IS Security Policy Violations:
A Rational Choice Perspective

Anthony Vance, Brigham Young University, USA

Mikko Siponen, University of Oulu, Finland

ABSTRACT

Employee violations of IS security policies are reported as a key concern for organizations. Although behavioral research on IS security has received increasing attention from IS scholars, little empirical research has examined this problem. To address this research gap, the authors test a model based on Rational Choice Theory (RCT)—a prominent criminological theory not yet applied in IS—which explains, in terms of a utilitarian calculation, an individual's decision to commit a violation. Empirical results show that the effects of informal sanctions, moral beliefs, and perceived benefits convincingly explain employee IS security policy violations, while the effect of formal sanctions is insignificant. Based on these findings, the authors discuss several implications for research and practice.

Keywords: *Deterrence Theory, IS Security, IS Security Compliance, IS Security Policies, Rational Choice Theory*

Encouraging employees to comply with IS security policies is a major challenge for organizations. This is because no IS security practice or technique, no matter how effective, can be ultimately successful if improperly implemented by its users (Aytes & Conolly, 2004; Ernst & Young, 2008; Puhakainen, 2006). Employees who are aware of their organization's IS security policies and yet willfully disregard or violate them pose a particular challenge, given that the existence of IS security policies and security awareness programs have little effect on these employees (Siponen, 2000; Stanton, Stam, Mastrangelo, & Jolton, 2005). Despite the clear need to understand and respond to this problem, little IS research has investigated employee violations of IS security policies.

Although IS scholars have examined IS security-related behavioral issues such as computer "abuse" and "misuse" (D'Arcy, Hovav, & Galletta, 2009; Lee, Lee, & Yoo, 2004; Straub, 1990), this body of research is not explicitly designed to measure the factors affecting intentional violations of IS security policies. For this reason, an understanding of computer abuse might not help to clarify a situation in which employees are aware of their organization's IS security policies, yet willfully choose to violate them.

Furthermore, IS research on computer abuse in particular has focused on the cost of a utilitarian deterrence approach: formal sanctions. In turn, the perceived benefits of norm

DOI: 10.4018/joeuc.2012010102

breaking, informal sanctions, and moral evaluations have received little or no attention from IS security scholars, even though recent studies in the field of Criminology have highlighted the important roles these constructs play in decisions to violate. More importantly, these perceived benefits have received no attention in the study of employee IS security policy violations. As a result, there is a need for studies that apply (a) informal sanctions, (b) moral evaluations, and (c) benefits in the area of IS security policy violation.

To address this need, we believe that Rational Choice Theory (RCT)—a prominent criminological theory that has not yet been applied to IS—is especially useful for studying employee IS security policy violations. This theory can be seen as a modern extension of classical deterrence theory, which holds that violations can be reduced by imposing sanctions that are certain and severe. However, RCT goes beyond deterrence theory by incorporating individuals' perceptions of benefits of violations and informal sanctions as well as espoused moral beliefs. According to RCT, individuals perform a mental utilitarian calculation involving each of these factors when making a decision to commit a violation. An empirical test given in two organizations strongly supports our model, showing that perceived benefits, moral beliefs, and informal sanctions have a significant impact on employees' intentions to violate IS security policies. However, contrary to the findings of several studies examining computer abuse, the effect of formal sanctions is not significant, suggesting that the contexts of computer abuse on the one hand and intentional violations of IS security policies on the other may be appreciably different.

The remainder of this paper is organized as follows: the second section contrasts previous work on IS security behavior in general with the specific problem of IS security policy violations. The third section develops our theoretical model and hypotheses, and the fourth section presents the empirical results. The fifth section discusses the implications of these findings for research and practice. Finally, the conclusion summarizes the key findings and contributions of the paper.

Previous Research on IS Security Behavior and Compliance

Previous research in the area of IS security behavior in an organizational context can be divided into three areas: (1) IS security awareness and training, (2) computer abuse, and (3) information security policy violations. In this section, we show below that while many contributions have been made in the first two areas, comparatively little research has directly addressed the problem of intentional violations of IS security policies. Next, we show that although the first two streams of research have made important contributions to IS security research, they have addressed distinctly different research questions than those examining factors that lead to deliberate violations of IS security policies.

IS Security Awareness and Training

Research on IS security awareness and training programs (Lafleur, 1992; McLean, 1992; Puhakainen, 2006; Siponen, 2000; Telders, 1991; Thomson & von Solms, 1998; Vroom & von Solms, 2002) offers important insights into how employees' awareness of IS security policies and guidelines can be increased (Lafleur, 1992; McLean, 1992; Thomson & von Solms, 1998; Vroom & von Solms, 2002). Such research also offers insights into how employees can be motivated to comply with such policies (Puhakainen, 2006; Siponen & Iivari, 2006). Contributions to this research stream generally comprise conceptual frameworks (Lafleur, 1992; McLean, 1992; Siponen, 2000; Telders, 1991; Thomson & von Solms, 1998; Vroom & von Solms, 2002) and qualitative studies on the effect of IS security education on employees' IS

security policy compliance. Although valuable, these studies do not examine the behavior of employees who are aware of IS security policies but who deliberately choose to violate them (Aytes & Connolly, 2003).

Computer Abuse

Computer abuse has received considerable attention in the area of IS security. This research stream can be traced back to the research of Parker (1976), who first studied and coined the term "computer abuse."[1] This term has been consistently defined in the field of information systems as "the unauthorized and deliberate misuse of assets of the local organizational information system by individuals," including the misuse of hardware, software, data, and computer services (Straub, 1990, p. 257; Harrington, 1996; D'Arcy et al., 2009).

While Parker (1976) did not explicitly apply theory in his work, subsequent studies on computer abuse have generally applied criminological theories, particularly deterrence theory (Grasmick & Bryjak, 1980). The first to do so was Straub (1990), who applied deterrence theory (involving the certainty and severity of formal sanctions) to examine whether information security investments deter computer abuse. He applied formal sanctions by linking the number of reported incidents to various information security countermeasures and found that these countermeasures reduced the number of computer abuse incidents within organizations. While Straub (1990) did not measure computer abuse at the level of individuals, subsequent studies have addressed this point. Harrington (1996) found support that codes of ethics act as deterrents because they induce a fear of punishment. Lee et al. (2004) studied whether a number of deterrents, such as security policies and awareness programs, deter computer abuse. They found that social norms and involvement lead to increased computer abuse. Finally, D'Arcy et al.'s (2009) study of IS misuse extended the classical deterrence theory to include preceding factors such as computer awareness and education as well as the formulation of security policies. They found that user awareness of IS security policies, IS security training, computer monitoring, and the severity of formal sanctions deters IS misuse.

Information Security Policy Violations

The third related research stream of IS security behavior within the organizational context is research on noncompliance with IS security policies. Studies in this stream assume that it is of utmost importance to measure and study violations of IS security policies within organizations. Emphasis is put on this simply because security managers are interested in explaining employees' noncompliance with security policies as well as in what can be done to promote compliance based on this information. Practically speaking, if the action in question is not a violation of the IS security policies of the organization, why should security managers of the organization care?

Studies in this research stream include Bulgurcu, Cavusoglu, and Benbasat (2010); Chan, Woon, and Kankanhalli (2005); Hagen (2009); Herath and Rao (2009a, 2009b); Myyry, Siponen, Pahnila, Vartiainen, and Vance (2009); Ng, Kankanhalli, and Xu (2009); Pahnila, Siponen, and Mahmood (2007); Siponen et al. (2006); Siponen, Mahmood, and Pahnila (2010); Siponen and Vance (2010); and Young (2010). Common to all of these studies is that they propose different models to explain or predict employees' adherence to IS security policies. These studies have applied different theories, from Protection Motivation Theory (Herath & Rao, 2009; Pahnila et al., 2007; Siponen et al., 2007, 2009) to health belief models (Ng et al., 2006) and theories of moral judgment (Myyry et al., 2009).

