MIS Quarterly

SPECIAL ISSUE

NEUTRALIZATION: NEW INSIGHTS INTO THE PROBLEM OF EMPLOYEE INFORMATION SYSTEMS SECURITY POLICY VIOLATIONS[1]

By: **Mikko Siponen**
Information Systems Security Research Centre
Department of Information Processing Science
University of Oulu
Linnanmaa
Oulu 3000
FINLAND
mikko.siponen@oulu.fi

Anthony Vance
Information Systems Department
Marriott School of Management
Brigham Young University
Provo, Utah 84602
U.S.A.
anthony@vance.name

Abstract

Employees' failure to comply with information systems security policies is a major concern for information technology security managers. In efforts to understand this problem, IS security researchers have traditionally viewed violations of IS security policies through the lens of deterrence theory. In this article, we show that neutralization theory, a theory prominent in Criminology but not yet applied in the context of IS, provides a compelling explanation for IS security policy violations and offers new insight into how employees rationalize this behavior. In doing so, we propose a theoretical model in which the effects of neutralization techniques are tested alongside those of sanctions described by deterrence theory. Our empirical results highlight neutralization as an important factor to take into account with regard to developing and implementing organizational security policies and practices.

Keywords: Neutralization theory, deterrence theory, IS security policies, IS security, compliance

Introduction

Employees' compliance with information security policies is reported as a key information security problem for organizations (Ernst & Young 2008; Puhakainen 2006). It is estimated that over half of all information systems security breaches are indirectly or directly caused by employees' poor IS security compliance (Dhillon and Moores 2001; Stanton et al. 2005). Employee violations of IS security policies are most often due to negligence or ignorance of IS security policies on the part of employees (Vroom and von Solms 2004), even in organizations in which IS security policies and staff are present (Puhakainen 2006).

To overcome the problem of employees' negligent IS security policy compliance, the use of sanctions, grounded in deterrence theory, is widely advocated by both practitioners (Bequai 1998; David 2002; Parker 1997; Wood 1982) and IS scholars (Kankanhalli et al. 2003; Straub 1990; Tudor 2000). We argue, based on research in Criminology, that employees' violation of IS security policies is not always best explained

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

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

by fear of sanctions because employees may use neutralization techniques (Piquero et al. 2005; Sykes and Matza 1957), rationalizations which allow them to minimize the perceived harm of their policy violations. This rationalizing behavior in turn reduces the deterring effect of sanctions. Our empirical results offer corroborative support for our assertion that neutralization theory is an important factor in IS security policy violations. The findings have implications for IS security practice and research. Our results suggest that practitioners should work to counteract employees' use of neutralization techniques.

The remainder of this paper is organized as follows. Previous studies that apply deterrence theory are reviewed. The theories underlying our model and hypotheses are discussed. We then describe the research method used and present the results. This is followed by a discussion of the results, limitations, and implications for future research and practice. Finally, we conclude by summarizing our key findings.

Previous Work on Deterrence Theory and Security Behavior in IS

A number of studies have applied deterrence theory in IS, especially severity and certainty of formal sanctions. To start with, Straub and Nance (1990) suggested that detection and punishment of violators minimizes computer abuse. Similarly, Straub (1990) found that the use of IS security deterrents resulted in a decreased incidence of computer abuse. The following deterrents were found effective: weekly hours dedicated to IS security, use of multiple methods to disseminate information about penalties and acceptable system usage, and clear statements of penalties for violations (Straub 1990). These were found to increase the employees' risk of getting caught (certainty of sanctions) and the perception that severe sanctions took place if caught (severity of sanctions). Straub and Welke (1998) carried out an action research study in which they highlighted the importance of communicating certainty and severity of sanctions as a part of employee education and training programs in order to minimize security violations. Following this research, Kankanhalli et al. (2003) studied whether the use of sanctions led to enhanced IS security effectiveness and found that deterrents, as measured in man-hours spent in security efforts, led to better IS security effectiveness. Straub et al. (1993) applied deterrence theory by carrying out a field experiment that tested whether student cheating during a programming assignment could be prevented. They concluded that managers should stress that violations of the organization's IS security policies will result in sanctions. Harrington (1996) found that codes of ethics, a type of formal sanction, applied to the organization generically did not affect employees' judgments or intentions to commit computer abuse. However, generic codes of ethics were found to affect employees who were high in *denial of responsibility*, a form of rationalization. Similarly, IS-specific codes of ethics did not affect judgement or intentions, except in the case of computer sabotage, a severe type of computer abuse. Thus, the effects of codes of ethics were found to be "sporadic and weak" (Harrington 1996, p. 273). D'Arcy et al. (2009) found that IS security policies, awareness programs, and computer monitoring influenced perceived severity of formal sanctions, which led to reduced intention to misuse IS. In their study, certainty of formal sanctions did not have any effect on intention to misuse IS.

In addition to formal sanctions in terms of deterrence theory, Siponen et al. (2007) applied both formal and informal sanctions in order to explain employees' IS security policy compliance. Siponen et al. found that deterrents predicted employees' compliance with IS security policies.

To summarize these findings, sanctions, informed by deterrence theory, is a widely suggested approach to reduce computer abuse and improve employee compliance with IS security policies in the IS security literature.

Following the idea of neutralization theory, previous research in criminology (Piquero et al. 2005), and findings by Puhakainen (2006), we postulate that violation of IS security policies by employees may not always be best explained by fear of sanctions because employees use neutralization techniques (Sykes and Matza 1957). These techniques provide employees a temporary release from their conventional restraints, including formal and informal sanctions (Akers and Sellers 2004). In the next section, we present the theoretical framework derived from neutralization theory.

Theoretical Framework

We preface our theoretical framework development with our full research model presented in Figure 1. The theoretical model comprises two theories from the field of Criminology: neutralization theory (Sykes and Matza 1957) and deterrence theory (Paternoster and Simpson 1996). Deterrence theory is included for nomological validity (Straub et al. 2004) so that the effect predicted by neutralization theory can be compared *vis-à-vis* with those of deterrence theory.

