit, work impediment, vulnerability, and safety. In the following sections, we discuss each outcome belief related to compliance under the corresponding belief about overall assessment of consequences.

Outcome Beliefs Leading to Perceived Benefit of Compliance

Three outcome beliefs, *intrinsic benefit*, *safety of resources*, and *rewards,* describe events with positive valence that follow from performing compliance behavior. Drawing on the rational decision making process in which outcomes of a course of action contribute to an individual's assessment of costs and benefits of the course of action (Paternoster and Pogarsky 2009), we posit that these outcome beliefs are likely to lead to a perception of a benefit of compliance. This is consistent with the belief formation process in TPB. In our context, we define *intrinsic benefit* as an employee's positive feelings, such as satisfaction, accomplishment, and fulfillment, about compliance with the ISP. Deci and Ryan (1985) suggested that intrinsic motives help people justify their actions in terms of internal reasons, such as their own inspirations. Hence,

> *Hypothesis 4a: Intrinsic benefit that an employee gains as a result of compliance with the ISP is positively associated with perceived benefit of compliance.*

Safety of resources is defined as an employee's perception that her information and technology resources at work are safeguarded as a result of her compliance with the requirements of the ISP. We believe that employees are concerned with the safety of their information and technology resources at work, and West (2008) argued that employees will be favorably influenced to comply with the ISP when they observe that security mechanisms are working. Hence,

> *Hypothesis 4b: Safety of resources at work obtained from the employee's compliance with the ISP is positively associated with perceived benefits of compliance.*

Rewards are defined as tangible or intangible compensation that an organization gives to an employee in return for compliance with the requirements of the ISP. They may include pay raises, monetary or nonmonetary awards, personal mention and appreciation in oral or written assessment reports, promotions, and reputation. Although rewarding compliance behaviors may not yet be common in practice, recent studies have discussed the possible role of incentives in encouraging desirable behaviors in the context of information security (Boss and Kirsch 2007; Pahnila et al. 2007). Moreover, rewards as an incentive have been found to be a significant mechanism for changing behaviors in various contexts in education, organizational behavior, and psychology. Hence,

> *Hypothesis 4c: Rewards an employee is given for compliance with the ISP are positively associated with perceived benefit of compliance.*

Outcome Beliefs Leading to Perceived Cost of Compliance

The precautions that the ISP requires an employee to take in order to ensure information security may lead to perceptible

and often immediate negative consequences to the employee, such as inconvenience and additional effort. Since compliance behaviors require time and effort that could have been directed to other business activities, an employee often perceives compliance with the ISP as a barrier to productivity (Siponen and Vance 2010; Warkentin et al. 2004). In some cases, complying with security requirements may even conflict with the employee's primary tasks and result in sacrificing information security in return for accomplishing those primary tasks (Pahnila et al. 2007). In our context, *work impediment*, defined as a detriment to an employee's daily job-related tasks and activities resulting from compliance with the requirements of the ISP, represents an event with negative valence. Hence,

Hypothesis 5a: An employee's work impediment caused by compliance with the ISP is positively associated with perceived cost of compliance.

Outcome Beliefs Leading to Perceived Cost of Noncompliance

Studies based on deterrence theory (Kankanhalli et al. 2003; Pahnila et al. 2007; Straub 1990) have highlighted the importance of sanctions in deterring crimes related to computer security. Sanctions are believed to lead employees to perceive that there is a cost associated with not adhering to security-related rules and regulation. Yet, a sanction, however useful, is not the only event that can help employees form beliefs about the cost of not adhering to the rules and regulations (Siponen 2000). Three outcome beliefs—*intrinsic cost*, *vulnerability of resources*, and *sanctions*—describe events with negative valence that follow from not performing compliance behavior. *Intrinsic cost* is defined as an employee's negative feelings—such as stress, guilt, shame, and embarrassment—that are due to noncompliance with the ISP. Paternoster and Simpson (1993, 1996) argued that self-imposed punishment discourages employees from committing corporate crimes and that self-imposed punishment in the form of embarrassment and shame is an effective deterrent for corporate employees. They suggested that, while external instruments such as rewards and punishments can motivate employees to refrain from corporate crimes, self-imposed punishment is a highly potent source of social control for those who are likely to engage in it. Hence,

Hypothesis 6a: Intrinsic cost that an employee incurs as a result of noncompliance with the ISP is positively associated with perceived cost of noncompliance.

Vulnerability of resources is defined as an employee's perception that information and technology resources at work are exposed to security-related risks and threats as a consequence of noncompliance with the ISP. An important concept in information security, vulnerability is the condition of a missing or ineffectively administered safeguard or control that allows a threat to occur with a greater impact, frequency, or both (Peltier 2005). Since the employee uses organizational resources, noncompliance results in vulnerabilities to resources that she uses in the organization. Hence,

Hypothesis 6b: Vulnerability of resources at work caused by an employee's noncompliance with the ISP is positively associated with perceived cost of noncompliance.

Sanctions are defined as tangible or intangible penalties—such as demotions, loss of reputation, reprimands, monetary or nonmonetary penalties, and unfavorable personal mention in oral or written assessment reports—incurred by an employee for noncompliance with the requirements of the ISP. Sanctions are believed to be an effective instrument in dealing with crime. In the information security context, studies such as those by Straub (1990), Straub and Nance (1990), and Straub and Welke (1998) have focused specifically on the deterrent effects of sanctions in reducing criminal behavior. Hence,

Hypothesis 6c: Sanctions that an employee may face for not complying with the ISP are positively associated with perceived cost of noncompliance.

Information Security Awareness

Employees' information security awareness is an important part of an effective information security management program (Cavusoglu et al. 2009). In the current study, *information security awareness* (ISA) is defined as an employee's general knowledge about information security and his cognizance of the ISP of his organization. *General information security awareness* and *ISP awareness* are the key dimensions of ISA. *General information security awareness* is defined as an employee's overall knowledge and understanding of potential issues related to information security and their ramifications. Beyond general ISA, organizations have specific expectations of their employees that are reflected in the ISP. *ISP awareness* is defined as an employee's knowledge and understanding of the requirements prescribed in the organization's ISP and the aims of those requirements. This definition is consistent with the view that security awareness is a state in which employees are aware of and are ideally committed to the security objectives of their organizations (Siponen 2000). ISP awareness is different from general ISA; for example, one

may be generally aware that using passwords is a necessary precaution but may not know that the organization requires that passwords be changed periodically or that they need to be of a certain length and character composition. Hence, we conceptualize that ISA consists of general ISA, along with ISP awareness.

ISA can be viewed as knowing something about information security. One's awareness of information security may be built from direct life experiences, such as having once been harmed by a virus attack or penalized for not adhering to security rules and regulations, or it can be based on information obtained from external sources, such as newspapers, professional journals, organizational policy documents, and/or organizational workshops. The TPB argues that *background factors* which create differences among individuals (such as, demographics, dispositions, experience, and knowledge) can influence behavior *indirectly* by affecting or forming behavioral, normative, and control beliefs (Ajzen and Albarracin 2007). Hence, in the context of information security, we posit that an employee's ISA, conceptualized as a background factor, leads to the formation of his outcome beliefs associated with compliance behavior. Hence,

Hypothesis (7a/7b/7c): An employee's ISA is positively associated with (intrinsic benefit/safety of resources/ rewards).

Hypothesis 8a: An employee's ISA is negatively associated with work impediment.

Hypothesis (9a/9b/9c): An employee's ISA is positively associated with (intrinsic cost/vulnerability of resources/sanctions).

While the TPB is regarded as a theory of the proximal determinants of behavior (that is, beliefs, attitudes, subjective norms, and perceived behavioral control determine behavioral intention and behavior), other variables (e.g., individual differences) can have their impact via influencing the main components of the TPB (Conner and Armitage 1998). In fact, Fishbein (2008) argues that almost an infinite number of variables may directly or indirectly influence the performance (or nonperformance) of any behavior. Ajzen and Albarracin (2007) reiterate the same point as they argue that background factors can influence intentions and behavior by their effects on the proximal determinants. Hence, we can argue that ISA directly influences an employee's attitude toward compliance since the TPB does not preclude the possibility that a TPB construct is influenced by a non-TPB construct (Ajzen and Albarracin 2007; Conner and Armitage 1998; Fishbein 2008).