Although research has been conducted on expected costs in the form of sanctions in the area of computer abuse (D'Arcy et al., 2009; Straub, 1990) and information security policies (Herath & Rao, 2009a, 2009b; Siponen et al., 2010), an unanswered question remains regarding the effect of expected benefits on

individuals' decisions to violate information security policies. This is an important question because abuses by organizational members in other contexts, such as white-collar crime, have been found to be strongly predicted by expected benefits (Paternoster & Simpson, 1996). By examining the impact of expected benefits within the context of information security policies, organizations will gain an understanding of how to better guard against and discourage violations of information security policies.

Theoretical Framework

In order to better understand the impact of expected benefits on IS security policy violations, we use Rational Choice Theory as the basis for our theoretical model (Paternoster & Simpson, 1993, 1996). Although RCT is a prominent theory in criminology (Cao, 2004), it has not yet been used in the field of Information Systems. RCT explains individuals' decisions to commit crimes as utilitarian calculations based on perceived benefits and both formal and informal sanctions. Although commonly applied to explain criminal behavior, RCT is designed to be "sufficiently general to cover all violations" (Becker, 1968, p. 170) and, therefore, is also applicable to the study of violations of organizational IS security policies.

Rational Choice Theory adopts a classical stance in Criminology in which individuals weigh costs and benefits when deciding whether to commit a crime. This view can be traced back to Bentham (1748–1832), to Beccaria (1738–1794), and, later, to Becker's (1968) Economic Theory of Crime. In this view, criminal behavior is rational and goal-oriented, based on an assessment of the perceived costs, sanctions, and benefits (Cao, 2004). To be more precise, an individual will commit a criminal act if the expected benefits are greater than the associated costs. Although some have criticized RCT for assuming a fully rational criminal (Cornish & Clarke, 1986), proponents of RCT hold that offenders' decisions to commit crimes are subjective assessments and "are often objectively wrong, due to individuals' bounded rationality" (Becker & Mehlkop, 2006, p. 197).

Because of its emphasis on a deliberate, calculative decision process, it has been theorized that RCT explains white-collar crime well (Paternoster & Simpson, 1996). In fact, a review of empirical studies using RCT found that it explains white-collar crimes better than it explains street-level crimes (Cao, 2004). For this same reason, and because RCT has been found to be effective in the corporate context, we expect it to be well suited for explaining intentional IS security policy violations, which also involve a deliberate violation of organizational norms.

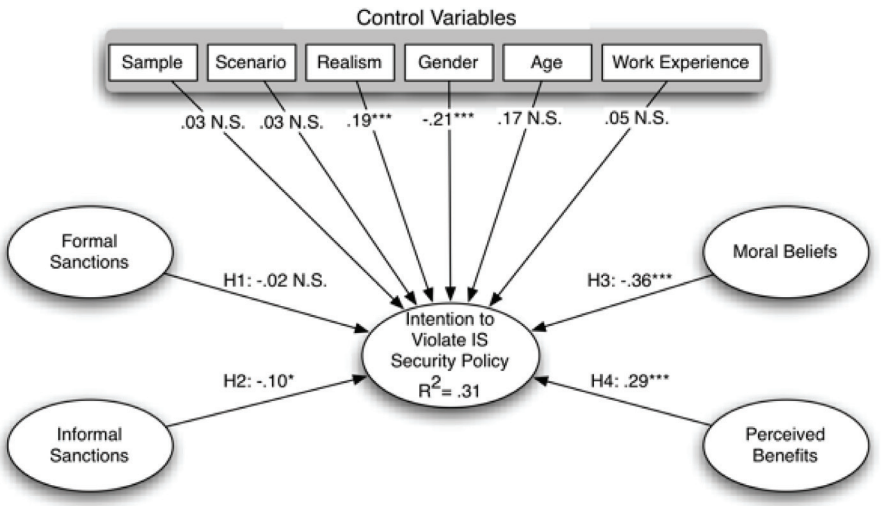
Research Model and Hypotheses

In order to better explain IS security policy violations in situations where employees are aware of the IS security policies, we developed a model, depicted in Figure 1, based on RCT. Consistent with RCT, our model includes disincentives (i.e., sanctions) as well as incentives (i.e., perceived benefits) for violating IS security policies. Further, the rational choice model suggests both informal sanctions (i.e., unstated social penalties) and formal sanctions (explicit penalties for specific forms of misconduct). Additionally, recent developments of RCT have incorporated the effect of moral beliefs into the utilitarian calculations that comprise considering an act. Accordingly, our model, too, incorporates moral beliefs. Each of these elements and their associated hypotheses are discussed below.

Formal Sanctions

Formal sanctions are explicit penalties imposed for specific forms of misconduct and are the mainstay of deterrence theory, which RCT extends. According to deterrence theory, undesirable behaviors can be deterred by imposing formal sanctions. The more forceful or effective the sanction, the more undesirable behaviors will be deterred. Further, the severity and certainty of sanctions are important factors that determine their effectiveness. In research on computer abuse, Straub (1990) found that sanctions deterred users from committing computer abuse. D'Arcy et al. (2009) similarly found that

Figure 1. Rational choice model of IS security policy violations



the severity of formal sanctions had a significant effect on users' intentions to commit computer abuses. Given this theoretical and empirical support, we hypothesize the following:

H1: Formal sanctions negatively affect intention to violate IS security policy.

Informal Sanctions

In the last several decades, criminologists and social psychologists have extended deterrence theory to include "non-legal costs" (Pratt & Cullen, 2000, p. 367), such as informal sanctions (Piquero & Tibbetts, 1996). Informal sanctions are unstated social penalties for undesirable behavior, such as the disapproval of friends or peers (Paternoster & Simpson, 1996), social censure (Bachman, Paternoster, & Ward, 1992), or embarrassment (Grasmick & Bursik, 1990). Empirical findings regarding the effects of informal sanctions present mixed results, depending on the type of offense involved. Paternoster and Simpson (1996) found that informal sanctions had a significant effect on intentions to commit white-collar crime, whereas the effect of formal sanctions was insignificant. Hence, we hypothesize that:

H2: Informal sanctions negatively affect intention to violate IS security policy.

Moral Beliefs

Some commentators have suggested that traditional views of RCT do not take into account the moral beliefs of individuals (Bachman et al., 1992). They maintain that offenders may refrain from offending not because they fear sanctions but simply because they evaluate the offense as morally wrong. Bachman et al. (1992) review prior research concerning the role of moral beliefs and highlight two possibilities in this respect. First, moral belief may be so strong that other factors are irrelevant. This view is consistent with the ethical doctrine of universal prescriptivism (Hare, 1981), which explains that moral beliefs override other concerns, such as assessments of potential benefits and sanctions. On the other hand, when moral beliefs are not strongly held, formal sanctions are then needed (Bachman et al., 1992).

Of these components, Paternoster and Simpson (1996) note that moral inhibitions were found to be the strongest predictor of corporate crime. This finding with respect to moral inhibitions is supported by various studies

(Bachman et al., 1992; Elis & Simpson, 1995). For example, Bachman et al. (1992) found that sexual assault was inhibited not only by formal sanctions but also by the perceived immorality of the act. In fact, Bachman et al. (1992) reported that formal sanctions were irrelevant for offenses regarded to be morally wrong.

Moral beliefs are relevant to the context of information security because choices regarding information security generally and security policies specifically involve a moral component (Myyry et al., 2009; Stahl, 2004). For this reason, we expect moral beliefs to influence noncompliance with IS security policies.