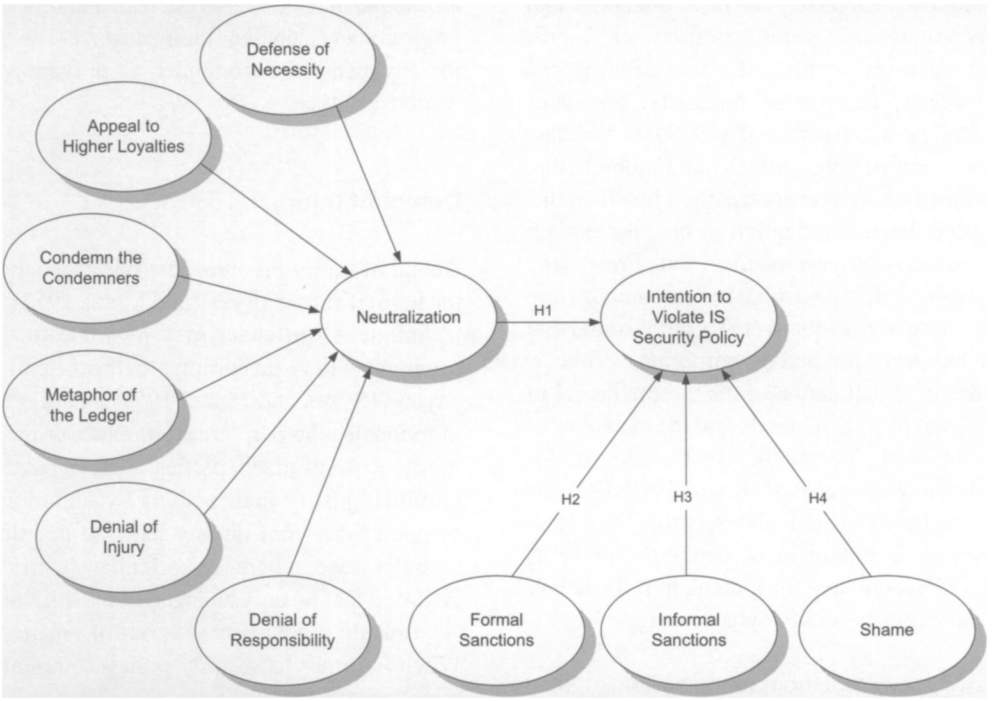

Figure 1. The Research Model

Neutralization theory claims that both law-abiding citizens and those who commit crimes or rule-breaking actions believe in the norms and values of the community in general (Sykes and Matza 1957). So why then do people break rules? Sykes and Matza suggested that people psychologically enable themselves to commit rule-breaking or any anti-social actions by applying techniques of neutralization. Neutralization techniques offer a way for persons to render existing norms inoperative by justifying behavior that violates those norms (Rogers and Buffalo 1974). For example, a person performing a deviant action justifies his/her behavior by claiming that no damage will really be done. In this way, the person avoids guilt by reasoning that there is no criminal behavior involved; after all, no one got hurt (Sykes and Matza 1957). Sykes and Matza maintained that in neutralizing their behavior, individuals can maintain their noncriminal image and drift back and forth between rule-breaking and law-abiding behavior (Piquero et al. 2005). This is the theoretical explanation for why sanctions may lose their efficacy in the presence of neutralization techniques.

Next we describe components of neutralization and deterrence theory as they relate to our model, and present our hypotheses.

Neutralization Theory

In their original formulation of neutralization theory, Sykes and Matza proposed five techniques of neutralization: denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners, and appeal to higher loyalties. Later, Klockars (1974) added "the metaphor of the ledger" and Minor (1981) added a technique named "the defense of necessity." We used four dimensions of Sykes and Matza, in addition to the metaphor of the ledger and the defense of necessity. We omit the denial of the victim dimension because our focus is compliance with IS security policies. The denial of the victim technique is based on the argument that the victim—the object of the act—deserves the consequences. In the case of compliance with security policies, it is difficult to point out who is the victim. Research results suggest that this omission is not problematic. For example, Eliason and Dodder (1999) reported that other dimensions of Sykes and Matza have better explanatory power. Furthermore, most research studies employing neutralization theory have used a subset of the techniques proposed by Sykes and Matza (Cao 2004).

A number of studies have offered empirical support for neutralization techniques. Eliason and Dodder studied

neutralization techniques exercised by deer poachers and found that four techniques of neutralization occurred most frequently in that context: denial of responsibility, the metaphor of the ledger, defense of necessity, and condemnation of the condemner. Byers et al. (1999) studied hate crimes perpetrated against the Amish and found that techniques of neutralization are prevalent in their justification. Pershing (2003) found that neutralization techniques explain rule-breaking in military environments, and Priest and McGrath (1970) showed that neutralization techniques are used to justify illicit drug use. Piquero et al. (2005) found that neutralization techniques predicted corporate crime. Hollinger (1991) reported that denial of the victim, denial of injury, condemnation of the condemners, and the metaphor of the ledger explained workplace theft. In the area of IS, Harrington (1996) found that *denial of responsibility* was significantly correlated with individuals' intention to commit computer abuse and their judgment of computer abuse as acceptable. Lim (2002) found that the metaphor of the ledger was invoked by employees to justify cyberloafing.

Although IS security policy violations are not criminal, they are violations of social norms, that is, established policies of the corporation which are often contractually binding on the employee. Akers and Sellers (2004) observed that criminological theories explain law-breaking or "any deviant behavior that violates social norms, whether or not such behavior also violates the law" (p. 2). Neutralization techniques have previously been successfully applied to behaviors that are rule-breaking but not necessarily criminal (Pershing 2003). The specific neutralization techniques examined in this study are discussed next.

Denial of Responsibility

Using the denial of responsibility technique, a person committing a deviant act defines himself as lacking responsibility for his/her actions (Rogers and Buffalo 1974; Sykes and Matza 1957). In this technique, the person rationalizes that the action in question is beyond his/her control (Piquero et al. 2005). The deviant views himself as a billiard ball, helplessly propelled through different situations (Sykes and Matza 1957). For example, Eliason and Dodder reported that deer poachers employed the denial of responsibility technique by stating that they did not know that the law prohibited hunting. In the context of IS security, Harrington found that denial of responsibility was significantly correlated with individuals' intention to commit computer abuse and to evaluate computer abuse as acceptable. Puhakainen (2006) reported a situation where employees denied their responsibility to comply with a policy to encrypt confidential e-mails because they rationalized that the policy was unclear. Parker (1976) reported that programmers labeled their mistakes as computer errors, thereby using the computer as a scapegoat for denial of responsibility.

Denial of Injury

Denial of injury involves justifying an action by minimizing the harm it causes (Sykes and Matza 1957). To illustrate this technique, an offender may regard auto theft as "just borrowing," which, according to the offender, does not hurt anyone (Sykes and Matza 1957). Parker (1998) found that individuals who perpetrate computer crimes frequently deny injury to victimized parties. He reported that computer criminals justify their actions by claiming that attacking a computer does not do any harm to people. Especially, he noted a case where an offender justified his action by claiming that he only changed two instructions in a program. As a result, a company was out of business for two weeks. When it comes to security policy compliance, an employee might argue that it is ok to violate information security policies if no harm is done to the company.

Defense of Necessity

Defense of necessity is based on the justification that if the rule-breaking is viewed as necessary, one should not feel guilty when committing the action (Minor 1981). In this way, the offender can put aside feelings of guilt by believing that an act was necessary and there was no other choice (Piquero et al. 2005). Eliason and Dodder found that deer poachers neutralized their actions through the defense of necessity by claiming that poaching is not wrong because they must provide food for their families through poaching. In the IS security policy context, Puhkainen reported that employees claimed that they did not have time to comply with the policies owing to tight deadlines.

Condemnation of the Condemners

According to this technique, one neutralizes his or her actions by blaming those who are the target of the action (Byers et al. 1999). For example, one may break the law because the law is unreasonable. In the information security context, an employee could say that it is not wrong to violate information security policies that are unreasonable. Parker (1998) reported that offenders engaged in computer crime often claimed that the law was unjust.

Appeal to Higher Loyalties

This technique is employed by those who feel they are in a dilemma that must be resolved at the cost of violating a law or policy (Sykes and Matza 1957). In an organization context, an employee may appeal to organizational values or hierarchies (Piquero et al. 2005). For example, an employee could argue that he/she must violate a policy in order to get his/her work done (Siponen and Iivari 2006).