The direct influence of ISA can be explained by adapting Rogers' (2003) model of five stages in the innovation-decision process to information security. The first three constructs of Rogers' model show the causal chain of *knowledge* influencing *persuasion*, which, in turn, influences *decisions*. One can adapt this causal chain to our context by viewing ISA as knowledge, viewing attitude toward compliance as persuasion, and viewing intention to comply as a decision. Different types of knowledge can be significant depending on the context. Adapting from Rogers, knowledge of information security threats and safeguards (*awareness-knowledge*) and knowledge about what an employee is expected to do with regard to information security (*how-to-knowledge*) are important in the information security context. Knowledge of information security threats can be viewed as general information security awareness and knowledge about what employees are supposed to do can be viewed as specific information security awareness, which is ISP awareness. Because knowledge influences persuasion in the innovation-decision process and because Rogers specifically recognized that "the individual forms a favorable or unfavorable *attitude* toward the innovation" in order to describe persuasion (Rogers 2003, p. 271; emphasis added), ISA influences the employee's *attitude* toward compliance in our context. Finally, because the persuasion stage influences decisions (Rogers 2003), attitude toward compliance influences the decision to comply with the ISP. In our model, this decision is represented with the construct *intention to comply*. This approach is consistent with the argument that providing organizational security awareness is the most important factor in persuading employees to change their compliance actions (Siponen 2000). Hence,

Hypothesis 10: An employee's ISA positively affects attitude toward complying with the requirements of the ISP.

We included a number of control variables in the study related to the characteristics of the employee and the organization in order to account for the impacts of these characteristics on an employee's intention to comply with the ISP. We believe that the level of education and technology knowledge of an employee, as well as the size, the industry type, and information-intensity of the organization, may influence compliance behavior. First, we posit that the higher an employee's level of education and technology knowledge, the more the intend to comply with the ISP. Further, we predict that the larger and more information-intensive the organization, the more emphasis it will give to ISP compliance. Furthermore, since some industries, such as those in the financial sector, are known to be more vulnerable to security-related crimes (Schneier 2005), we expect that compliance may be higher in those industries.

Mediating Effect of Attitude

While there is a general agreement in the literature that beliefs influence behavioral intention through positive affect (Agarwal 2000), a few studies have questioned the *full* mediation role of attitude in the relationship between beliefs and behavioral intention (Bagozzi 1982; Davis 1993; Davis et al. 1989). In the TRA and TPB, attitude is posited to fully mediate the effects of beliefs on intention. However, alternative models provide empirical evidence for direct belief-intention links, without beliefs necessarily activating a positive affect (Triandis 1977). Davis et al. (1989) argued that, empirically, attitude did little to help elucidate the causal linkages between behavioral beliefs and intention and that attitude only partially mediated the effects of beliefs on intention, so the technology acceptance model does not include an attitude construct. In light of the nature of some of the findings in the literature that are not in line with the theoretical prescriptions of the TRA and TPB, it is important to investigate the role of attitude in our context.[2] Consistent with the TPB, we conceptualize that beliefs about the overall assessment of consequences will affect intention to comply through attitude toward compliance. That is, attitude is postulated to fully mediate the effects of an employee's assessment beliefs on intention to comply with the ISP. Further, Rogers (2003) argues that knowledge affects the adoption decision through persuasion. Accordingly, we conceptualize that attitude fully mediates the effects of an employee's ISA on intention to comply with the ISP. Hence, we propose the following hypotheses:

Hypothesis 11a: The effect of an employee's perceived benefit of compliance is fully mediated by attitude toward complying with the requirements of the ISP.

Hypothesis 11b: The effect of an employee's perceived cost of compliance is fully mediated by attitude toward complying with the requirements of the ISP.

Hypothesis 11c: The effect of an employee's perceived cost of noncompliance is fully mediated by attitude toward complying with the requirements of the ISP.

Hypothesis 11d: The effect of an employee's ISA is fully mediated by attitude toward complying with the requirements of the ISP.

[2]We would like to thank an anonymous reviewer for this suggestion.

Research Methodology

We used the survey method to test our model. We developed the initial survey instrument by first identifying and creating appropriate measurements based on a comprehensive literature review. Then the initial survey instrument was refined based on card-sorting exercises and exploratory data analysis from two small-scale pretests. Data was collected by administering the final survey instrument online.

Item Development

The process of item development began with an investigation of theoretical and empirical literature. When possible, the measurement items of the constructs were developed based on existing scales in extant literature that have been proven reliable; otherwise, we developed new measures by closely following our definitions of constructs in this study. Based on our conceptualization of ISA, we operationalized it as a second-order construct composed of two first-order constructs: general ISA and ISP awareness. Table 2 presents all of the constructs, along with the types, sources, and number of their measurement items. All constructs were measured *reflectively* with multiple items on seven-point Likert scales. The anchors of the measurement items are shown in Table 3.

Instrument Pretesting and Refinement

We asked for feedback on our initial measurement items from several IS faculty members and graduate students at our institution who had experience in survey research methods. We also obtained feedback from the participants in an academic workshop held in our faculty after we presented our preliminary research plans. Based on the feedback, several items were reviewed and modified. Next, the initial set of items and the predefined categories were submitted for a card-sorting test (Moore and Benbasat 1991). Eleven graduate students, none of whom had participated in the item review and all of whom had work experience, participated in two card-sorting exercises. Results of the first exercise indicated that some constructs should be merged and some of the construct names and definitions should be revised. At the end of the exercise, we asked the participants to report other factors that they might consider in the context of ISP compliance, and safety and vulnerability were identified at this stage. After we developed items for safety and vulnerability, the revised set of items and revised category definitions were submitted for another card-sorting exercise. The sorting resulted in satisfactory classification of items into predefined categories, so the items were deemed appropriate and were used in our pilot testing.

Table 2. Sources of Measurement Items

Construct	Type	Source	Items
Information Security Awareness	Reflective		
General ISA (subconstruct)	Reflective	Developed for this study	3
ISP Awareness (subconstruct)	Reflective	Developed for this study	3
Perceived Benefit of Compliance	Reflective	Developed for this study	4
Intrinsic Benefit	Reflective	Developed for this study	4
Safety of Resources	Reflective	Developed for this study	6
Rewards	Reflective	Boss and Kirsch 2007	4
Perceived Cost of Compliance	Reflective	Developed for this study	3
Work Impediment	Reflective	Developed for this study	4
Perceived Cost of Noncompliance	Reflective	Developed for this study	4
Intrinsic Cost	Reflective	Developed for this study	4
Vulnerability of Resources	Reflective	Developed for this study	5
Sanctions	Reflective	Boss and Kirsch 2007	4
Attitude	Reflective	Ajzen 1991	4
Normative Beliefs	Reflective	Ajzen 1991	3
Self-Efficacy to Comply	Reflective	Developed for this study	3
Intention to Comply	Reflective	Ajzen 1991	3

We next developed an online questionnaire, which was reviewed by 15 MBA students at our institution. Based on their feedback, we improved the appearance of the online survey. The items and scales were then subjected to two rounds of pilot testing, the first of which was conducted with 110 respondents drawn from panel members of a professional research company. Half of the respondents (55) completed the questionnaire and commented on the wording, length, and instructions, and reported concerns if they had any. The validity and reliability of the measurement items were investigated using the responses of 27 participants who had no missing answers. Based on our analysis of the data and the comments provided by the participants, the measurement items were further modified. After the revisions, we conducted another card-sorting exercise with six participants and, based on the results, the wording of some measurement items was modified in order to improve the clarity of items and to ensure that constructs were distinguishable. Subsequently, the second pilot test was conducted with another group of respondents (n = 147) drawn from panel members of a professional research company. In all, 71 respondents completed the questionnaire, although the responses of 27 participants were discarded because of missing answers. Based on the analysis of data and participant feedback, all of the measurement items were deemed adequate and ready to be used in the main survey.

Data Collection: Sample and Procedure

The proposed model (Figure 1) was tested using the items presented in Table 3. We collected data by administering a web-based questionnaire survey, which was deemed appropriate since our target respondents were employees who use the IT resources of their organizations and had access to the Internet. A professional market research company located in the United States provided a nationwide sample of their panel members.