H3: Moral beliefs negatively affect intention to violate IS security policy.

Perceived Benefits

Rational Choice Theory predicts that perceived benefits positively affect decisions to commit violations. Empirical studies have found wide support for this relationship. Perceived benefits might be intrinsic, such as the thrill or excitement experienced by some when committing a crime (Wood, Gove, Wilson, & Cochran, 1997), or extrinsic, such as money (Ducan, Lafree, & Piquero, 2005). In the area of information security policy compliance, time saving has been identified as a major incentive to violate policies. Puhakainen (2006) found in a series of qualitative interviews that because information security policies were perceived to slow down work by the addition of procedures, interviewees perceived saving time as a clear benefit of avoiding IS security policies. Hence, we hypothesize that:

H4: Perceived benefits positively affect intention to violate IS security policy.

Method

Scenario Method

To empirically examine IS security policy violations, we employed a hypothetical scenario method, which presents respondents with a hypothetical situation followed by a question regarding the likelihood that they would behave in the same way under similar circumstances (Nagin & Paternoster, 1993). This method was chosen for several reasons. First, IS security policy violations, like other socially undesirable behaviors, are difficult to measure directly via conventional means due to respondents' tendency to conceal information or to respond to questions in socially desirable ways (Trevino, 1992). In contrast, because of the hypothetical, third-person nature of the scenarios, the scenario method provides an indirect means of measuring socially undesirable behavior, offering respondents a less intimidating means of reporting their intentions (Harrington, 1996). For this reason, the scenario method is commonly used to research ethical/unethical behavior in the social sciences in general (O'Fallon & Butterfield, 2005) and in the field of Information Systems in particular (Banerjee, Cronan, & Jones, 1998; D'Arcy et al., 2009; Harrington, 1996).

In addition to these methodological advantages, the scenario method provides substantial theoretical benefits when applied to RCT, which holds that a potential offender weighs probabilities of costs and benefits within a specific context (Becker, 1968). Contextual details are also thought to have bearing in this calculation, as both cost/benefit considerations and contextual details are thought to be considered simultaneously when making a decision to offend (Bachman et al., 1992).

Because of these factors, RCT has most often been examined in Criminology using a hypothetical scenario methodology (Paternoster & Simpson, 1996). This is because, first, individuals' decision-making is a rational and calculated activity based on the specific characteristics of the scenario, a key assumption of RCT. In fact, Grasmick and Bursik (1990) state that a study using RCT requires a hypothetical scenario methodology to make this calculative activity possible.

Second, the scenario includes context-specific information widely thought to be important in deciding whether to commit deviant

behavior. Bachman et al. (1992) and Klepper and Nagin (1989) strongly recommend including contextual information in scenarios describing an offense, and they criticize traditional surveys that use questions that are not connected to any specific context. Thus, the scenario method is particularly amenable to the application of RCT because a specific offense is described within a specific context that includes descriptions of costs and benefits, allowing respondents to make an intuitive calculation when reporting their intention to violate the policy.

Scenario Design

To improve the generalizability of our findings across a variety of IS policy violations, we designed three scenarios describing different IS policy violations. A key step in designing the scenarios was to ensure that they are realistic and commonplace to respondents (Piquero & Hickman, 1999). To do so, we surveyed 111 IT security practitioners using a belief-elicitation process designed by Limayem and Hirt (2003). This involved asking the practitioners, via an open-ended questionnaire, to list four IS security policy violations that were both common and consequential. We obtained 54 responses, yielding a 49% response rate. We then categorized the responses using content analysis (Krippendorff, 2004) and ranked the responses. The top three IS security policy violations cited by practitioners were (1) sharing or writing down passwords, (2) failing to lock or log out of workstations when not in use, and (3) copying sensitive data to unsecure portable USB storage devices. We then designed scenarios around each of these common policy violations.

To ensure that the designed scenarios were realistic in content, 15 IT security managers reviewed each scenario. After three rounds of reviews and revisions, a consensus was reached that the scenarios were realistic in form and detail. The final scenarios are listed in Appendix A.

Instrumentation

Items were drawn from previously validated instruments where possible (Straub, 1989) and are listed in Table A2 of Appendix A. In cases where previous instruments used only a single indicator for an independent variable, additional items were derived to enable reliability testing.

For the deterrence constructs, each severity-of-sanction measure was multiplied by its corresponding certainty-of-sanction measure. This yielded several composite sanction measures that "reflected both the risk and cost of perceived punishment" (Nagin & Paternoster, 1993, p. 481).

For the *perceived benefits* construct, previous research indicates that time saving is a key motivator for violations of employee IS security policy (Puhakainen, 2006). Because we could not find measures that describe saving time by violating IS security policies, we created four new items for this construct based on the qualitative interview analyses of Puhakainen (2006). Qualitative feedback on the content validity of these items was obtained from two IT security managers who acted as subject matter experts. Reliability for these measures was assessed via a pretest (described later), the results of which showed that the measures exhibit excellent reliability (Straub et al., 2004).

The dependent variable, *intention to violate IS security policy*, was measured using a single item: "What is the chance that you would do what [the scenario character] did in the described scenario?" The response scale ranged from 0 ("no chance at all") to 10 ("100 percent chance"). Although Cook and Campbell (1979) caution against the use of single-item measures to avoid mono-operation bias that could prevent constructs from being reliably measured, Straub et al. (2004) point out that in certain cases a single-item measure is most appropriate. Such is the case with the measure of *intention* in scenario-based surveys in which respondents are asked the probability of their behaving similarly to the character in the scenario (Pogarsky, 2004). Because measurement error is not expected for this item, a single item is typically used (Paternoster & Simpson, 1996).

In addition to questions relating to theoretical constructs in our model, we also asked respondents demographic questions for age,

Table 1. Descriptive statistics for samples

Sample	Sample Frame	Response Rate	Average Age	Average Work Experience in Years	Male/Female %*
IT Services Company	300	134 (45%)	45	21.5	48% / 52%
Bank	400	69 (17%)	44	21	28% / 71%
Total	700	203 (29%)	45	21	59% / 41%
* *Note.* Some respondents chose not to report gender.					

gender, and length of work experience. Furthermore, we asked respondents to rate how realistic they found the scenario to be, from 0 ("not realistic at all") to 10 ("100% realistic").

Pretest

We pretested our instrument to evaluate the psychometric properties of the items (Boudreau et al., 2001). Data for the pretest were collected from 39 part-time students at a Finnish university who also had work experience. This sample was chosen because students attending the university are made aware of and are obliged to follow the university's information security policy. Furthermore, formal sanctions are in place for those found violating the policy. Thus, respondents were familiar with the IS security policies and the potential sanctions for violations. In addition, these were part-time students who work in companies. Thus, as employees, the students were likely familiar with IS security policies. Item reliabilities were assessed using Cronbach's α. Items contributing to poor reliability were rephrased or dropped.

Primary Data Collection

Primary data was collected from two Finnish organizations: a high-tech services company and a major bank, both of which handle sensitive information. These organizations were chosen to compose the sample frame because both organizations use IS security policies and have clear sanctions in place for policy violations. Further, both organizations publish their IS security policies within the company and employ IS security managers in charge of overseeing compliance with IS security policies. Thus, respondents were knowledgeable of the survey subject matter. Descriptive statistics for the data collected are shown in Table 1. Given the difficulties in obtaining information security-related data from companies (Kotulic & Clark, 2004), the response rate in this context can be regarded as quite good.

A web-based survey was used to collect data within the organizations. When the survey was accessed, each employee was presented with one of the three scenarios selected at random by the survey software. A total of 73 respondents received the "sharing password" scenario, 66 respondents received the "failing to log out of the workstation" scenario, and 64 respondents received the "copying sensitive data" scenario.