The Metaphor of the Ledger

The metaphor of the ledger uses the idea of compensating bad acts with good acts (Klockars 1974). That is, an individual believes that he/she has previously performed a number of good acts and has gained a surplus of good will, and as a result of this, can afford to do some bad actions (Klockars 1974; Piquero et al. 2005). Previous research has found that employees in corporate environments neutralize their actions through the metaphor of the ledger by rationalizing that their overall past good behavior justifies occasional rule-breaking (Hollinger 1991; Minor 1981). Lim (2002) studied the metaphor of the ledger in a corporate context and found that employees justify their nonwork related web surfing because of their good job performance. Similarly, employees could argue that their general adherence to security policies compensates their occasional violation of security policies.

Multidimensional Nature of Neutralization Construct

We chose to model neutralization as a multidimensional second-order construct (Jarvis et al. 2003) for several reasons. First, it is clear from our review of neutralization theory that several distinct dimensions of neutralization exist (Cromwell and Thurman 2003). Although these dimensions are conceptually distinct, at a more abstract level, each can be viewed as describing a different facet of the overall construct of neutralization (Jarvis et al. 2003; Law and Wong 1999). MacKenzie et al. (2005) observed that multidimensional second-order constructs are useful when a greater specificity of understanding is wanted in understanding a theoretical construct. Whereas two or three measurement items might suffice to define a construct of peripheral interest, a multidimensional construct allows researchers to develop items that describe a construct in terms of multiple subconstructs, bringing the nature of the construct into sharper relief. Thus, Petter et al. (2007) observed "a complex construct that is the main topic of study may deserve to be modeled as a multidimensional construct so as to permit a more thorough measurement and analysis" (p. 627). This research approach is consistent with our goal to understand the effects of various neutralization techniques on employees' intention to violate IS security policies.

We further conceptualized neutralization as a Type II second-order construct (Jarvis et al. 2003), a second-order construct that is formatively composed of reflective subconstructs. A construct composed in this manner is useful "when multiple subconstructs and measurement items are necessary to fully capture the entire domain of the construct" (Petter et al. 2007 p. 627). This description is especially applicable to neutralization theory because of the variety of dimensions of neutralization identified in criminological research. However, each neutralization subconstruct is modeled reflectively because its associated measurement items are interchangeable, are manifestations of the subconstruct, and covary (Petter et al. 2007). In summary, we conceptualize the construct *neutralization* as a multidimensional second-order construct comprised of first-order constructs that represent specific neutralization strategies. Based on the above considerations, we hypothesize that

H1: Neutralization positively affects intention to violate IS security policy.

Deterrence Theory

Deterrence theory, which can be traced back to Bentham (1748-1832) and Beccaria (1738-1794), posits that individuals weigh costs and benefits when deciding whether or not to commit a crime, and they choose crime when it pays. To be more precise, if an individual believes that the risk of getting caught is high (certainty of sanctions), and severe penalties will be applied if one is caught (severity of sanctions), then deterrence theory posits that individuals will not commit crimes. In the last few decades, research on deterrence theory has undergone a number of extensions (Grasmick and Bryjak 1980; Piquero and Tibbetts 1996). The most notable of these is the addition of "non-legal costs" (Pratt and Cullen 2000, p. 367), such as informal sanctions and shame (Piquero and Tibbetts 1996). Informal sanctions include the disapproval of friends or peers for a given action (Paternoster and Simpson 1996).

Following Braithwaite (1989) and Paternoster and Simpson (1993), we have included shame as a deterrent in addition to formal and informal sanctions. Shame refers to a feeling of guilt or embarrassment if others knew of one's socially undesirable actions (Eliason and Dodder 1999; Paternoster and Simpson 1996). Tangney (1995) held that shame affects

an individual's self esteem. Similarly, Paternoster and Simpson (1996) separated shame from informal and formal sanctions because shame is a self-imposed sanction. Following Paternoster and Simpson (1993), shame can be regarded as a deterrent, and therefore part of deterrence theory, because it is assumed to have effects similar to other sanctions (Braithwaite 1989; Elis and Simpson 1995). This means that individuals may estimate probable shame, just as one might calculate other sanctions (Tibbetts 1997). In fact, research on deterrence has found positive evidence that shame functions as a deterrent and decreases individuals' motivation to perform crimes (Grasmick and Bursik 1990; Nagin and Paternoster 1993). We argue that employees' violation of IS security policies are poorly explained by sanctions in the presence of neutralization techniques (Sykes and Matza 1957) which weaken restraints imposed by formal and informal sanctions (Akers and Sellers 2004). Nevertheless, we include the effects of sanctions in our model to provide nomological validity and to facilitate comparisons with past studies (Straub et al. 2004). We therefore offer the following hypotheses consistent with deterrence theory:

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

H3: Informal sanctions negatively affect intention to violate IS security policy.

H4: Shame negatively affects intention to violate IS security policy.

Research Design

We empirically assessed our model using a hypothetical scenario method (Weber 1992). This technique, also known as a vignette or policy capturing method, uses vignettes that "present subjects with written descriptions of realistic situations and then request responses on a number of rating scales that measure the dependent variables of interest" (Trevino 1992, pp. 127-128). Scenario-based methods are a common means of assessing antisocial and ethical/unethical behavior (Pogarsky 2004). In a review of 174 ethical decision-making articles appearing in premier business journals, 55 percent employed a scenario method (O'Fallon and Butterfield 2005). In the field of IS, the scenario method has been used to study ethical issues such as software piracy (Moores and Chang 2006), computer abuse (Banerjee et al. 1998; D'Arcy et al. 2009; Harrington 1996), and privacy concerns (Malhotra et al. 2004), as well as more general topics such as media choice (Straub and Karahanna 1998) and electronic channel selection (Choudhury and Karahanna 2008).

The scenario method offers several advantages for research on unethical or socially undesirable behavior. First, scenarios afford an indirect way of measuring intention to commit unethical behavior, which is difficult to measure directly because individuals are likely to conceal their behavior and respond to questions in socially desirable ways (Trevino 1992). Because scenarios describe another's behavior in hypothetical terms, the respondent may feel less intimidated to report an intention to act similarly to the person described in the scenario (Harrington 1996).

Second, scenarios can incorporate situational details thought to be important in decisions to behave unethically (Klepper and Nagin 1989). Survey questions that ask respondents in general terms—that is, without reference to a particular context or situation—whether they would behave unethically force respondents to contrive in their own minds circumstances in which they might consider doing so. This can introduce measurement error if the imagined circumstances are different from those in which unethical behavior is actually performed (Bachman et al. 1992). Scenarios provide a way to enhance the realism of decision-making situations by providing contextual detail while simultaneously ensuring that these details are uniform across respondents (Alexander and Becker 1978).

Third, the scenario method provides a methodological advantage because it allows unethical behavior to be measured prospectively (Pogarsky 2004). Traditional surveys link past behavior (as the dependent variable) with present perceptions of theoretical constructs in the survey, possibly creating measurement error (Bachman et al. 1992). For these reasons, a prospective measure of behavior such as "intention to commit an act" is recommended in criminological literature (Bachman et al. 1992; Grasmick and Bursik 1990).