We asked the research company to contact participants who are employed by a diverse set of organizations. The research company sent an e-mail invitation to 3,150 of its panel members to create a diverse sample population. The identities of participants were kept confidential by the research company. In return for their participation, participants were given a points-based incentive redeemable for prizes. According to the statistics of the server hosting the online survey, 1,098 panel members accepted the invitation and, among them, 928 individuals opted to participate in the survey by accepting the consent agreement. Those panel members were first asked questions regarding their demographics (see Table A2 in Appendix A), followed by a set of questions to eliminate the participants who worked in organizations without an explicitly written ISP and/or who were unaware of the require-

Table 3. Measurement Items and Item Loadings

Items	Dimensions/Questions	Scale	Mean	STD	Loading
ITC	**Intention to comply with the ISP**				
	I intend to comply with the requirements of the ISP of my organization in the future.	a	6.532	0.915	0.974
	I intend to protect information and technology resources according to the requirements of the ISP of my organization in the future.	a	6.573	0.908	0.975
	I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information and technology in the future.	a	6.550	0.926	0.982
GISA	**General information security awareness**				
	Overall, I am aware of the potential security threats and their negative consequences.	b	6.106	1.062	0.920
	I have sufficient knowledge about the cost of potential security problems.	b	5.739	1.370	0.844
	I understand the concerns regarding information security and the risks they pose in general.	b	6.304	0.962	0.977
ISPA	**ISP Awareness**				
	I know the rules and regulations prescribed by the ISP of my organization.	b	5.890	1.130	0.952
	I understand the rules and regulations prescribed by the ISP of my organization.	b	6.000	1.100	0.949
	I know my responsibilities as prescribed in the ISP to enhance the IS security of my organization.	b	5.719	1.355	0.918
A	**Attitude**				
	To me, complying with the requirements of the ISP is _____.				
	unnecessary...necessary	c	6.278	1.132	0.892
	unbeneficial...beneficial	c	6.131	1.275	0.936
	unimportant...important	c	6.246	1.269	0.928
	useless...useful	c	6.054	1.397	0.923
NB	**Normative Beliefs**				
	_____ think that I should comply with the requirements of the ISP.				
	My colleagues	a	5.966	1.358	0.851
	My executives	a	6.457	1.055	0.927
	My managers	a	6.351	1.183	0.945
SE-C	**Self Efficacy to Comply**				
	I have the necessary _____ to fulfill the requirements of the ISP.				
	skills	d	5.987	1.170	0.969
	knowledge	d	5.955	1.181	0.977
	competencies	d	6.002	1.143	0.974
CC	**Perceived Cost of Compliance**				
	Complying with the requirements of the ISP is _____ for me.				
	time consuming	b	3.125	1.878	0.933
	burdensome	b	2.966	1.840	0.945
	costly	b	2.543	1.787	0.902

Table 3. Measurement Items and Item Loadings (Continued)

Items	Dimensions/Questions	Scale	Mean	STD	Loading
WI	**Work Impediment**				
	Complying with the requirements of the ISP _____.				
	holds me back from doing my actual work	b	2.655	1.776	0.959
	slows down my response time to my colleagues, customers, managers, etc.	b	2.745	1.798	0.959
	hinders my productivity at work	b	2.692	1.794	0.971
	impedes my efficiency at work	b	2.733	1.812	0.971
IB	**Intrinsic Benefit**				
	My compliance with the requirements of the ISP would make me feel _____.				
	content	b	5.530	1.437	0.945
	satisfied	b	5.558	1.452	0.959
	accomplished	b	5.455	1.544	0.958
	fulfilled	b	5.291	1.595	0.936
R	**Rewards**				
	_____ I comply with the requirements of the ISP.				
	My pay raises and/or promotions depend on whether	b	3.093	2.053	0.872
	I will receive personal mention in oral or written assessment reports if	b	2.847	2.017	0.909
	I will be given monetary or non-monetary rewards if	b	2.364	1.909	0.907
	My receiving tangible or intangible rewards are tied to whether	b	2.504	1.923	0.925
SR	**Safety of Resources**				
	Complying with the requirements if the ISP _____ my resources at work.				
	would strengthen the security controls over	b	5.259	1.650	0.869
	would enhance safety of	b	5.478	1.531	0.926
	would improve protection of	b	5.532	1.531	0.936
	would eliminate the risk of damage to	b	5.409	1.590	0.919
	would prevent potential security related risks concerning	b	5.616	1.459	0.929
	would lead to less security related problems associated with	b	5.509	1.532	0.922
BC	**Perceived Benefit of Compliance**				
	My compliance with the requirements of the ISP would _____.				
	be favorable to me	b	5.435	1.687	0.947
	result in benefits to me	b	4.858	1.921	0.975
	create advantages for me	b	4.647	1.965	0.963
	provide gains to me	b	4.522	1.969	0.957
S	**Sanctions**				
	_____ I don't comply with the requirements of the ISP.				
	I will probably be punished or demoted if	b	5.114	1.780	0.907
	I will receive personal reprimand in oral or written assessment reports if	b	5.125	1.823	0.907
	I will incur monetary or non-monetary penalties if	b	3.657	2.266	0.784
	My facing tangible or intangible sanctions is tied to whether	b	4.446	2.104	0.898

Table 3. Measurement Items and Item Loadings (Continued)

Items	Dimensions/Questions	Scale	Mean	STD	Loading
VR	**Vulnerability of Resources**				
	If I don't comply with the requirements of the ISP, my resources _____.				
	will be at risk	b	5.526	1.638	0.938
	will be vulnerable	b	5.580	1.620	0.955
	can be exploited	b	5.543	1.639	0.948
	can be misused	b	5.608	1.591	0.956
	can be compromised	b	5.694	1.553	0.958
CNC	**Perceived Cost of Noncompliance**				
	My noncompliance with the requirements of the ISP would _____.				
	be harmful to me	b	5.002	1.903	0.925
	impact me negatively	b	5.287	1.806	0.951
	create disadvantages for me	b	5.138	1.893	0.964
	generate losses for me	b	4.881	1.993	0.924

Scale: a 1 = Strongly Disagree — 7 = Strongly Agree
b 1 = Not at All — 7 = Very Much
c 1 = Extremely; 2 = Quite; 3 = Slightly; 4 = Neither; 5 = Slightly; 6 = Quite; 7 = Extremely
d. 1 = Almost Never;2 = Very Rarely; 3 = Rarely; 4 = Occasionally; 5 = Frequently; 6 = Very Frequently; 7 = Almost Always

ments of their organization's ISP (see Table A1 in Appendix A). The participants were not told that we would be using these questions as exclusion criteria. In total, 258 of the participants met the exclusion criteria (i.e., on a seven-point Likert scale, those who selected completely unaware (1), or unaware (2)) were excluded from answering the rest of the survey. Of the remaining 670 respondents, 175 were later eliminated because of incomplete answers, and 31 were eliminated after data runs indicated unreliable responses (i.e., answers exhibiting certain unlikely patterns, such as all 7 or alternating 6 and 7). In the end, a sample of 464 usable questionnaires was included in the data analysis for an effective response rate of 42 percent. A possible nonresponse bias was addressed by using the procedure recommended by Armstrong and Overton (1977); no significant differences were found between the first third and the last third of the respondents' data, so we concluded that nonresponse bias was not an issue in this study.

Of the 464 respondents in the final sample, 52 percent were female, and 36 percent were in the 36 to 45 age range. The average length of computer usage was 17.6 years, and the average usage of the Internet was 12.2 years. The total of respondents that reported working for information-intensive companies was 28 percent. The sample was quite evenly distributed in terms of the responsibilities of the respondents, and the annual sales revenue and size of the companies they worked for (sample demographics are presented in Table A2 in Appendix A.). The data collected represents a diverse employee population since it includes employees with different backgrounds who work in a large number of diverse organizations. We believe that one of the strengths of our study is the heterogeneity of our data sample, which is likely to reduce the potential bias arising from the influence of unique policy matters or organizational or cultural factors that can be present when dealing with a limited number of organizations.

Data Analyses and Results

Assessment of Measurement Validation

The measurement and the structural models were tested using structural equation modeling. The component-based partial least squares (PLS) approach was used to evaluate the psychometric properties of measurement scales and to test the research hypotheses proposed in this study. The PLS, as a component-based approach, is appropriate for this study because the PLS focuses on prediction of data and is well suited for exploratory models and theory development. The Smart-PLS software package (version 2.0.M3) (Ringle et al. 2005) was used for the estimations. The measurement quality of reflective constructs was assessed by examining the convergent validity, individual item reliability, composite

reliability, and discriminant validity of the measurement model (Barclay et al. 1995). Since the measures of all constructs had adequate reliability and validity assessments, all of the measurement items of these constructs were kept for testing the structural model. Subsequently, we estimated the structural model to test the research hypotheses.