To test whether respondents responded similarly to the three scenarios, we performed a one-way ANOVA comparing the effect of the different scenarios on respondents' reported intentions. There was no significant difference in intention across the three scenarios. Likewise, we performed a *t*-test to evaluate whether there was a difference in reported intention between the two organizations. There was no significant difference. Given these results, we used a combined dataset to perform the analysis and used control variables to test for possible effects of the sample and scenarios in the analysis.

Results

We analyzed our model using Partial Least Squares (PLS) by means of SmartPLS software

(Ringle, Wende, & Will, 2005). We chose PLS because of its ability to simultaneously evaluate both the measurement and structural models and because of its usefulness for exploratory theory-building research (Chin, Marcolin, & Newsted, 2003; Gefen, Straub, & Boudreau et al., 2000). We have documented our steps to test the reliability and validity of our model in Appendix B; tests to assess common methods variance are reported in Appendix C. The results of all of these tests met the standards of high rigor for quantitative IS research (Straub et al., 2004).

Assessing the Effects of Control Variables

In testing our hypotheses, we controlled for the effects of six variables: subsample, scenario received, reported realism of the scenario, gender, age, and work experience. To do so, we followed an approach similar to hierarchical regression, in which we first tested a model consisting only of the control variables and their effects on *intention to violate IS security policy*. Collectively, the control variables explained 7% of the variance in *intention.* Next, we added our theoretical constructs and their effects to the model. In this full model, explained variance increased from 7% to 31%. To test whether this increase was significant, we performed the following analysis. First, the effect size of adding the theoretical constructs to the model was calculated as $f^2 = (R^2_{\text{Full model}} - R^2_{\text{Partial Model}})/(1 - R^2_{\text{Full Model}})$ (Chin et al., 2003), which yielded a large effect size of .35 (Cohen, 1988). Next, the significance of this change in explained variance was obtained by calculating a pseudo F-test in which the effect size (f^2) was multiplied by (n - k - 1), where n is the sample size and k is the number of independent variables (Mathieson, Peacock, & Chin, 2001). This yielded a significant result ($F = 69.73, p < .001$), indicating that the theoretical variables explain substantially more variance in the model than do the control variables.

In the full model, only realism and gender had significant effects. Realism had a positive effect (with a path coefficient of .19), while gender had a negative effect on compliance (-.21). For realism, this significant effect implies that the more realistic or relatable that respondents considered the scenario to be, the greater their intention to behave similarly in that situation. It may also imply that the more identification respondents felt with the situation described by the scenario, the greater their intention. For gender, the item was coded 0 for "female" and 1 for "male." Thus, this negative finding implies that men in this sample were less likely to violate the information security policy than were women.

Results of Theoretical Model Testing

The results of our theoretical model testing are depicted in Figure 2.

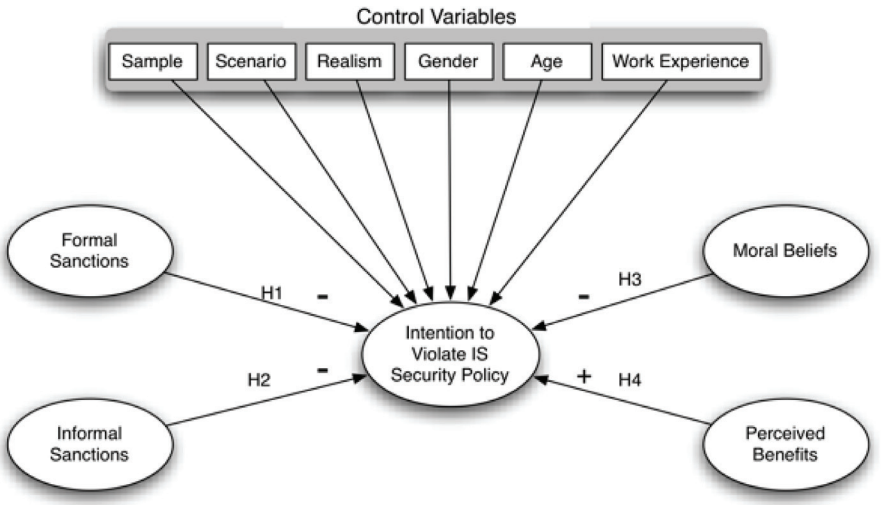
For the first two hypotheses, *formal sanctions* had no significant effect on *intention to violate IS security policy*. Thus, H1 was not supported. The effect of *informal sanctions* was significant, albeit at the .10 alpha level. Furthermore, the size of the path coefficient for this effect was -.10, lower than the .20 threshold for what would be considered a meaningful coefficient size (Chin, 1998). Therefore, although *informal sanctions* had a significant effect on *intention*, this effect was insufficient to support H2.

In contrast to the insignificant effects of sanctions, *moral beliefs* had a significant negative effect on *intention*, with a path coefficient of -.36 ($p < .001$). Thus, H3 was supported. Similarly, *perceived benefits* had a significant positive effect on *intention*, with a path coefficient of 29 ($p < .001$); thus, H4 was also supported.

Discussion

Based on these results, we next highlight several findings. First, we find that *moral beliefs* are an excellent predictor of *intention to violate IS security policies*. This finding is consistent with studies in Criminology (Bachman et al., 1992; Elis & Simpson, 1995; Paternoster & Simpson,

*Figure 2. Research model showing results of PLS analysis. N.S. = non-significant; *p < .10; ***p < .001*



1996). In the area of IS security, this finding is consistent with D'Arcy et al. (2009), who found that moral commitment had a similar negative effect on IS misuse intentions (-.37, $p < .001$). Furthermore, in IS security research, Siponen (2000, 2002) postulated the possible role of moral beliefs as a key motivational factor for employees to comply with IS security policies. However, to our knowledge, the current study is the first to have empirically examined the role of moral beliefs with respect to employees' intentional violations of IS security policies. This finding implies that if employees view violations of IS security policies as morally wrong, they are unlikely to commit them; similarly, if employees feel that it is morally acceptable to violate the norm, they are more likely to do so.

Second, *perceived benefits* also had a significant positive effect on *intention*, although in the opposite direction to *moral beliefs*. Rational Choice Theory describes a mental calculation in which not only potential sanctions are taken into account when considering an act of violation but also potential benefits, which in our case was saving time. While the role of perceived benefits has not been studied in the IS security literature to our knowledge, this finding is consistent with studies in Criminology (Ducan et al., 2005; Wood et al., 1997). This finding suggests that if employees see benefit in violating IS security policy, they are more likely to do so. This implication may seem obvious, but it is important for managers to take into account potential benefits that may prompt noncompliance. For example, security managers may wish to use IS security training to address saving time as a perceived rationalization for policy violations.

Third, the effect of formal sanctions was not supported. While the results are consistent with the RCT of Paternoster and Simpson (1996), the research findings regarding sanctions in the field of IS are mixed. For example, D'Arcy et al. (2009) found that only the severity of formal sanctions effectively reduced IS misuse. Hu, Xu, Dinev, and Ling (2010) found that formal sanctions had little impact on employee intentions to commit computer offenses. Finally, the effect of informal sanctions was not supported, though a small, somewhat significant effect ($p < .10$) was detected.

These results may imply that formal sanctions (such as penalties) and informal sanctions (such as lost respect in the eyes of management and co-workers) do not work as deterrents in

the context of employees' compliance with IS security procedures. One interpretation of the findings regarding informal sanctions is that employees do not care about penalties and the loss of respect associated with security policy violations. One reason for this may be that they perceive penalties and lack of respect to be minor issues. Another possibility is to interpret the results as viewed through Kohlberg's Cognitive Theory of Moral Development (Kohlberg, 1976, 1984), which suggests that only people who are in the initial stages of moral development are influenced by sanctions.