Scenario Design

To ensure the generalizability of our findings across different kinds of IS security policy violations, we designed three different scenarios describing common and important policy violations in coordination with 54 information security professionals (see Appendix B for full details on the development of the scenarios). For the administration of the survey, one of the three scenarios was randomly selected and presented to a respondent, followed by the survey items. The design of one scenario per respondent was chosen because of the large number of survey items associated with each scenario (Paternoster and Simpson 1996). However, scenario-based

studies with few survey items often use a design of multiple scenarios per respondent (Jasso 2006).

Instrumentation

Items were adapted from previously validated instruments where possible (Boudreau et al. 2001) and were measured on an 11-point scale from 0 to 10 (Paternoster and Simpson 1996). In some cases, additional items were derived from the original items to allow reliability to be assessed. Composite measures for deterrence constructs were calculated to "create a sanction measure that reflected both the risk and cost of perceived punishment" (Nagin and Paternoster 1993, p. 481). This was done by multiplying each severity measure by its associated certainty measure. All measurement items are included in Appendix A.

The dependent variable, *Intention to Violate IS Security Policy*, was measured using a single item adapted from Paternoster and Simpson (1996) which read, "What is the chance that you would do what Pekka did in the described scenario?" The response scale for this item ranged from 0 (no chance at all) to 10 (100% chance). Although Cook and Campbell (1979) noted a reliability threat from using a single measure, Straub et al. (2004) pointed out that in some situations a single measure is most appropriate. A weakness of single item measures is the inability to validate whether the construct was accurately captured (Straub et al. 2004). However, in the case of the scenario method, respondents report the probability that they would do what the scenario character did via a single measure that appears immediately following the scenario (Pogarsky 2004). Because measurement error is not expected for this reported probability, a single item was used. This is the case for the Defining Issues Test (DIT), one of the most widely replicated scenario studies (Rest 1979; Rest and Narvaez 1994). Consistent with these studies, the intention measure appeared first in the instrument immediately after the hypothetical scenario.

In addition to items measuring latent constructs, we included a single-item measure that asked respondents to rate how realistic the given scenario was. This item ranged from 0 (not believable) to 10 (100% believable). Finally, basic biographical data was collected, including gender, age, and work experience.

Pretest

Before the pretest, the items and scenarios were individually reviewed by 15 information security managers. After three rounds of review and modification, all security managers reached consensus that the scenarios and items were relevant, realistic, and readable. To validate the psychometric properties of the instrument (Straub 1989), we pretested the survey with office personnel at two Finnish organizations (a knowledge management company and a steel producer) for a total of 90 responses. This sample was chosen because IT security policies were implemented at both sites. The reliability of measurement items for each construct was assessed using Cronbach's α; convergent and discriminant validity was assessed using principal components analysis. Both assessments yielded acceptable results in almost all instances. Measurement items with unacceptably low Cronbach's α were rephrased or dropped.

Primary Data Collection

Primary data for the study were collected from administrative personnel from three organizations in Finland: the administration office of a university, a major electrical company, and the corporate office of a large supermarket chain. For the university administration office, located in central Finland, approximately half of the respondents were IT support staff with a master's degree, while the other half were administrative staff handling payroll, finances, and legal contracts with a university or technical degree.

For the corporate office of the supermarket chain, located in southern Finland, respondents were either marketing employees responsible for designing and implementing market strategies, or finance employees in charge of developing services available within the chain's stores. Nearly all employees in this sample held a master's degree.

For the electrical company, located in central Finland, respondents were administrative staff that performed customer service, designed electrical services, and provided IT support. Most employees possessed a university degree.

Respondents in all organizations sampled handled sensitive information. All three organizations featured published IS security policies so respondents were familiar with the subject matter of the survey. Additionally, all three organizations employ IT security managers and enforce compliance with IT policies with explicitly defined formal sanctions. The descriptive statistics for each subsample are presented in Table 1.

The required sample size to evaluate our model is 60 according to the "rule of ten" heuristic (Barclay et al. 1995). However, following the sample size recommendations of Marcoulides and Saunders (2006), we collected over six times

Table 1. Descriptive Statistics for Samples

Sample	Sample Frame	Response (Rate)	Average Age	Average Work Experience	Male/ Female %*
Office staff, university	220	114 (52%)	43	20	43% / 47%
Office staff, electrical company	99	41 (41%)	42	19	46% / 37%
Office staff, supermarket chain	1130	240 (21%)	40	17	34% / 63%
Total	1449	395 (27%)	41	18	38% / 56%

*Note: Some respondents chose not to report gender.

this number to ensure sufficient power and reliability in the results.

For the entire sample, the average score for realism (on an 11-point scale of 0 to 10) was 7.42, indicating that the scenarios were generally thought to be realistic by participants. For reported intention to violate the IS security policy as did the character in the scenario, the average score was 3 (on a scale of 0 to 10). Some 68 percent of respondents reported a non-zero probability of violating the IS security policy, which is comparable to similar hypothetical scenario studies performed in Criminology (Paternoster and Simpson 1996).

Model Analysis

We analyzed our theoretical model using partial least squares (PLS) using SmartPLS (Ringle et al. 2005). We chose a structural equation modeling (SEM) technique rather than regression to test our theory because of our conceptualization of *neutralization* as a multidimensional second-order construct (MacKenzie et al. 2005), for which SEM methods are better suited. We chose PLS rather than a covariance-based SEM technique such as LISREL because of the ability of PLS to model second-order constructs that are formatively composed of first-order factors, such as our conceptualization of neutralization. This type of second-order construct specification is problematic for analysis using LISREL (Chin 1998). Furthermore, PLS is more suitable when the purpose of the model is to predict, rather than to test established theory, in which case LISREL is preferred (Chin et al. 2003; Gefen et al. 2005). We document our tests performed to validate our model in Appendices B and C, which include tests for convergent and discriminant validity and common methods bias. The results of these tests demonstrate that our model meets or exceeds the rigorous standards expected for positivist IS research (Straub et al. 2004).

Results of Theoretical Model Testing

Consistent with our theory that neutralization techniques can explain policy violations in addition to sanctions, we took a multistage approach to analyzing the model analogous to hierarchical regression. First, we examined the effects of six control variables on *intention to violate IS security policy*: sample organization, scenario type, realism, gender, age, and work experience.

We included gender, age, and work experience to test whether these demographics affected the dependent variable. Since data were collected from different organizations, we also included this variable as a control. Further, each participant was randomly given one of three scenarios. A one-way ANOVA found that the reported level of *intention* significantly differed depending on the scenario received (the password scenario had the highest average of reported intention at 3.52, followed by the USB scenario at 3.19 and the workstation-logout scenario at 2.11). For this reason, we controlled for the effect of scenario type on *intention*. Finally, because we found that respondents' perception of how realistic the scenario was significantly correlated with *intention* ($r = .23$, $p < .005$), we also controlled for its effect. Collectively, these variables explained 10 percent of the variance of *intention*. However, only reported realism was found to have a significant effect (although scenario type also had a significant effect in the full model presented later).