Table 3 shows the questionnaire items, as well as the descriptive statistics of all the constructs, including means, standard deviations, and the level of each item's contribution to the overall factor.

First, to ensure the individual item reliability and convergent validity of constructs, we examined factor loadings of individual measures on their respective underlying constructs, as well as the average variance extracted (AVE). All of the measurement item loadings on respective constructs were above the recommended minimum value of 0.707, indicating that at least 50 percent of the variance was shared with the construct (Chin 1998) (see Table 3). The AVE values for all reflective constructs were greater than the minimum recommended value of 0.50 (see Table B1 in Appendix B), indicating that the items satisfied the convergent validity.

Second, to ensure the discriminant validity of constructs in the research model, the square root of the average variance extracted (AVE) for each construct was compared with the other correlation scores in the correlation matrix. The square root of the AVE for each construct in the model, as reported in the diagonal of the correlation of constructs matrix in Table B1 in Appendix B, was larger than the corresponding off-diagonal correlations of the constructs to their latent variables. We also performed confirmatory factor analysis and examined the cross loadings of the items on other constructs and found that, as recommended, all of the measurement item loadings on the intended constructs were above 0.78 and were at least 0.1 less on their loadings on other constructs (Gefen and Straub 2005) (See Table B2 in Appendix B).

To confirm the scale reliability and internal consistency of the constructs in the research model, we calculated the composite reliability (Fornell and Larcker 1981) and Cronbach's alpha scores. A composite reliability and Cronbach's alpha values of 0.7 or greater is considered acceptable (Gefen et al. 2000; Nunnally and Bernstein 1994); as reported in Table B1, the composite reliability values for all of the constructs in the research model were greater than 0.92 and Cronbach's alpha values were greater than 0.88, demonstrating that all constructs had adequate reliability assessment scores. All of the construct measures were deemed to be reflective as their indicators satisfy the recommended criteria specified in Jarvis et al. (2003) and Petter et al. (2007). We also tested dimensionality of the constructs included in the study. The dimensionality of each construct was examined by performing a series of confirmatory factor analyses, each using a different extraction method (principal component analysis, principal axis factoring, and maximum likelihood). We found that every construct of the study is one dimensional.

If the independent and dependent variables in a study are not obtained from different sources and are not measured in different contexts, common method bias can be a potential threat to the study (Podsakoff et al. 2003). We considered the statistical approach suggested by Podsakoff et al. (2003) and applied Liang et al.'s (2007) method to determine whether common method bias was a concern. As suggested, we created the PLS model and included a common method factor that links to all of the single-indicator constructs that were converted from observed indicators. Because the method factor loadings were insignificant and the indicators' substantive variances were substantially greater than their method variances (Table B3), we concluded that common method bias is unlikely to be a serious concern (Williams et al. 2003).

Structural Model Testing

As proposed in our research methodology, the measurement of the structural model was estimated using the PLS approach to structural equation modeling. The PLS algorithm and the bootstrapping re-sampling method with 464 cases and 1,000 re-samples were used to estimate the structural model. The results of the model estimation, including standardized path coefficients, significance of the paths based on a two-tailed t-test, and the amount of variances explained (R^2), are presented in Figure 2.

Based on the significant path coefficients (Figure 2), all hypotheses were supported ($p < 0.01$). Approximately 35.2 percent of the variance was explained for intention to comply. While TBP constructs explain 34.5 percent of the variance, the control variables explain only an additional 0.7 percent. In the variance explained by the TBP constructs, attitude accounts for 36.7 percent of the variance explained in intention to comply, normative belief accounts for 40.6 percent, and self-efficacy for 22.8 percent.

Since we conceptualized ISA as a second-order construct formed by general ISA and ISP awareness, we looked at the weights of these subdimensions and found that they are significant ($t_1 = 0.51$ and $t_2 = 0.58$), suggesting that each subdimension significantly contributes to the underlying overall factor. Although details are not shown here, we conducted a pseudo F-test (Gefen et al. 2000; Mathieson et al. 2001),

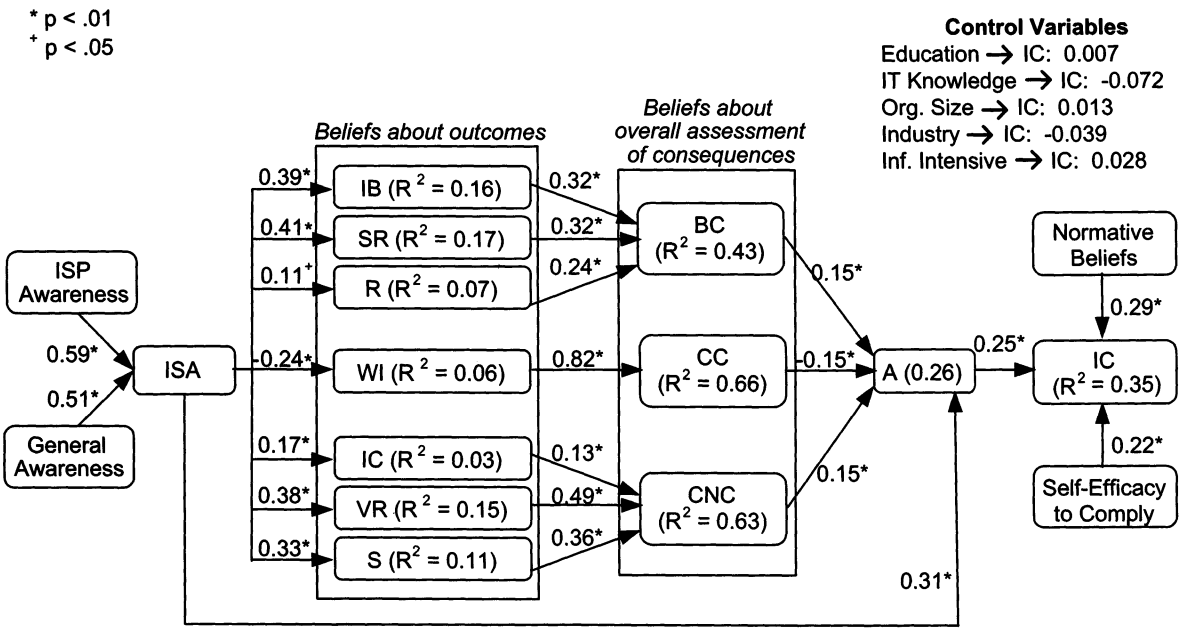

Figure 2. The Results of the Structural Model Testing

with the result that the contributions of all factors were significant in explaining the variance in an employee's intention to comply.

We conducted the analysis suggested by Baron and Kenny (1986) to test the mediating effect of attitude on intention to comply. Consistent with our theoretical basis, our research model hypothesizes that assessment beliefs and ISA influence intention completely through attitude (full mediation effect of attitude). However, we do not rule out the possibility that the effect of assessment beliefs and ISA may be partially mediated through attitude (partial mediation effect of attitude). Therefore, we performed the mediation analysis to determine if full or partial mediation effects are present. The results of our mediation analysis are presented in Table 4. The coefficients in column 1 for each independent variable (IV) are significant, satisfying initial conditions to test mediation role of attitude. Following Baron and Kenny, when Path a and Path b are controlled, the coefficient of Path c for the IV is reduced (i.e., the coefficient of Path c in column 2 is smaller than that of column 1) for every IV. This suggests that attitude toward compliance either fully or partially mediates the effects of each IV on intention. If Path c becomes statistically insignificant and is close to zero, the analysis suggests the existence of a full mediation. According to the test results, while attitude fully mediates the effects of benefit of compliance and cost of noncompliance on intention to comply with the ISP, it partially mediates the effects of cost of compliance and ISA on intention to comply with the ISP.