Implications for Practice

Our findings suggest that organizations should pursue other means of discouraging IS security policy violations besides formal sanctions. Formal sanctions serve an important role in that they "provide an important legal foundation allowing organizations to take clearly defined actions against those who violate policy" (Siponen & Vance, 2010, p. 498). However, our findings indicate that formal sanctions may not always be effective in deterring policy violations. Thus, in addition to formal sanctions, security managers should engage in positive means of enforcement. In practice, this means that organizations should arrange IS security training sessions in which the IS security educator attempts to persuade organizational members that the violation of IS security policies is morally wrong and that compliance with policies is morally correct. However, it is important to note here that such a strategy requires that the organization's IS security activities can withstand moral scrutiny (Siponen, 2002).

With respect to the perceived benefits of violating IS security policies, we suggest that top management and supervisors communicate a clear and consistent message stating that saving work time does not justify violating IS security policies and that adherence to IS security policies is integral to employee job descriptions and responsibilities.

Implications for Research

Previous studies in moral development literature suggest that people can gradually change their moral judgment through well-designed moral education and argumentation (Kohlberg, 1984). With this backdrop, and keeping in mind our finding that moral beliefs have a significant effect on intention to violate IS security policy, the key avenue for future research is to study the effect of carefully designed moral persuasion techniques on employees' compliance with IS security policies. A number of strategies may be pursued in such an educational program. One is the Kohlberg-Blatt method of inducing cognitive conflict (Crain, 2004). Another method favored by Kohlberg (1976) is role-taking opportunities, which refer to opportunities to consider others' viewpoints. In the IS security policy compliance context, considering others' viewpoints could encourage discussion regarding the consequences of noncompliance with IS security policies for members of the organization and the organization as a whole.

Such educational interventions can be measured by traditional pre- and post-tests with self-reports or objective measures. The pretest measurement provides the baseline for employee attitudes before the IS security training. The post-test is administered after the IS security training sessions in order to see the effect on employees' attitudes about the moral discussion provided by the IS security training. The pretest/post-test design can also be used in the case of employees who do not have sufficient knowledge to successfully answer the pretest before the educational intervention. (For instance, employees may not understand a pretest question like, "Do you use email encryption to encrypt confidential email messages?" or may confuse it with the concept of encryption of a remote login connection. As a result, they may provide incorrect information in the pretest.) In addition, experiments with control groups are especially welcome (Greenberg, 1990).

Similarly, pre- and post-tests are needed to study how organizations can overcome employees' perceptions of benefits for violating IS security policies. Based on research in other fields (Greenberg, 1990), we suggest the implementation of carefully designed IS security training sessions in which educators provide persuasive messages arguing that saving time does not justify violations of IS security policies.

Limitations

It is important to consider two principal limitations of this study. First, as is the case with most IS research, data were collected from within a single country. It may be possible that the results of this study will not generalize to other countries and cultures. A needed avenue of future research is to examine the effects of sanctions, benefits, and moral beliefs across cultures.

Another limitation of the study is the examination of intention rather than actual behavior. It is possible that respondents' reported intentions differ from their actual behaviors. However, two considerations help to mitigate this limitation. First, the informational value of reported intention is not tied only to its use as a proxy for actual behavior. Rather, in the context of scenario studies, reported intention is indicative of "a motivational state that exists just prior to the commission of an act. We think of it as a measured reflection of a predisposition to commit [an act]" (Paternoster & Simpson, 1996, p. 561). Thus, reported intention is a measure of predisposition to violate IS security policies, making it well suited as a measure of prospective behavior.

Second, a large number of studies in the social sciences have found that reported intentions do correlate strongly with actual behavior (Albarracin, Johnson, Fishbein, & Muellerleile, 2001; Notani, 1998; Sutton, 1998). Within the field of Criminology, reported intentions to offend have been found to correlate highly with past offenses (Grasmick & Burisk, 1990; Nagin & Paternoster, 1993), actual offenses in the future (Beck & Ajzen, 1991; Green, 1989; Murray & Erickson, 1987), and concurrent offending behavior (Pogarsky, 2004). Thus, strong empirical support exists that validates the intention measure as a useful surrogate measure of actual behavior. Nevertheless, this limitation should be kept in mind when interpreting the results of this study.

CONCLUSION

While employees' compliance with IS security policies is reported to be a key concern for organizations, little empirical research has devoted attention to this concern. To address a related problem, namely computer abuse, IS scholars have applied utilitarian-based deterrence approaches that focus on formal sanctions. In comparison, informal sanctions, perceived benefits, and moral evaluations have received less or no attention from IS security scholars. As recent studies in Criminology have highlighted the role of moral beliefs over formal sanctions, it is important to study the role of moral beliefs and benefits with respect to employees' adherence to IS security policies. To fill this gap in the research, we have tested a model based on RCT, which can be seen as an extension of deterrence theory. It explains individuals' decisions to break norms as being utilitarian calculations based on perceived benefits, moral beliefs, and formal and informal sanctions. The results of our tests mainly support our model, suggesting that perceived benefits have a substantial impact on employees' noncompliance with IS security policies. In turn, moral beliefs also have a substantial effect. The practical implications of our study suggest that organizations should focus on IS security awareness activities that address moral beliefs and perceived benefits of noncompliance. Finally, future research should employ experiments and surveys to study the effect of IS security training sessions and campaigns.

REFERENCES

Albarracin, D., Johnson, B., Fishbein, M., & Muellerleile, P. (2001). Theories of reasoned action and planned behavior as models of condom use: A meta-analysis. *Psychological Bulletin*, *127*(1), 142–161. doi:10.1037/0033-2909.127.1.142

Aytes, K., & Connolly, T. (2003, August 4–6). A research model for investigating human behavior related to computer security. In *Proceedings of the 2003 American Conference on Information Systems,* Tampa, FL.

Aytes, K., & Connolly, T. (2004). Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing*, *16*(3), 22–40. doi:10.4018/joeuc.2004070102

Bachman, R., Paternoster, R., & Ward, S. (1992). The rationality of sexual offending: Testing a deterrence/rational choice conception of sexual assault. *Law & Society Review*, *26*(2), 343–372. doi:10.2307/3053901

Banerjee, D., Cronan, T. P., & Jones, T. W. (1998). Modeling IT ethics: A study in situational ethics. *Management Information Systems Quarterly*, *22*(1), 31–60. doi:10.2307/249677

Beck, L., & Ajzen, I. (1991). Predicting dishonest actions using the theory of planned behavior. *Journal of Research in Personality*, *25*, 285–301. doi:10.1016/0092-6566(91)90021-H

Becker, G. S. (1968). Crime and punishment: An economic approach. *The Journal of Political Economy*, *76*, 169–217. doi:10.1086/259394

Becker, R., & Mehlkop, G. (2006). Social class and delinquency: An empirical utilization of rational choice theory with cross-sectional data of the 1990 and 2000 German general population surveys (ALLBUS). *Rationality and Society*, *18*(2), 193–235. doi:10.1177/1043463106063323

Boudreau, M., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: A state of-the-art assessment. *Management Information Systems Quarterly*, *25*(1), 1–26. doi:10.2307/3250956

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

Cao, L. (2004). *Major criminological theories: Concepts and measurement*. Belmont, CA: Wadsworth.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, *1*(3), 18–41.

Chin, W. (1998). Issues and opinions on structural equation modeling. *Management Information Systems Quarterly*, *22*(1), vii–xvi.