Next, we analyzed the added effects of deterrence constructs *formal sanctions*, *informal sanctions*, and *shame* in the model. Of these constructs, only *informal sanctions* was significant ($-.22$, $p < .01$). As a whole, explained variance for the model increased from 10 percent to 19 percent. To test whether this increase was significant, we performed the following analysis. First, the size of the effect of adding a new component 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). Next, a pseudo F-test was cal-

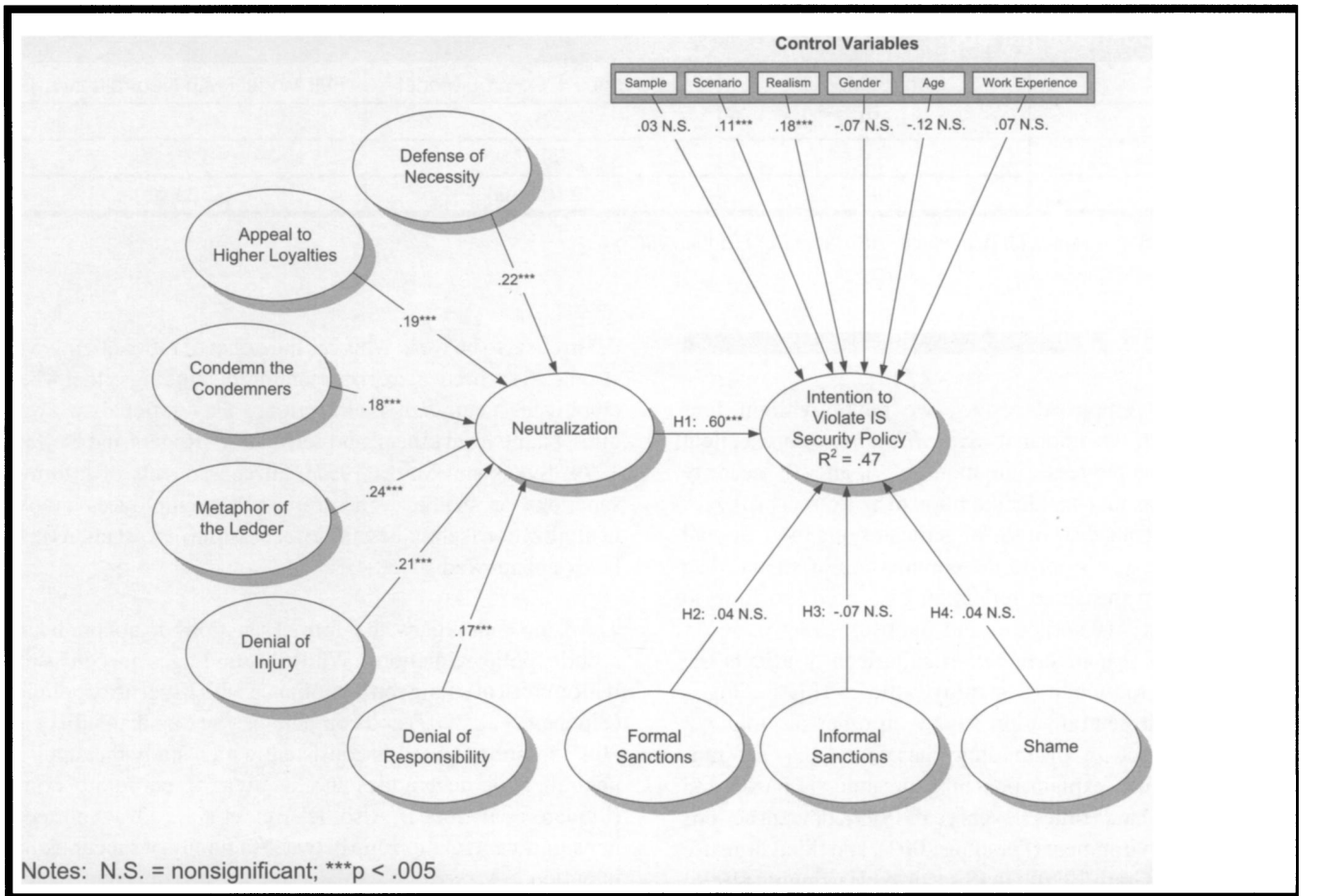

Figure 2. Research Model Showing Results of PLS Analysis

culated by multiplying the effect size (f^2) by (n – k – 1), where *n* is the sample size and *k* is the number of independent variables (Mathieson et al. 2001). Although the size of the effect was small (.12), the change in R^2 was significant (F = 44.73, p < .001), indicating that *informal sanctions* explains significantly more variance in *intention to violate security policies* than do the control variables alone.

Finally, *neutralization* was added to the model to demonstrate its ability to explain variance in *intention* beyond that explained by the deterrence constructs (see Figure 2). The addition of *neutralization* to the model increased the explained variance in *intention* from .19 to .47, a highly significant change given the pseudo F-test described above (198.42, p < .001). Further, the effect size of *neutralization* was large at .52, where .35, .15, and .02 are respectively large, medium, and small effects (Cohen 1988). These tests strongly support the addition of *neutralization* to the model, demonstrating that it explains substantially more variance than do the deterrence constructs alone. The results of this multistage analysis are summarized in Table 2.

The full PLS model evaluated is depicted in Figure 2. As predicted, *neutralization* had a strong, significant effect on *intention to violate IS security policy*, as demonstrated by the large and significant path coefficient (.60, p < .005). Supporting the excellent results of the discriminant and convergent validity tests, all path coefficients from first-order *neutralization* constructs to the second-order construct are significant and above or near .20 (Chin 1998), indicating that *neutralization* performs well as a second-order construct.

Interestingly, although *informal sanctions* was significant in the deterrence model without the *neutralization* construct, with the presence of *neutralization* in the model, none of the deterrent effects were significant. Thus hypotheses H2, H3, and H4 were not supported. Further, the path coefficients for these effects were too small to be considered meaningful (Chin 1998).

Table 2. Model Comparison			
	Control Model	Deterrence + Control Model	Full Model (with Neutralization)
R^2	.10	.19	.47
ΔR^2	—	.09***	.28***
Effect size	—	.12 (small)	.52 (large)

***p < .001; effect sizes small (.02), medium (.15), large (.35) (Cohen 1988)

Discussion

Based on our empirical results, we next highlight four findings. First, we find that *neutralization* is an excellent predictor of employees' intention to violate IS security policies. We do not consider intention to be a direct proxy for behavior, but instead see it as "an indicator 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 and Simpson 1996, p. 561). Thus, we find that *neutralization* significantly affects the predisposition to violate IS security policy. This finding is consistent with neutralization studies in other disciplines. Previous research in Criminology has found that neutralization techniques explain poaching behavior (Eliason and Dodder 1999), hate crimes (Byers et al. 1999), deviant actions in a military environment (Pershing 2003), and illicit drug use (Priest and McGrath 1970). In IS security, Harrington (1996) found that rationalizations were strongly correlated with intentions to commit computer abuse. Puhakainen (2006) reported based on his qualitative interviews that employees fail to comply with IS security policies because they perceive that their workload is high; they are busy with other assignments; security policies slow them down; and other work is more important. While Puhakainen did not link these findings to neutralization theory, these findings can be seen as the means by which employees' neutralize their actions. Similarly, Parker (1976) reported a number of excuses for committing computer crimes that can be interpreted as neutralization techniques.