Discussion, Implications, and Future Research

Discussion of the Findings

This study identifies three broad classes of beliefs about overall assessment of compliance-related consequences–benefit of compliance, cost of compliance, and cost of noncompliance–to provide theoretical explanations for the antecedents of an employee's attitude toward compliance with the ISP. This attitude positively influences an employee's intention to comply with the ISP. Furthermore, information security awareness (ISA), which is formed by general ISA and ISP awareness, influences an employee's attitude to comply with the ISP directly, as well as indirectly, through the employee's compliance-related outcome beliefs. Overall, we found strong support for our theoretical model. Based on data collected from 464 employees who had some familiarity with the requirements of their organizations' ISPs, all of the hypotheses were supported.

Table 4. Results of Mediation Analysis

	IV: BC		IV: CC		IV: CNC		IV: ISA	
	1	2	1	2	1	2	1	2
Path a	.335*	.336*	-2.14*	-2.11*	.336*	.334*	.426*	.425*
Path b	.481*	.455*	.481*	.433*	.481*	.447*	.481*	.301*
Path c	**.237***	**.070**	**-0.316***	**-.215***	**.247***	**0.77**	**.557***	**.414***
	Full Mediation		**Partial Mediation**		**Full Mediation**		**Partial Mediation**	

*p < .01

Note 1: **Path a:** IV → Attitude; **Path b:** Attitude → Intention; **Path c:** IV → Intention.

Note 2: **Column (1)** represents path coefficients that are estimated for Paths a, b, and c *independently* for the given IV. **Column (2)** represents path coefficients that are estimated *simultaneously* for all of the paths (i.e., Paths a, b, and c) for the given IV.

Note 3: If Path c in Column (1) is significant while it is not in Column (2), then Attitude **fully mediates** the impact of IV on Intention. If both Path c coefficients in Columns (1) and (2) are significant, while Column (1) is larger than Column (2), then Attitude **partially mediates** the impact of IV on Intention.

As hypothesized, we found that the effects of attitude, normative beliefs, and self-efficacy to comply on an employee's intention to comply are significant. Thus, hypotheses 1, 2, and 3 were fully supported.

Consistent with the proposed research model, we found that three beliefs about overall assessment of consequences, along with ISA, exerted significant influence on an employee's attitude toward compliance. Hence, hypotheses 4, 5, and 6 were fully supported. Our findings also indicated that the beliefs about overall assessment of consequences had almost equal influence on an employee's attitude toward compliance, suggesting that no single belief has a predominant effect on attitude. Furthermore, the outcome beliefs that were postulated as constituting the beliefs about overall assessment of consequences were found to exert strong influence on the level of their corresponding constructs.

As we hypothesized, an employee's ISA has a direct significant influence on attitude toward compliance and plays a major role in shaping outcome beliefs. ISA has a strong influence on attitude toward compliance, confirming the existing literature that has highlighted the importance of ISA. As hypothesized, ISA influences work impediment negatively and the other six outcome beliefs positively.

We found that the impacts of benefit of compliance and cost of noncompliance on intention to comply with the ISP are fully mediated by an employee's attitude toward compliance. Hence, hypotheses 11a and 11c are supported. However, the impacts of cost of compliance and ISA on intention to comply with the ISP are partially mediated by an employee's attitude toward compliance. Hence, hypotheses 11b and 11d are not supported. Our mediation analysis reveals that attitude plays a significant role by either partially or fully mediating the impacts of assessment beliefs and ISA in our research model.

We found no significant impact of control variables—level of education and technology knowledge, the size of organization, industry type of organization, or information intensity of organization—on an employee's intention to comply with the ISP. Industry type also had no significant impact on explaining an employee's intention to comply. Although some industries, such as those in the financial sector, are known to be more vulnerable to security-related crimes (Schneier 2005), our results suggest that compliance behavior can be better explained by factors rooted in our theoretical model (an employee's beliefs and ISA), than by the organization's industry.

Theoretical Contributions

Our study makes important theoretical contributions to the emerging body of knowledge about the behavioral and organizational issues of information security. First, the extant literature has investigated factors rooted in deterrence theory and protection motivation theory to explain the ISP compliance but, to the best of our knowledge, this is the first study that, drawing on RCT, offers a theoretical explanation and empirical support for the impact of an employee's beliefs about the consequences of compliance and noncompliance with the ISP on attitude toward compliance with the ISP. We showed that attitude toward compliance can be traced back to cognitive beliefs, which are modeled in two levels. Our results indicate that beliefs about overall assessment of consequences are the immediate antecedents of attitude. Further, we identified seven outcome beliefs that provide the founda-

tion for an employee's beliefs about overall assessment of consequences, so our results suggest that factors that motivate employees to comply with the ISP extend beyond instruments such as sanctions and rewards.

Second, while the extant literature has discussed the roles of rewards and sanctions, which drive the benefits of compliance and the costs of noncompliance in our model, this study is the first to investigate empirically the role of the cost of compliance in the context of an employee's compliance with the ISP. We show that the impact of the cost of compliance is as strong as the impacts of the benefit of compliance and the cost of noncompliance, thereby highlighting the importance of this construct in the context of information security.

Our study is, to our best knowledge, the first to investigate the role of ISA on shaping an employee's attitude and compliance-related outcome beliefs. Our findings show that ISA exerts a significantly positive influence on outcome beliefs, which influence the employee's beliefs about the benefit of compliance and the cost of noncompliance, while ISA exerts a significantly negative influence on the outcome belief that leads to perceptions of the cost of compliance.

Finally, given some of the prior findings related to the mediation role of attitude and the prescriptions made in the literature about the non-inclusion of attitude in adoption models (e.g., in the widely applied TAM), we thought it important to investigate the role of attitude in the ISP compliance context. We conclude that attitude plays a key role in explaining the relationships between assessment beliefs and intention as well as between ISA and intention; hence, we recommend that it be included in the theoretical model of ISP compliance as a mediator.

Practical Implications

The results of our study offer important practical implications for information security practitioners. Our findings provide evidence of the significant impact of motivational factors other than rewards and sanctions that reinforce an employee's compliance behavior. Since outcome beliefs play an important role in shaping an employee's consequence beliefs, which are shown to positively influence attitudes toward compliance, as a practical implication, we suggest that information security awareness programs should be designed to emphasize these outcome beliefs; security practitioners should design their information security awareness programs so employees' beliefs about intrinsic cost and benefit, safety, and vulnerability are reinforced. Further, our results indicate that an employee's perception that compliance impedes job-related functions can be lessened by ISA. Thus, ensuring information security awareness can directly and indirectly alter employees' belief sets about compliance with the ISP. This implies that creating a security-aware culture within the organization will improve information security. Therefore, we suggest that organizations create appropriate training and security awareness programs that ensure employees' ISA, as well as their self-efficacy about compliance.

Further, since an employee's compliance-related outcome beliefs are shown to be significant in affecting cost-benefit assessments, these beliefs can be shaped by external interventions designed to influence these perceptions and affect/improve compliance behavior. Therefore, we believe that practitioners can use external instruments to complement their security training and awareness programs.

Unlike Boss and Kirsch (2007), who found that rewards do not significantly contribute to the mandatoriness of ISP compliance, we found that rewards exert a significant impact on an employee's perception of the benefit of compliance. While rewards may not lead employees to believe that ISP requirements are mandatory, they can still be used to motivate employees to comply. Based on our finding that rewards influence perceptions of the benefit of compliance, which, in turn, affects employees' attitude toward compliance, employees should know that they will be rewarded for their pro-security behaviors.

Further, since employees perceive work impediments to be costly, organizations should allocate a certain amount of employees' time to be used to fulfill the requirements of the ISP so compliance efforts do not compete with daily job-related activities. This would definitely lessen their perception that compliance impedes their daily job functions and motivate them to comply with their ISPs. Similarly, practitioners should strive to simplify the security procedures that employees are required to perform and provide adequate training to their employees so employees will not perceive the requirements and procedures specified by the ISP as burdensome.

Another finding of the study is that an employee's self-efficacy about compliance positively influences intention to comply. This finding suggests that organizations should provide training to their employees to ensure that they know what they need to do to comply with information security rules and regulations.

Limitations and Future Research Directions

One limitation of this study relates to the selection of participants. At the beginning of the survey questionnaire, each respondent was asked whether his organization had established an ISP and whether the respondent was aware of the ISP's requirements, and we excluded from the survey those who worked in an organization without a written ISP or who were not aware of the requirements of their organizations' ISPs. The selection of participants who were aware of information security requirements may have created a favorability bias in the responses. However, the hypotheses in this study could not be examined with participants who were completely unaware of the existence or the requirements of their ISPs, or who did not work under the rules of ISPs.