Chin, W., Marcolin, B., & Newsted, P. (2003). A Partial Least Squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic mail emotion/adoption study. *Information Systems Research*, *14*(2), 189–217. doi:10.1287/isre.14.2.189.16018

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale, NJ: Erlbaum.

Cook, T. D., & Campbell, D. T. (1979). *Quasi experimentation: Design and analytical issues for field settings*. Chicago, IL: Rand McNally.

Cornish, D., & Clarke, R. V. (1986). Introduction . In Cornish, D., & Clarke, R. (Eds.), *The reasoning criminal* (pp. 1–16). New York, NY: Springer-Verlag.

Crain, W. (2004). *Theories of development: Concepts and applications*. Upper Saddle River, NJ: Prentice Hall.

D'Arcy, J., Hovav, A., & Galletta, D. F. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98. doi:10.1287/isre.1070.0160

Ducan, L., Lafree, G., & Piquero, A. R. (2005). Testing a rational choice model of airline hijackings. *Criminology*, *43*(4), 1031–1065. doi:10.1111/j.1745-9125.2005.00032.x

Elis, L. A., & Simpson, S. (1995). Informal sanction threats and corporate crime: Additive versus multiplicative models. *Journal of Research in Crime and Delinquency*, *20*(3), 233–252.

Ernst & Young. (2008). *Ernst & Young's 2008 global information security survey*. London, UK: Author.

Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *JMR, Journal of Marketing Research*, *18*(1), 39–50. doi:10.2307/3151312

Gefen, D., & Straub, D. W. (2005). A practical guide to factorial validity using PLS-graph: Tutorial and annotated example. *Communications of the AIS*, *16*(5), 91–109.

Gefen, D., Straub, D. W., & Boudreau, M.-C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the AIS*, *4*(7), 1–70.

Grasmick, H. G., & Bryjak, G. J. (1980). The deterrent effect of perceived severity of punishment. *Social Forces*, *59*(2), 471–491.

Grasmick, H. G., & Bursik, R. (1990). Conscience, significant others, and rational choice: Extending the deterrence model. *Law & Society Review*, *24*(3), 837–862. doi:10.2307/3053861

Green, D. E. (1989). Measures of illegal behavior in individual-level deterrence research. *Journal of Research in Crime and Delinquency*, *26*(3), 253–275. doi:10.1177/0022427889026003004

Greenberg, J. (1990). Employee theft as a reaction to underpayment inequity: The hidden cost of pay cuts. *The Journal of Applied Psychology*, *75*(5), 561–568. doi:10.1037/0021-9010.75.5.561

Hagen, J. (2009). Human relationships: A never-ending security education challenge? *IEEE Security & Privacy*, *7*(4), 65–67. doi:10.1109/MSP.2009.92

Hare, R. M. (1981). *Moral thinking: Its levels, methods and point*. Oxford, UK: Clarendon.

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *Management Information Systems Quarterly*, *20*(3), 257–278. doi:10.2307/249656

Herath, T., & Rao, H. R. (2009a). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, *18*, 106–125. doi:10.1057/ejis.2009.6

Herath, T., & Rao, H. R. (2009b). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*, 54–165. doi:10.1016/j.dss.2009.02.005

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2010). The centrality of low self-control in internal computer offenses. In B. Molyneux (Ed.), *Proceedings of the Dewald Roode Information Security Workshop 2010*, Waltham, MA (pp. 316-345).

Klepper, S., & Nagin, D. (1989). The deterrent effect of perceived certainty and severity of punishment revisited. *Criminology*, *27*(4), 721–746. doi:10.1111/j.1745-9125.1989.tb01052.x

Kohlberg, L. (1976). Moral stages and moralization: The cognitive-developmental approach . In Lickona, T. (Ed.), *Moral Development and Behavior: Theory, research, and social issues* (pp. 31–53). New York, NY: Holt, Rinehart and Winston.

Kohlberg, L. (1984). *The psychology of moral development*. New York, NY: Harper & Row.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management*, *41*, 597–607. doi:10.1016/j.im.2003.08.001

Krippendorff, K. (2004). *Content analysis: An introduction to its methodology*. Thousand Oaks, CA: Sage.

Lafleur, L. M. (1992). Training as part of a security awareness program. *Computer Control Quarterly*, *10*(4), 4–11.

Lee, S. M., Lee, S.-G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, *41*(6), 707–718. doi:10.1016/j.im.2003.08.008

Limayem, M., & Hirt, S. G. (2003). Force of habit and information systems usage: Theory and initial validation. *Journal of the AIS*, *4*(1), 65–97.

Malhotra, N., Kim, S., & Patil, A. (2006). Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research. *Management Science*, *52*(12), 1865–1883. doi:10.1287/mnsc.1060.0597

Mathieson, K., Peacock, E., & Chin, W. (2001). Extending the technology acceptance model: The influence of perceived user resources. *The Data Base for Advances in Information Systems*, *32*(3), 86–112.

McLean, K. (1992). IS security awareness—Selling the cause. In *Proceedings of the 8th International Conference on IS Security (IFIP/Sec '92)*.

Murray, G., & Erickson, P. (1987). Cross-sectional versus longitudinal research: An empirical comparison of projected and subsequent criminality. *Social Science Research*, *16*, 107–118. doi:10.1016/0049-089X(87)90011-1

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *1*(18), 126–139. doi:10.1057/ejis.2009.10

Nagin, D., & Paternoster, R. (1993). Enduring individual differences and rational choice theories of crime. *Law & Society Review*, *27*(3), 467–496. doi:10.2307/3054102

Ng, B. Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior using the health belief model. *Decision Support Systems*, *46*(4), 815–825. doi:10.1016/j.dss.2008.11.010

Notani, A. (1998). Moderators of perceived behavioral control's predictiveness in the theory of planned behavior: A meta-analysis. *Journal of Consumer Psychology*, *7*(3), 247–271. doi:10.1207/s15327663jcp0703_02

Nunnally, J. C. (1967). *Psychometric theory*. New York, NY: McGraw-Hill.

O'Fallon, M., & Butterfield, K. (2005). A review of the empirical ethical decision-making literature: 1996–2003. *Journal of Business Ethics*, *59*(4), 375–413. doi:10.1007/s10551-005-2929-7

Pahnila, S., Siponen, M. T., & Mahmood, A. (2007, July). Which factors explain employees' adherence to information security policies? An empirical study. In *Proceedings of the PACIS 2007 Conference*, Auckland, New Zealand.

Parker, D. B. (1976). *Crime by computer*. New York, NY: Scribner.

Paternoster, R., & Simpson, S. (1993). A rational choice theory of corporate crime. In R. V. Clarke & M. Felson (Eds.), *Advances in Criminological Theory: Vol. 5. Routine activity and rational choice* (pp. 37–58). New Brunswick, NJ: Transaction.

Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law & Society Review*, *30*(3), 549–584. doi:10.2307/3054128

Pavlou, P., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *Management Information Systems Quarterly*, *31*(1), 105–136.

Piquero, A., & Hickman, M. (1999). An empirical test of Tittle's control balance theory. *Criminology*, *37*(2), 319–342. doi:10.1111/j.1745-9125.1999.tb00488.x

Piquero, A., & Tibbetts, S. (1996). Specifying the direct and indirect effects on low self-control and situational factors in offenders decision making: Toward a more comparative model of rational offending. *Justice Quarterly*, *13*(3), 481–510. doi:10.1080/07418829600093061

Podsakoff, P. M., MacKenzie, S. B., Lee, J., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *The Journal of Applied Psychology*, *88*(5), 879–903. doi:10.1037/0021-9010.88.5.879

Pogarsky, G. (2004). Projected offending and implications for heterotypic continuity. *Criminology*, *42*(1), 111–135. doi:10.1111/j.1745-9125.2004.tb00515.x

Pratt, T. C., & Cullen, F. T. (2000). The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis. *Criminology*, *38*(3), 931–964. doi:10.1111/j.1745-9125.2000.tb00911.x

Puhakainen, P. (2006). *Design theory for information security awareness*. Unpublished doctoral dissertation, University of Oulu, Finland.