The second finding is that, although *informal sanctions* significantly predicts *intention*, in the presence of *neutralization*, the effect of *informal sanctions* on *intention* is insignificant. Part of this finding can be understood in terms of a comparison in effect size. In our analysis, the deterrence constructs collectively had a small effect (.12), whereas the effect of *neutralization* was quite large (.52) (Cohen 1988). Previous research in Criminology has highlighted the small effect size of sanctions (Cook 1980; Tittle 1980). Harrington (1996) also found the effects of codes of ethics, a kind of deterrence, to be weak whereas the effect of rationalizing was strong. A theoretical explanation for this finding is that when employees neutralize their actions, they rationalize away guilt, blame from others, and self-blame (Rogers and Buffalo 1974; Sykes and Matza 1957), all components of informal sanctions or shame. Therefore, when employees invoke neutralization techniques, the effect of informal sanctions may be overshadowed.

Third, our data suggest that formal sanctions do not predict IS security policy violations. While this finding is not consistent with empirical studies on compliance with IS security policies (Siponen et al. 2007) and computer abuse (Kankanhalli et al. 2003; Straub 1990), it is consistent with a study that applied neutralization techniques in the area of corporate crime (Piquero et al. 2005). Also, D'Arcy et al. (2009) reported a nonsignificant relationship between certainty of sanctions and intention. A possible explanation for the different results between this study and previous studies on IS security policy compliance and computer abuse is that neutralization techniques enable people to break the rules, while at the same time enabling them to view themselves as a rule-abiding in general (Rogers and Buffalo 1974; Sykes and Matza 1957).

Finally, the fourth finding is the report of the most common and important IS security violations, shown in Table B1 of Appendix B. To our knowledge, this is the first study that provides security managers' views on the most important and common IS security violations.

Limitations

A key limitation of the paper is the sample, which was collected from three Finnish organizations. Although the results of the model are consistent across the organizations, care should be taken in generalizing these findings to other organizations. Similarly, because national culture has been found to have a substantial effect in IS studies (Leidner and Kayworth 2006), caution should be taken in generalizing these results to other cultures.

Also, the use of intention as the dependent variable raises the question of whether intention indicates actual behavior. We offer two justifications for the use of intention as the dependent variable. First, measures of intention in criminological research are indicative of a motivation state or predisposition to commit an act (Paternoster and Simpson 1996) and are widely accepted in criminological research (Bachman et al. 1992; Cao 2004). Second, studies exploring the relationship between intention and actual behavior suggest a strong relationship between the two (Fishbein and Ajzen 1975; Green 1989; Pogarsky 2004). Thus, although the lack of a measure of actual behavior is a limitation, the *intention* measure is nonetheless a valuable approximation that yields insight into IT security policy violation research.

Another limitation of this study is that some respondents may have already violated the IT security policy described in the scenario, in which case respondents may have responded highly to neutralization items in order to preserve their self-image. Because each respondent received one of three scenarios describing different IT security policy violations, we deem it unlikely that sufficient previous violators of policy existed in our sample to skew our results. However, since we did not measure previous violations of policy, we include this as a limitation.

Also, while the use of one item is a standard way to measure intention to violate in scenario-based instruments in Criminology (Paternoster and Simpson 1996; Pogarsky 2004) and in Social Psychology (Rest and Narvaez 1994), there still remains the possibility of a threat to reliability due to mono-operation bias (Cook and Campbell 1979). This can be regarded as a possible limitation of the study.

Finally, the cross-sectional design of the study limits our findings in at least two ways. First, because neutralization enables drift, a "temporary period of irresponsibility or an episodic relief from moral constraint" (Maruna and Copes 2005, p. 231), it would be useful to observe patterns in drift over time, and how sanctions become more or less effective during periods of drift. The cross-sectional design of this study precludes such observations.

Second, the cross-sectional design makes it impossible to infer causation. Specifically, because we do not show that deterrents occur before neutralization techniques are introduced, we cannot claim that neutralization techniques reduce the effect of deterrents, although neutralization theory makes this implication (Sykes and Matza 1957). A longitudinal survey such as that performed by Paternoster et al. (1982) or an experiment might be used to provide evidence for this possibility.

Implications for Practice

Previous work in other areas suggests that techniques such as adequate explanation to justify the organizational policy through seminars (Greenberg 1990), victim-offender mediation (Thurman et al. 1984), and persuasive discussion (Fox 1999) aimed at inhibiting these neutralization techniques are useful means to change behavior. Based on these findings, we suggest the following strategies to challenge the rationalizations by employees.

With respect to denial of injury, research in other areas has suggested that "victim-offender mediations" (Braithwaite 1999) or persuasive discussion (Fox 1999; Thurman 1984) make the offenders realize that there is an injury. In the IS security context, we suggest that organizations establish training sessions or other meetings where the employees are persuaded to understand why an injury may occur if an IS security policy is not followed. Puhakainen (2006) reported the use of scenario-based exercises as part of a training session as a good way to make employees realize what harm could happen if the security policies are violated. Also, because the influence of supervisors on their employees' security behavior is reported as a promising avenue to increase security policy compliance (Siponen et al. 2007), we suggest that supervisors should be encouraged to raise awareness of potential damage to the organization if the employees do not follow the security policies.

With respect to denial of responsibility, supervisors in one-on-one interactions and speakers in company seminars need to stress that there is no excuse for IS security policy non-compliance, even if the employees are not sure what the policy is or if they don't fully understand it. Previous research on employees' noncompliance with policies suggests that training is a useful way to achieve this (Puhakainen 2006). Here the important aspect is to stress that all employees have the responsibility for their IS security actions and no one can escape this responsibility. Also, we suggest that security managers need to ensure that IS security policies are advertised prominently in the organization. It is also important to make sure that the IS security policies are readable and understandable for all employees.

Regarding the defense of necessity, research in other areas suggests managers should emphasize to the employees that even when they are under the pressure of a tight deadline there is no excuse to use a shortcut that violates IS security policies. Finally, it is important to stress that the violation of IS security policies is the employee's own choice. Security managers need to make sure that team leaders do not encourage their subordinates to bypass security rules when facing deadlines.

In the same vein, with respect to the appeal to higher loyalties, security managers at organizations need to ensure that team leaders and line managers do not support their subordinates in violating IS security policies in order to get their jobs done. Here it is important to educate the employees to internalize that compliance with IS security policies is part and parcel of their work, and any neglect of compliance with IS security policies should be seen as negligence of one's work responsibilities. Following this idea, condemnation of the condemners views should be tackled by justifying that even though compliance with IS security policies may require extra effort, it is important to make this extra effort and follow the IS security policy.

As for the metaphor of the ledger, we suggest that it is important to point out to employees that their general compliance with policies is not enough; violation of any IS security policy cannot be justified. Similarly, employees should understand that hard work for the company does not give them justification to violate IS security policies occasionally.

In this study we offered information on the most common and important IS security violations as reported by 54 IS security experts. While we acknowledge that this information may not be generalizable, it is nonetheless a useful reference point for practitioners.

Finally, although the effect of formal sanctions was not found to be significant in our analysis, we urge caution in concluding that formal sanctions are not effective deterrents. Formal sanctions have been found to be effective in other contexts (Kankanhalli et al. 2003; Straub 1990). In addition, according to the theory of cognitive moral development (Kohlberg 1969), individuals at the "obedience" stage of moral development are only deterred by threat of sanctions. This suggests that formal sanctions should be used because of their effectiveness in deterring these individuals. Further, beyond their role as deterrents, formal sanctions (such as codes of ethics) serve as an important legal foundation allowing organizations to take clearly defined actions against those who violate policy[2] (Harrington 1996). We therefore believe that formal sanctions serve an important role in the implementation and enforcement of IS security policies.