Another limitation is that the data were collected in a cross-sectional manner and, as a result, even though the directions of the hypotheses were based on solid theories, the statistical analysis may have provided an indication of correlation, rather than causation. For example, while ISA initially leads to the formation of an employee's attitude toward compliance, over time, as a more favorable attitude is developed, more effort can be expended to become even more aware of information security related issues and requirements. To unveil the causal relations, future research can collect data across time by surveying the same individuals at different time instances.

The perception-based measure for ISA we used and our decision to measure the compliance intention instead of actual compliance behavior can also be viewed as limitations. Employees' levels of awareness on general information security and the requirements of the ISPs can be measured objectively by exhaustive lists of questions, but this approach was not practical for this study because we collected the data from employees who worked in a variety of organizations. Similarly, it would be possible to measure the actual compliance behavior by observing the actual compliance-related activities performed by the employees, but this was not practical with such a large and diverse sample. For the sake of the generalizability of our results, we opted out of objective measurements of the ISP and actual compliance behavior. Case studies about ISP compliance that focus on employees from one or a few organizations would also be useful future research since such case studies could provide an opportunity to measure employees' ISA and their actual compliance with the requirements of their organizations' ISP objectively.

Since we found that ISA plays a key role in employees' compliance behavior, another fruitful research direction is to examine the dimensions of ISA. In particular, identifying the factors that lead to ISA would be an important contribution to academics, since there is a gap in the literature in this direction. Such research would also be useful to practitioners, since they can use those factors to formulate their ISA programs.

Researchers could also investigate the kinds of ISA that exist at different levels of the organizational hierarchy, since different aspects of awareness may be more effective in altering perceptions for employees at different levels. For example, while customer representatives might comprehend the consequences of an information security issue better in terms of how customer relationships are affected, the sales managers might do so better in terms of lost sales. These kinds of differences among employees can be used to tailor security awareness programs to employees at different levels of the organization.

Respondents to this study self-reported their intention to comply with the requirements of the ISP, and it is possible that some concealed their true intentions because they perceived noncompliance as socially undesirable (Trevino 1992). One way to alleviate this limitation is to use scenarios (Siponen and Vance 2010) that provide a richer description of a hypothetical employee and to indirectly ask about the beliefs of the study participant through the situation of the employee in the hypothetical scenario. Another limitation of the study may be that it captures compliance at a high level of abstraction. Use of scenarios can help reveal the differences in an employee's intentions to comply with specific rules and regulations, since scenarios can provide detailed explanations about specific policies (i.e., password policy, Internet use policy, remote access policy, and so on). Hence, future research should investigate employee compliance behavior in regard to these specific policies by providing detailed scenarios.

Our study investigates the importance of an employee's beliefs concerning the consequences of performing or not performing compliance requirements in shaping attitude toward compliance. One possible direction for future research is to investigate whether there are other beliefs that play roles in shaping employee attitude toward compliance and to compare them to the beliefs about overall assessment of consequences identified in this study in terms of their contributions to attitude. A similar research direction is to investigate whether there are other outcome beliefs that play a role in shaping beliefs about overall assessment of consequences and to compare them to the outcome beliefs identified in this study in terms of their contributions to beliefs about overall assessment of consequences.

Future research can also trace an employee's subjective norms and perceived behavioral control to these constructs' underlying foundations of beliefs. Although an employee's subjective norms and perceived behavior control are shown to influence compliance intention, our research model traces only attitude to its underlying foundation of compliance-related beliefs. However, we do not mean to suggest that an employee's subjective norm and perceived behavior control are not important; the antecedents of these constructs in the context of information security deserve further attention.

In this paper, sanctions are conceptualized as various forms of penalties that the organization imposes on an employee for noncompliance with the ISP. Deterrence literature has argued that severity, certainty, and celerity are important factors in determining how much deterrence a sanction can provide. Since we did not consider these factors, future research could investigate how severity, certainty, and celerity of sanctions influence an employee's perception of the cost of non-compliance.

Recently, Myyry et al. (2009) argued that moral reasoning and the values of an employee influence compliance with information security rules. A fruitful research direction would be to investigate the joint role of consequence-based motivations and morality/values on employee compliance behavior.

Finally, this study focused on individual factors leading to compliance or noncompliance, but future research might investigate the impact of organizational factors such as organizational sanctions (e.g., losing customers, facing litigation, incurring financial detriments) or rewards (e.g., increasing trustworthiness, reputation, and good image) on an employee's attitude toward compliance. Another extension of the research along this line can incorporate both individual factors and institutional factors to explain compliance intention and to study the relative importance of those factors in shaping an employee's intention to comply with the ISP.

Acknowledgments

We would like to thank the senior editor, the associate editor, and the four anonymous reviewers for their constructive feedback during the review process. This research was supported by a grant from the Social Sciences and Humanities Research Council of Canada.

References

Agarwal, R. 2000. "Individual Acceptance of Information Technologies," in *Framing the Domains of IT Management: Projecting the Future...Through the Past*, R. W. Zmud (ed.), Cincinnnati, OH: Pinnaflex Education Resources, pp. 85-104.

AIRC. 2008. *Attack Intelligence Research Center Annual Threat Report: 2008 Overview and 2009 Predictions*, Attack Intelligence Research Center, Alladin Knowledge Systems, Belcamp, MD (available online at http://www.aladdin.com/pdf/airc/AIRC-Annual-Threat-Report2008.pdf).

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179-211.

Ajzen, I., and Albarracin, D. 2007. "Chapter 1: Predicting and Changing Behavior: A Reasoned Action Approach," in *Prediction and Change of Health Behavior: Applying the Reasoned Action Approach,* I. Ajzen, D. Albarracin, and R. Hornik (eds.), Hillsdale, NJ: Lawrence Erlbaum & Associates, pp. 3-21.

Ajzen, I., and Fishbein, M. 1980. *Understanding Attitudes and Predicting Social Behavior*, Englewood Cliffs, NJ: Prentice-Hall.

Armstrong, S. J., and Overton, T. S. 1977. "Estimating Non-Response Bias in Mail Surveys," *Journal of Marketing Research* (14:3), pp. 396-402.

Bagozzi, R. P. 1982. "A Field Investigation of Causal Relations among Cognitions, Affect, Intentions, and Behavior," *Journal of Marketing Research* (19:4), pp. 562-583.

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

Bandura, A. 1992. "Self-efficacy," in *Encyclopedia of Human Behavior,* V. S. Ramachandran (ed.), New York: Academic Press, Volume 4, pp. 71-81.

Bandura, A. 1997. *Self-Efficacy: The Exercise of Control,* New York: W. H. Freeman.

Barclay, D., Higgins, C., and Thompson, R. 1995. "The Partial Least Squares (PLS) Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration," *Technology Studies* (2:2), pp. 285-309.

Baron, R. M., and Kenny, D. A. 1986. "The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic and Statistical Considerations," *Journal of Personality and Social Psychology* (51:6), pp. 1173-1182.

Becker, G. S. 1968. "Crime and Punishment: And Economic Approach," *The Journal of Political Economy* (76:2), pp. 169-217.

Becker, G. S. 1993. *Human Capital: A Theoretical and Empirical Analysis with Special Reference to Education* (3rd ed.), Chicago: The University of Chicago Press.

Boss, S. R., and Kirsch, L. J. 2007. "The Last Line of Defense: Motivating Employees to Follow Corporate Security Guideliness," in *Proceedings of the 28th International Conference on Information Systems*, Montreal, December 9-12.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. "If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18:2), pp. 151-164.

Brancheau, J. C., Janz, B. D., and Wetherbe, J. C. 1996. "Key Issues in Information Systems Management: 1994-95 SIM Delphi Results," *MIS Quarterly* (20:2), pp. 225-242.

Cavusoglu, H., Cavusoglu, H., and Raghunathan, S. 2004. "Economics of IT Security Management: Four Improvements to Current Security Practices," *Communications of the Association for Information Systems* (14), pp. 65-75.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., and Benbasat, I. 2009. "Information Security Control Resources in Organizations: A Multidimensional View and Their Key Drivers," working paper, Sauder School of Business, University of British Columbia.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004a. "A Model for Evaluating IT Security Investments," *Communications of the ACM* (47:7), pp. 87-92.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004b. "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers," *International Journal of Electronic Commerce* (9:1), pp. 69-104.