Ringle, C. M., Wende, S., & Will, A. (2005). *SmartPLS*. Hamburg, Germany: SmartPLS.

Siponen, M. T. (2000). A conceptual foundation for organizational IS security awareness. *Information Management & Computer Security*, *8*(1), 31–41. doi:10.1108/09685220010371394

Siponen, M. T. (2002). On the role of human morality in information system security: From the problems of descriptivism to non-descriptive foundations . In Salehnia, A. (Ed.), *Ethical issues of information systems* (pp. 255–271). Hershey, PA: Idea Group.

Siponen, M. T., & Iivari, J. (2006). IS security design theory framework and six approaches to the application of IS security policies and guidelines. *Journal of the Association for Information Systems*, *7*(7), 445–472.

Siponen, M. T., Mahmood, A., & Pahnila, S. (2010). Why employees don't comply with information security policies: An empirical investigation. *IEEE Computer*, *43*(10), 64–71.

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

Stahl, B. (2004). Responsibility for information assurance and privacy: A problem of individual ethics? *Journal of Organizational and End User Computing*, *16*(3), 59–77. doi:10.4018/joeuc.2004070104

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

Straub, D. W. (1989). Validating instruments in MIS research. *Management Information Systems Quarterly*, *13*(2), 147–169. doi:10.2307/248922

Straub, D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research*, *1*(3), 255–276. doi:10.1287/isre.1.3.255

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

Sutton, S. (1998). Predicting and explaining intentions and behavior: How well are we doing? *Journal of Applied Social Psychology*, *28*, 1317–1338. doi:10.1111/j.1559-1816.1998.tb01679.x

Telders, E. (1991). Security awareness programs: A proactive approach. *Computer Security Journal*, *7*(2), 57–64.

Thomson, M. E., & von Solms, R. (1998). IS security awareness: Educating your users effectively. *Information Management & Computer Security*, *6*(4), 167–173. doi:10.1108/09685229810227649

Trevino, L. K. (1992). Experimental approaches to studying ethical-unethical behavior in organizations. *Business Ethics Quarterly*, *2*(2), 121–136. doi:10.2307/3857567

Vroom, C., & von Solms, R. (2002). A practical approach to IS security awareness in the organization. In *Proceedings of the 17th International Conference on IS Security (SEC2002)*.

Wood, P. B., Gove, W. R., Wilson, J. A., & Cochran, J. K. (1997). Nonsocial reinforcement and habitual criminal conduct: An extension of learning theory. *Criminology*, *35*(2), 335–366. doi:10.1111/j.1745-9125.1997.tb00879.x

Young, K. (2010). Policies and procedures to manage employee internet abuse. *Computers in Human Behavior*, *26*(6), 1467–1471. doi:10.1016/j.chb.2010.04.025

ENDNOTES

1 Parker described his choice of the term "computer abuse" in this way: "The first proposal for my research was titled 'Computer-Related Crime.' Law researchers reviewed the proposal, saying, 'Parker, you are a computer technologist. What are you doing, trying to decide what a crime is? After all, there are only six people in the whole world qualified to address that subject.' I next changed the name of the research to 'Anti-Social Use of Computers.' Sociologists who reviewed the proposal came back to me and said, 'Parker, you are computer technologist. What are you doing, trying to decide what is social and antisocial? After all, there are only six people in the whole world qualified to address that subject.' I thought to myself, 'All right, you guys, I will play your game.' I changed the title of the research to 'Computer Abuse'—a term that had not been used or at least formalized before" (Parker, 1976, p. xi).

2 N. B. These convergent validity tests were not performed for the dependent variable, *intention to violate IS security policy*, because these tests are not applicable for single-item measures.

Anthony Vance is as an Assistant Professor of Information Systems in the Marriott School of Management of Brigham Young University. He has earned PhD degrees in Information Systems from Georgia State University, USA; the University of Paris—Dauphine, France; and the University of Oulu, Finland. He received a BS in IS and Masters of Information Systems Management (MISM) from Brigham Young University, during which he was also enrolled in the IS Ph.D. preparation program. His previous experience includes working as a visiting research professor in the Information Systems Security Research Center at the University of Oulu, where he remains a research fellow. He also worked as an information security consultant for Deloitte. His work is published in MIS Quarterly, Journal of Management Information Systems, *and* European Journal of Information Systems. *His research interests are information security, trust in information systems, and internal control.*

Mikko Siponen is a Professor and Director of the IS Security Research Centre in the Department of Information Processing Science at the University of Oulu, Finland. He is also vice-head of the department. He holds a PhD in philosophy from the University of Joensuu, Finland, and a Ph.D. in Information Systems From the University of Oulu, Finland. His research interests include IS security, IS development, computer ethics, and philosophical aspects of IS. He has 33 published or forthcoming papers in journals such as MIS Quarterly, Journal of the Association for Information Systems, European Journal of Information Systems, Information & Organization, Information Systems Journal, Information & Management, ACM Database, Communications of the ACM, IEEE Computer, IEEE IT Professional and ACM Computers & Society. *He has received over 5.4 million USD of research funding from corporations and numerous funding bodies. He has served as a senior and associate editor for ICIS and ECIS. He is currently a guest senior editor for the MIS Quarterly special issue entitled 'Information Systems Security in a Digital Economy'. He sits on the editorial boards of the* European Journal of Information Systems, Journal of Organizational and End User Computing, *and* Journal of Information Systems Security. *In 2009 he was ranked as fourth productive IS scholar in Europe. The Finnish Funding Agency for Technology and Innovation ranked the IS Security Research Center that Dr. Siponen established and lead as the top ICT research group in Finland.*

APPENDIX A. SCENARIOS AND INSTRUMENTATION

Table A1. Hypothetical scenarios

Violation	Scenario
USB drive	Pekka is a middle level manager in a medium-sized company where he has worked for several years. Pekka is currently working on a sales report that requires the analysis of the company's customer database. This database contains customer names, phone numbers, credit card numbers, and purchase histories. Because of the sensitive nature of corporate data, the company has a strict policy prohibiting the copy of corporate data to unencrypted portable media, such as USB drives. However, Pekka will be traveling for several days and would like to analyze the corporate database on the road. Pekka expects that copying the data to the USB drive and taking it on the road could save the company a lot of time and money. The firm is experiencing growing sales and revenues in an industry that is economically deteriorating. He also knows that an employee was recently reprimanded for copying sensitive corporate data to a USB drive. Pekka copies the corporate database to his portable USB drive and takes it off company premises.
Workstation logout	Seija is a middle-level manager in a medium-sized company where she was recently hired. Her department uses an inventory procurement software application program to make inventory purchases. To ensure that only authorized individuals make inventory purchases, the company has a firm policy that employees must log out or lock their computer workstation when not in use. However, to make work more convenient, Seija's manager directs her to leave her user account logged-in for other employees to freely use. Seija expects that keeping her user account logged-in could save her company time. She also knows that keeping the workstation logged-in is a common practice in the industry and an employee recently was reprimanded for leaving the workstation logged-in. Seija leaves the workstation logged-in when she is finished.
Passwords	Hannu is a low-level manager in a small company where he was recently hired. His company has a strong policy that each computer workstation must be password-protected and that passwords are not to be shared. However, Hannu is on a business trip and one of his co-workers needs a file on his computer. Hannu expects that sharing his password could save his company a lot of time. He also knows that the firm has mandatory information security training. Hannu shares his password with his co-worker.