Implications for Research

Our results highlight a number of opportunities for future research on employees' IS security policy compliance. First, Robinson and Kraatz (1998) reported that techniques of neutralization are used more often in organizations where the norms stating what constitutes acceptable behavior are weak. Consequently, we suggest that there is a need to study whether weak cultural norms increase employees' use of neutralization techniques. Research is also needed to explore whether there are specific reasons why neutralization techniques emerge. Neutralization theory suggests that individuals break the rules when they learn neutralization techniques (Piquero et al. 2005; Sykes and Matza 1957), not when they are associated with other rule breakers as suggested by differential association theory. Future research is needed to study whether this assertion is true.

A second research stream related to the use of neutralization strategies is how best to inhibit neutralization techniques. Previous studies in other fields suggest that careful explanation and justification for organizational policies through seminars and education sessions has a key role in inhibiting employees' attempts to use techniques of neutralization (Greenberg 1990). Hence, there is a need to study the effect of educational programs based on theories of learning and campaigns based on principles of marketing (Puhakainen 2006). Experiments with control groups are especially welcomed (Greenberg 1990). With respect to educational programs, an interesting question for future research is whether web-based education is more useful as compared to face-to-face educational sessions in inhibiting neutralization techniques invoked by the employees. Both qualitative and quantitative empirical research methods are needed to study this issue. First, we suggest the use of a pretest study to explore the baseline level of the employees by means of interviews or surveys, or both. Then we suggest several educational or campaign sessions, grounded upon solid theories, where employees are persuaded to comply with the policies. After each campaign or educational session, we suggest the collection of a posttest to gauge possible changes in employee behavior. In addition to the subjective and self-reported measures, we also encourage the use of positive measures.

This leads us to the third research avenue. This paper used self-reported intention as the dependent variable. While there is strong theoretical support for this practice, there is a need to study compliance by use of objective measures in order to see if there is a difference between these two approaches. Clearly, the use of objective measures is difficult, and requires some kind of monitoring to see whether the employees comply with policies. We believe that the common IS security policy violation problems reported in this study (e.g., "employees do not lock or log out of workstation") might be noted by observing the offices of a large organization in person. While such ethnographical observation is not trivial, we suggest this as an important avenue for future research.

[2]We thank an anonymous reviewer for this insight.

Alternatively, logs of employees' activity could provide objective measures of compliant behaviors.

Conclusion

There is no doubt that employees' lack of compliance with IS security policies is a key problem that security managers encounter in organizations. Previous research in the IS field has viewed this problem through the lens of deterrence theory. The results of this study—although qualified by their limitations—suggest that neutralization techniques influence employees' intentions to violate IS security policies. Our study, therefore, highlights neutralization as an important factor to take into account with regard to developing and implementing organizational security policies and practices.

Our study highlights several directions for future research. First, additional surveys are needed to generalize the findings of this study to other contexts and cultures. Experimental studies are needed to demonstrate the causal effect of neutralization on noncompliance, possibly also comparing the effects of neutralization *vis-à-vis* those of sanctions. Second, in both survey and experimental designs, future research could also explore why employees "drift" into a state in which they begin using neutralization techniques. Third, employees' security policy compliance should be evaluated via objective measures. Finally, policy awareness campaigns and educational sessions on neutralization need to be examined in order to identify effective means of inhibiting the use of neutralization techniques and thus improve IS security policy compliance.

Acknowledgments

The authors wish to thank the corporate sponsors of the Information Systems Security Research Center at the University of Oulu, Finland: City of Oulu, Elektrobit Corp., Elisa Corp., F-Secure Corp., Fortum Corp., Nokia Corp., Outokumpu Oyj, SOK (Suomen Osuuskauppojen Keskuskunta), STUK (Radiation and Nuclear Safety Authority), TVO (Teollisuuden Voima Oyj). They also thank senior editor Seymour Goodman and associate editor Merrill Warkentin for their editorial guidance and support, as well as three anonymous reviewers for their insightful comments throughout the review process.

References

Akers, R. L., and Sellers, C. S. 2004. *Criminological Theories: Introduction, Evaluation, and Application* (4th ed.), Los Angeles: Roxbury Press.

Alexander, C. S., and Becker, H. J. 1978. "The Use of Vignettes in Survey Research," *Public Opinion Quarterly* (42:1), pp. 93-104.

Bachman, R., Paternoster, R., and Ward, S. 1992. "The Rationality of Sexual Offending: Testing a Deterrence/ Rational Choice Conception of Sexual Assault," *Law & Society Review* (26:2), pp. 343-372.

Banerjee, D., Cronan, T. P., and Jones, T. W. 1998. "Modeling IT Ethics: A Study in Situational Ethics," *MIS Quarterly* (22:1), pp. 31-60.

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

Bequai, A. 1998. "Employee Abuses in Cyberspace: Management's Legal Quagmire," *Computers and Security* (17:8), pp. 667-670.

Boudreau, M., Gefen, D., and Straub, D. W. 2001. "Validation in Information Systems Research: A State-of-the-Art Assessment," *MIS Quarterly* (25:1), pp. 1-26.

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

Braithwaite, J. 1999. "Restorative Justice: Assessing Optimistic and Pessimistic Accounts," *Crime and Justice: A Review of Research* (25), pp. 1-127.

Byers, B., Crider, B. W., and Biggers, G. K. 1999. "Bias Crime Motivation: A Study of Hate Crime and Offender Neutralization Techniques Used against the Amish," *Journal of Contemporary Criminal Justice* (15:1), pp. 78-96.

Cao, L. 2004. *Major Criminological Theories: Concepts and Measurement*. Belmont, CA: Wadsworth Publishing.

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

Chin, W., Marcolin, B., and 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), pp. 189-217.

Choudhury, V., and Karahanna, E. 2008. "The Relative Advantage of Electronic Channels: A Multidimensional View," *MIS Quarterly* (32:1), pp. 127-157.

Cohen, J. 1988. *Statistical Power Analysis for the Behavioral Sciences* (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum Associates.

Cook, P. J. 1980. "Research in Criminal Deterrence: Laying the Groundwork for the Second Decade," *Crime and Justice: A Review of Research* (2), pp. 211-268.

Cook, T. D., and Campbell, D. T. 1979. *Quasi Experimentation: Design and Analytical Issues for Field Settings*, Chicago: Rand McNally.

Cromwell, P., and Thurman, Q. 2003. "The Devil Made Me Do It: Use of Neutralizations by Shoplifters," *Deviant Behavior* (24:6), pp. 535-550.

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

David, J. 2002. "Policy Enforcement in the Workplace," *Computers & Security* (21:6), pp. 506-513.

Dhillon, G., and Moores, S. 2001. "Computer Crimes: Theorizing About the Enemy Within," *Computers and Security* (20:8), pp. 715-723.

Eliason, S. L., and Dodder, R. A. 1999. "Techniques of Neutralization Used by Deer Poachers in the Western United States: A Research Note," *Deviant Behavior* (20:3), pp. 233-252.