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

Conner, M., and Armitage, C. J. 1998. "Extending the Theory of Planned Behaviour: A Review and Avenues for Further Research," *Journal of Applied Social Psychology* (28:15), pp. 1429-1464.

Damasio, A. R. 1994. *Descartes' Error: Emotion, Reason, and the Human Brain*, New York: Putnam.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Davis, F. D. 1993. "User Acceptance of Information Technology: System Characteristics, User Perceptions and Behavioral Impacts," *International Journal of Man-Machine Studies* (38:3), pp. 475-487.

Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. 1989. "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science* (35:8), pp. 982-1003.

Deci, E. L., and Ryan, R. M. 1985. *Intrinsic Motivation and Self-determination in Human Behavior,* New York: Plenum.

Dhillon, G. 1997. *Managing Information System Security*, London: Macmillan.

Dhillon, G., and Backhouse, J. 2001. "Current Directions in Information Security Research: Toward Socio-Organizational Perspectives," *Information Systems Journal* (11:2), pp. 127-153.

Dinev, T., Goo, J., Hu, Q., and Nam, K. 2008. "User Behavior Towards Protective Information Technologies: The Role of National Cultural Differences," *Information Systems Journal* (19:4), pp. 391-412.

Doherty, N. F., and Fulford, H. 2006. "Aligning the Information Security Policy with the Strategic Information Systems Plan," *Computers and Security* (25:1), pp. 55-63.

Durgin, M. 2007. "Understanding the Importance of and Implementing Internal Security Measures," SANS Institute Reading Room (https://www2.sans.org/reading_room/whitepapers/policyissues/1901.php).

Elffers, H., Heijden, P., and Hezemans, M. 2003. "Explaining Regulatory Noncompliance: A Survey Study of Rule Transgression for Two Dutch Instrumental Laws, Applying the Randomized Response Method," *Journal of Quantitative Criminology* (19, 4), pp. 409-439.

Elster, J. 1999. *Alchemies of the Mind: Rationality and the Emotions*, New York: Cambridge University Press.

Ernst & Young. 2008. "Moving Beyond Compliance: Ernst & Young's 2008 Global Information Security Survey" (available online at http://www.ey.com/Publication/vwLUAssets/2008_Global_Information_Security_Survey_english/$FILE/2008_GISS_ingles.pdf).

Fishbein, M. 2007. "A Reasoned Action Approach: Some Issues, Questions, and Clarifications," in *Prediction and Change of Health Behavior: Applying the Reasoned Action Approach*, I. Ajzen, D. Albarracin, and R, Hornik (eds.), Hillsdale, NJ: Lawrence Erlbaum & Associates, pp. 281-296.

Fishbein, M. 2008. "A Reasoned Action Approach to Health Promotion," *Medical Decision Making* (28:6), pp. 834-844.

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

Fishbein, M., and Cappella, J. N. 2006. "The Role of Theory in Developing Effective Health Communications," *Journal of Communication* (56), pp. 1-17.

Fishbein, M., and Yzer, M. C. 2003. "Using Theory to Design Effective Health Behavior Interventions," *Communication Theory* (13:2), pp. 164-183.

Fornell, C., and Larcker, D. F. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1), pp. 39-50.

Furnell, S. M., Gennatou, M., and Dowland, P. S. 2002. "A Prototype Tool for Information Security Awareness and Training," *Logistics Information Management* (15:5), pp. 352-357.

Gefen, D., and Straub, D. 2005. "A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example," *Communications of the AIS* (16), pp. 91-109.

Gefen, D., Straub, D. W., and Boudreau, M. C. 2000. "Structural Equation Modeling And Regression: Guidelines For Research Practice," *Communications of the AIS* (4), pp. 1-77.

Giles, M., McClenahan, C., Cairns, E., and Mallet, J. 2004. "An Application of the Theory of Planned Behavior to Blood Donation: The Importance of Self-efficacy," *Health Education Research* (19:4), pp. 380-391.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R. 2006. "CSI/FBI Computer Crime and Security Survey," Computer Security Institute (available online at http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf).

Hentea, M. 2005. "A Perspective on Achieving Information Security Awareness," in *The Information Universe: Issues in Informing Science and Information,* E. Cohen (ed.), Santa Rosa, CA: Informing Science Institute, Volume 2, pp. 169-178.

Herath, T., and Rao, H. G. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

Hirschi, T. 1969. *Causes of Delinquency,* Berkeley, CA: University of California Press.

Huselid, M. A. 1995. "The Impact of Human Resource Management Practices on Turnover, Productivity, and Corporate Financial Performance," *Academy of Management Journal* (38:3), pp. 635-872.

Jarvis, C. B., MacKenzie, S. B., and Podsakoff, P. M. 2003. "A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research," *Journal of Consumer Research* (30:2), pp. 199-218.

Kankanhalli, A., Teo, H.-H., Tan, B. C., and Wei, K.-K. 2003. "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management* (23:2), pp. 139-154.

Klepper, S., and Nagin, D. 1989a. "Tax Compliance and Perceptions of the Risks of Detection and Criminal Prosecution," *Law and Society Review* (23:2), pp. 209-240.

Klepper, S., and Nagin, D. 1989b. "The Deterrent Effect of Perceived Certainty and Severity of Punishment Revisited," *Criminology* (27:4), pp. 721-746.

Lee, J., and Lee, Y. 2002. "A Holistic Model of Computer Abuse Within Organizations," *Information Management and Computer Security* (10:2/3), pp. 57-63.

Lee, S. M., Lee, S. G., and Yoo, S. 2003. "An Integrative Model of Computer Abuse based on Social Control and General Deterrence Theories," *Information and Management* (41:6), pp. 707-718.

Liang, H., Saraf, N., Hu, Q., Xue, Y. 2007. "Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management," *MIS Quarterly* (31:1), pp. 59-87.

Liska, A. E., and Steven F. M. 1999. *Perspectives on Crime and Deviance* (3rd ed.), Upper Saddle River, NJ: Prentice Hall.

Lohmeyer, D. F., McCrory, J., and Pogreb, S. 2002. "Managing Information Security," *The McKinsey Quarterly, Special Edition: Risk and Resilience* (2), pp. 12-16.

Mathieson, K., Peacock, E., and Chin, W. 2001. "Extending the Technology Acceptance Model: The Influence of Perceived User Resources," *The Database for Advances in Information Systems* (32:3), pp. 86-112.

McCarthy, B. 2002. "New Economics of Sociological Criminology," *Annual Review of Sociology* (28:1), pp. 417-442.

Mitnick, K. D., and Simon, W. L. 2002. *The Art of Deception: Controlling the Human Element of Security,* Indianapolis, IN: Wiley Publishing, Inc..

Moore, G. C., and Benbasat, I. 1991. "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation," *Information Systems Research* (2:3), pp. 192-222.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study," *European Journal of Information Systems* (18), pp. 126-139.

Neumann, P. G. 1999. "Risks of Insiders," *Comunications of the ACM* (42:12), pp. 160.

Nunnally, J. C., and Bernstein, I. 1994. *Psychometric Theory* (3rd ed.), New York: McGraw Hill.

O'Grady, P. 2002. *Relativism*, Montreal: McGill-Queen's University Press.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior towards IS Security Policy Compliance," in *Proceedings of the 40th Hawaii International Conference on System Sciences,* Los Alamitos, CA: IEEE Computer Society Press, pp. 156-166.

Paternoster, R. 1989. "Decisions to Participate in and Desist from Four Types of Common Delinquency: Deterrence and the Rational Choice Perspective," *Law and Society Review* (23:1), pp. 7-40.

Paternoster, R., and Pogarsky, G. 2009. "Rational Choice, Agency and Thoughtfully Reflective Decision Making: The Short and Long-Term Consequences of Making Good Choices," *Journal of Quantitative Criminology* (25:2), pp. 103-127.

Paternoster, R., and Simpson, S. 1993. "A Rational Choice Theory of Corporate Crime," in *Routine Activity and Rational Choice: Advances in Criminological Theory*, R. V. Clarke and M. Felson (eds.), New Brunswick, NJ: Transaction Books, pp. 37-58.