Table A2. Measurement items

Constructs	Item	Source
Formal Sanctions—certainty 1	What is the chance you would receive sanctions if you violated the company information security policy?	Nagin and Paternoster (1993)
Formal Sanctions—certainty 2	What is the chance that you would be formally sanctioned if management learned that you had violated the company information security policy?	Derived from Nagin and Paternoster (1993)
Formal Sanctions—certainty 3	What is the chance that you would be formally reprimanded if management learned you had violated the company information security policy?	Derived from Nagin and Paternoster (1993)
Formal Sanctions—severity 1	How much of a problem would it be if you received severe sanctions if you violated the company information security policy?	Nagin and Paternoster (1993)
Formal Sanctions—severity 2	How much of a problem would it create in your life if you were formally sanctioned for doing what [the scenario character] did?	Derived from Nagin and Paternoster (1993)
Formal Sanctions—severity 3	How much of a problem would it create in your life if you were formally reprimanded for doing what [the scenario character] did?	Derived from Nagin and Paternoster (1993)
Informal sanctions—certainty 1	How likely is it that you would lose the respect and good opinion of your co-workers for violating the company information security policy?	Nagin and Paternoster (1993)

continued on following page

Table A2. continued

Informal sanctions—certainty 2	How likely is it that you would jeopardize your promotion prospects if management learned that you had violated the company information security policy?	Nagin and Paternoster (1993)
Informal sanctions—certainty 3*	How likely is it that you would lose the respect and good opinion of your manager, if management learned that you had violated company IT security policies?	Derived from Nagin and Paternoster (1993)
Informal sanctions—severity 1	How much of a problem would it create in your life if you lost the respect and good opinion of your co-workers for violating the company information security policy?	Nagin and Paternoster (1993)
Informal sanctions—severity 2	How much of a problem would it create in your life if you jeopardized your future job promotion prospects for doing what [the scenario character] did?	Nagin and Paternoster (1993)
Informal sanctions—severity 3*	How much of a problem would it create in your life if you lost the respect of your manager for violating the company information security policy?	Derived from Nagin and Paternoster (1993)
Moral Beliefs 1	I feel that the [scenario] character acted wrongly by violating company IT security policy.	Derived from Paternoster and Simpson (1996)
Moral Beliefs 2	How morally wrong would it be to do what the person did in the scenario?	Paternoster and Simpson (1996)
Moral Beliefs 3*	It is morally right to violate company IT security policies.	Derived from Paternoster and Simpson (1996)
Perceived Benefits 1	If I would do what [the scenario character] did, I would save time.	New measure
Perceived Benefits 2	If I would do what [the scenario character] did, I would save work time.	New measure
Perceived Benefits 3	Noncompliance with the information security policies saves work time.	New measure
Perceived Benefits 4	Noncompliance with the information security measure saves employees' time.	New measure
Note. *Dropped to improve reliability or construct validity.		

APPENDIX B. MODEL VALIDATION

To establish factorial validity and reliability for the measurement model, we followed the PLS validation procedures outlined by Gefen and Straub (2005). To test convergent validity, we performed a bootstrap with 600 resamples and then examined the t-values of the outer model loadings. Convergent validity is demonstrated when all indicators load significantly on their respective latent construct. In our case, all indicators exhibited loadings that were significant at the .001 level (Table B1), denoting strong convergent validity. An additional test of convergent validity put forward by Fornell and Larcker (1981) is that the average variance extracted (AVE), a measure of variance explained by a latent construct for the variance observed in its measurement items, should be at least .50 or higher. The AVE values are shown in Table B2. Both tests indicate a high degree of convergent validity[2].

To evaluate discriminant validity, two tests were performed. First, the cross-loadings of measurement items on latent constructs were examined. In this test, discriminant validity is demonstrated when an item more highly loads on its intended construct than on any other construct. Following Gefen and Straub (2005), this difference in loadings should be at least .10. In

Table B1. PLS loadings for convergent validity

Construct	Item	Loading
Moral Beliefs	MoralA	0.90***
	MoralB	0.88***
Benefits	Benefits1	0.90***
	Benefits2	0.92***
	Benefits3	0.75***
	Benefits4	0.72***
Formal Sanctions	FormA	0.79***
	FormB	0.92***
	FormC	0.86***
Informal Sanctions	InformA	0.81***
	InformB	0.96***
***$p < .001$		

Table B2. AVE scores

Construct	AVE
Formal Sanctions	.74
Informal Sanctions	.78
Benefits	.68
Moral Beliefs	.80

Table B3. Cross-loadings of measurement items to latent constructs

Construct	Item	1	2	3	4
Benefits (1)	Benefits1	**0.90**	-0.10	0.00	-0.14
	Benefits2	**0.92**	-0.17	-0.05	-0.20
	Benefits3	**0.75**	-0.10	0.06	-0.16
	Benefits4	**0.72**	-0.23	-0.07	-0.18
Formal Sanctions (2)	FormA	-0.21	**0.79**	0.43	0.33
	FormB	-0.13	**0.92**	0.64	0.41
	FormC	-0.11	**0.86**	0.67	0.34
Informal Sanctions (3)	InformA	0.03	0.48	**0.81**	0.24
	InformB	-0.04	0.68	**0.96**	0.32
Moral Beliefs (4)	MoralA	-0.09	0.36	0.29	**0.90**
	MoralB	-0.27	0.40	0.28	**0.88**

Table B4. Correlation of the latent variable scores with the square root of AVE

Construct	1	2	3	4
Benefits (1)	**0.83**			
Formal Sanctions (2)	-0.17	**0.86**		
Informal Sanctions (3)	-0.02	0.68	**0.88**	
Moral Beliefs (4)	-0.20	0.42	0.32	**0.89**

Table B5. Reliability scores

Construct	Composite Reliability	Cronbach's α
Formal	.89	.82
Informal	.88	.75
Moral Beliefs	.89	.75
Benefits	.90	.85

this test, all items showed excellent discriminant validity (Table B3). Therefore, the model demonstrates high discriminant validity.

A second test of discriminant validity is to compare the AVE score for each construct. In the AVE test of discriminant validity, the square root of a given construct's AVE should be larger than any correlation of the given construct with any other construct in the model (Chin, 1998). All the results of this test were acceptable. Our results depicted in Table B4 again demonstrate strong discriminant validity.

Finally, to test the reliability of measurement items, SmartPLS was used to compute the Cronbach's α as well as the composite reliability score, which is evaluated in the same way as Cronbach's α (Fornell & Larcker, 1981). Both scores are reported in Table B5. All constructs exhibited a reliability score well over the .60 threshold accorded to exploratory research (Nunnally, 1967).

APPENDIX C. ASSESSING COMMON METHODS VARIANCE

Because measures for the dependent and independent variables were taken from the same instrument, we performed two tests to gauge the influence of common methods bias in our data. First, we performed Harman's one-factor test to see whether one factor accounted for the majority of variance in the data (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). To do so, we entered all items used in the instrument into an unrotated exploratory factor analysis. This yielded 41 factors, the largest of which accounted for 28% of the variance, showing no evidence of common methods bias. As an additional test, we examined the latent variable correlations to see whether any two latent constructs correlated highly (at .90 or more), another possible manifestation of common methods bias (Pavlou, Liang, & Xue, 2007). No constructs were found to correlate so highly. Given these results, and because evidence suggests that methods biases are not as serious in the field of IS as compared to those in other disciplines (Malhotra, Kim, & Patil, 2006), we conclude that there is little threat of common methods bias in our data.