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

Peltier, T. R. 2004. *Information Security Policies and Procedures: A Practitioner's Reference*, Boca Raton, FL: Auerbach Publications.

Peltier, T. R. 2005. *Information Security Risk Analysis* (2nd ed.), Boca Raton, FL: CRC Press.

Petter, S., Straub, D., and Rai, A. 2007. "Specifying Formative Constructs in Information Systems Research," *MIS Quarterly* (31:4), pp. 623-656.

Podsakoff, P., MacKenzie, S., Lee, J., and Podsakoff, N. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88:5), pp. 879-903.

PricewaterhouseCoopers. 2008. "Employee Behaviour Key to Improving Information Security, New Survey Finds," June 23, (http://www.ukmediacentre.pwc.com/content/detail.aspx?releaseid=2672&newsareaid=2).

Puhakainen, P. 2006. "A Design Theory for Information Security Awareness," working paper, Faculty of Science, University of Oulu, Finland.

Ransbotham, S., and Mitra, S. 2009. "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise," *Information Systems Research* (20:1), pp.121-139.

Ringle, C. M., Wende, S., and Will, A. 2005. *SmartPLS* (Release 2.0 (beta)), University of Hamburg, Hamburg, Germany (http://www.smartpls.de).

Rogers, E. M. 2003. *Diffusion of Innovations* (5th ed.), New York: Free Press.

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

Rogers, R. W. 1983. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation," in *Social Psychology: A Source Book*, B. L. Cacioppo and L. L. Petty (eds.), London: Guildford Press, pp. 153-176.

Schneier, B. 2005. "Attack Trends: Beyond the Numbers," report by Counterpane Internet Security Inc.

Siponen, M. T. 2000. "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management and Computer Security* (8:1), pp. 31-41.

Siponen, M. T. 2001. "Five Dimensions of Information Security Awareness," *Computers and Society* (31:2), pp. 24-29.

Siponen, M. T. 2005. "An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice," *European Journal of Information Systems* (14:3), pp. 303-315.

Siponen, M. T., and Iivari, J. 2006. "Six Design Theories for IS Security Policies and Guidelines," *Journal of the Association for Information Systems* (7:7), pp. 445-472.

Siponen, M. T., Pahnila, S., and Mahmood, A. 2007. "Employees' Adherence to Information Security Policies: An Empirical Study," in *New Approaches for Security, Privacy and Trust in Complex Environments*, H. Venter, M. Eloff, L. Labuschagne, J. Eloff, and R. von Solms, Boston: Springer, pp. 133-144.

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

Siponen, M. T., and Willison, R. 2007. "A Critical Assessment of IS Security Research Between 1990-2004," in *Proceedings of the 15th European Conference on Information Systems*, St. Gallen, Switzerland, June 7-9, pp. 1551-1559.

Soo Hoo, K. J. 2000. "How Much Is Enough: A Risk Management Approach to Computer Security," working paper, Center for International Security and Cooperation, Stanford University (available online at http://cisac.stanford.edu/publications/how_much_is_enough__a_riskmanagement_approach_to_computer_security/).

Stajkovic, A. D., and Luthans, F. 1997. "A Meta-Analysis of the Effects of Organizational Behavior Modification on Task Performance, 1975-95," *Academy of Management Journal* (40:5), pp. 1122-1149.

Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. 2005. "Analysis of End User Security Behaviors," *Computers and Security* (24:2), pp. 124-133.

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

Straub, D. W. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), pp. 441-469.

Straub, D. W., and Nance, W. D. 1990. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly* (14:1), pp. 45-60.

Straub, D. W., and Welke, R. J. 1998. "Coping With Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), pp. 441-469.

Symantec. 2009. *Symantec Internet Security Threat Report: Trends for 2008*, Symantec Corporation, Cupertino, CA(available online at http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiv_04-2009.en-us.pdf).

Thomson, M. E., and von Solms, R. 1998. "Information Security Awareness: Educating Your Users Effectively," *Information Management and Computer Security* (6:4), pp. 167-173.

Tolman, E. C. 1932. *Purposive Behavior in Animals and Men*, New York: Appleton Century-Crofts.

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

Triandis, H. C. 1977. *Interpersonal Behavior,* Monterey, CA: Brooks/Cole.

Tyler, T. R., and Blader, S. L. 2005. "Can Businesses Effectively Regulate Employee Conduct? The Antecedents of Rule Following in Work Settings," *Academy of Management Journal* (48:6), pp. 1143-1158.

Vardi, Y., and Weitz, E. 2004. *Misbehavior in Organizations: Theory, Research, and Management*, Hillsdale, NJ: Lawrence Erlbaum Associates.

Warkentin, M., Davis, K., and Bekkering, E. 2004. "Introducing the Check-Off Password System (COPS): An Advancement in User Authentication Methods and Information Security," *Journal of Organizational and End User Computing* (16:3), pp. 41-58.

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

West, R. 2008. "The Psychology of Security," *Communications of the ACM* (51:4), pp. 34-40.

Whitman, M. E. 2008. "Chapter 6: Security Policy: From Design to Maintenance," in *Information Security: Policy, Processes, and Practices,* D. W. Straub, S. Goodman, and R. Baskerville (eds.), Armonk, NY: M. E. Sharpe, pp. 123-151.

Whitman, M. E., Townsend, A. M., and Aalberts, R. J. 2001. "Information Systems Security and the Need for Policy," in *Information Security Management – Global Challenges in the Next Millennium,* G. Dhillon, London: Idea Group, pp. 9-18.

Williams, L. J., Edwards, J. R., and Vandenberg, R. J. 2003. "Recent Advances in Causal Modeling Methods for Organizational and Management Research," *Journal of Management* (29:6), pp. 903-936.

Willison, R. 2006. "Understanding the Perpetration of Employee Computer Crime in the Organisational Context," *Information and Organization* (16:4), pp. 304-324.

Wixom, B. H., and Todd, P. A. 2005. "Theoretical Integration of User Satisfaction and Technology Acceptance," *Information Systems Research* (16:1), pp. 85-102.

Woon, I. M., and Kankanhalli, A. 2003. "Measuring Factors that Infleunce Information Security Effectiveness in Organizations," in *Proceedings of the 13th Annual Workshop on Information Technologies and Systems*, Seattle, WA, December 12-13, pp. 19-24.

Wright, B. R. E., Caspi, A., Moffitt, T. E., and Paternoster, R. 2004. "Does the Perceived Risk of Punishment Deter Criminally Prone Individuals? Rational Choice, Self-Control, and Crime," *Journal of Research in Crime and Delinquency* (41:2), pp. 180-213.

Yi, M. Y., and Hwang, Y. 2003. "Predicting the Use of Web-Based Information Systems: Self-Efficacy, Enjoyment, Learning Goal Orientation, and the Technology Acceptance Model," *International Journal of Human-Computer Studies* (59:4), pp. 431-449.

About the Authors

Burcu Bulgurcu is a Ph.D. student in Management Information Systems at the Sauder School of Business, University of British Columbia, Vancouver, Canada. She received her M.Sc. degrees in

MIS from the Sauder School and in Information Systems from Informatics Institute, Middle East Technical University, Turkey. Her current research focuses on behavioral and organizational aspects of information privacy and security. She is particularly interested in understanding technology users' information privacy and security protection behaviors and developing necessary tools to help them protect their information assets.

Hasan Cavusoglu received his Ph.D. degree in Management Science with a specialization in MIS from the University of Texas at Dallas. He is currently an associate professor of Management Information Systems at the Sauder School of Business, University of British Columbia. His current research interests are economics of information systems, economics of information security, and management of technology and information. He has published in *Management Science*, *Information Systems Research*, *IEEE Transactions on Engineering Management*, *IEEE Transactions on Software Engineering*, *Information Technology and Management*, and *Communications of the AIS*.

Izak Benbasat is a Fellow of the Royal Society of Canada and a CANADA Research Chair in Information Technology Management at the Sauder School of Business, University of British Columbia. He received his Ph.D. in Management Information Systems from the University of Minnesota. He currently serves on the editorial boards of *Information Systems Journal* and *Journal of Management Information Systems*. He was editor-in-chief of *Information Systems Research*, editor of the Information Systems and Decision Support Systems Department of *Management Science*, and a senior editor of *MIS Quarterly*. The general theme of his research is improving the communication between information technology, management, and IT users.