Elis, L. A., and Simpson, S. 1995. "Informal Sanction Threats and Corporate Crime: Additive Versus Multiplicative Models," *Journal of Research in Crime and Delinquency* (20:3), pp. 233-252.

Ernst & Young. 2008. "Ernst & Young 2008 Global Information Security Survey" (http://faisaldanka.wordpress.com/2008/10/20/ernst-young-2008-global-information-security-survey/).

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

Fox, K. J. 1999. "Reproducing Criminal Types: Cognitive Treatment for Violent Offenders in Prison," *Sociological Quarterly* (40:3), pp. 435-453.

Gefen, D., Rose, G., Warkentin, M., and Pavlou, P. 2005. "Cultural Diversity and Trust in IT Adoption: A Comparison of Potential E-Voters in the USA and South Africa," *Journal of Global Information Management* (13:1), pp. 54-78.

Grasmick, H. G., and Bryjak, G. J. 1980. "The Deterrent Effect of Perceived Severity of Punishment," *Social Forces* (59:2), pp. 471-491.

Grasmick, H. G., and Bursik, R. 1990. "Conscience, Significant Others, and Rational Choice: Extending the Deterrence Model," *Law and Society Review* (24:3), pp. 837-862.

Green, D. E. 1989. "Measures of Illegal Behavior in Individual-Level Deterrence Research," *Journal of Research in Crime and Delinquency* (26:3), pp. 253-275.

Greenberg, J. 1990. "Employee Theft as a Reaction to Underpayment Inequity: The Hidden Cost of Pay Cuts," *Journal of Applied Psychology* (75:5), pp. 561-568.

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

Hollinger, R. C. 1991. "Neutralizing in the Workplace: An Empirical Analysis of Property Theft and Production Deviance," *Deviant Behavior* (12:2), pp. 169-202.

Jarvis, C. B., Mackenzie, S., Podsakoff, P., Mick, D., and Bearden, W. 2003. "A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research," *Journals of Consumer Research* (30:2), pp. 199-218.

Jasso, G. 2006. "Factorial Survey Methods for Studying Beliefs and Judgments," *Sociological Methods & Research* (34:3), pp. 334-423.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y., 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. 1989. "The Deterrent Effect of Perceived Certainty and Severity of Punishment Revisited," *Criminology* (27:4), pp. 721-746.

Klockars, C. B. 1974. *The Professional Fence*, New York: Free Press.

Kohlberg, L. 1969. "Stage and Sequence: The Cognitive-Developmental Approach to Socialization," in *Handbook of Socialization Theory and Research,* D. Goslin (ed.), Chicago: Rand McNally, pp. 347-380.

Law, K., and Wong, C. 1999. "Multidimensional Constructs in Structural Equation Analysis: An Illustration Using the Job Perception and Job Satisfaction Constructs," *Journal of Management* (25:2), pp. 143-160.

Leidner, D., and Kayworth, T. 2006. "A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict," *MIS Quarterly* (30:2), pp. 357-399.

Lim, V. K. G. 2002. "The IT Way of Loafing on the Job: Cyberloafing, Neutralizing and Organizational Justice," *Journal of Organizational Behavior* (23:5), pp. 675-694.

MacKenzie, S. B., Podsakoff, P. M., and Jarvis, C. B. 2005. "The Problem of Measurement Model Misspecification in Behavioral and Organizational Research and Some Recommended Solutions," *Journal of Applied Psychology* (90:4), pp. 710-730.

Malhotra, N., Kim, S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns(IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336-355.

Marcoulides, G., and Saunders, C. 2006. "PLS: A Silver Bullet?," *MIS Quarterly* (30:2), pp. iii-ix.

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

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.

Minor, W. W. 1981. "Techniques of Neutralization: A Reconceptualization and Empirical Examination," *Journal of Research in Crime and Delinquency* (18:2), pp. 295-318.

Moores, T., and Chang, J. 2006. "Ethical Decision Making in Software Piracy: Initial Development and Test of a Four-Component Model," *MIS Quarterly* (30:1), pp. 167-180.

Nagin, D. S., and Paternoster, R. 1993. "Enduring Individual Differences and Rational Choice Theories of Crime," *Law & Society Review* (27:3), pp. 467-496.

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

Parker, D. B. 1976. *Crime by Computer*, New York: Charles Scribner's Sons.

Parker, D. B. 1997. "Information Security in a Nutshell," *Information Systems Security* (6:1), pp. 14-19.

Parker, D. B. 1998. *Fighting Computer Crime: A New Framework for Protecting Information*, New York: John Wiley & Sons.

Paternoster, R., Saltzman, L. F., Waldo, G. P., and Chiricos, T. G. 1982. "Perceived Risk and Deterrence: Methodological Artifacts in Perceptual Deterrence Research," *Journal of Criminal Law and Criminology* (73:3), pp. 1238-1258.

Paternoster, R., and Simpson, S. 1993. "A Rational Choice Theory of Corporate Crime," in *Advances in Criminological Theory: Routine Activity and Rational Choice*, 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 & Society Review* (30:3), pp. 549-584.

Pershing, J. L. 2003. "To Snitch or Not to Snitch? Applying the Concept of Neutralization Techniques to the Enforcement of Occupational Misconduct," *Sociological Perspectives* (46:2), pp. 149-178.

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

Piquero, A. R., and Tibbetts, S. G. 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), pp. 481-510.

Piquero, N. L., Tibbetts, S. G., and Blankenship, M. B. 2005. "Examining the Role of Differential Association and Techniques of Neutralization in Explaining Corporate Crime," *Deviant Behavior* (26:2), pp. 159-188.

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

Pratt, T. C., and Cullen, F. T. 2000. "The Empirical Status of Gottfredson and Hirschi's General Theory of Crime: A Meta-Analysis," *Criminology* (38:3), pp. 931-964.

Priest, T. B., and McGrath, J. H. 1970. "Techniques of Neutralization: Young Adult Marijuana Smokers," *Criminology* (8:2), pp. 185-194.

Puhakainen, P. 2006. *A Design Theory for Information Security Awareness*, Oulu, Finland: University of Oulu.

Rest, J. R. 1979. *Development in Judging Moral Issues*. Minneapolis, MN: University of Minnesota Press.

Rest, J. R., and Narvaez, D. 1994. *Moral Development in the Professions*, Hillsdale, NJ: Lawrence Erlbaum Associates.

Ringle, C. M., Wende, S., and Will, A. 2005. "Smart PLS 2.0," University of Hamburg, Hamburg, Germany (http://www.smartpls.de).

Robinson, S. L., and Kraatz, M. S. 1998. "Constructing the Reality of Normative Behavior: The Use of Neutralization Strategies by Organizational Deviants," *Monographs in Organizational Behavior and Industrial Relations* (23), pp. 203-220.

Rogers, J. W., and Buffalo, M. D. 1974. "Neutralization Techniques: Toward a Simplified Measurement Scale," *Pacific Sociological Review* (17:3), pp. 313-331.

Siponen, M., and 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), pp. 445-472.

Siponen, M., Pahnila, S., and Mahmood, A. 2007. "Employees' Adherence to Information Security Policies: An Empirical Study," in *Proceedings of the IFIP SEC 2007*, Sandton, Gauteng, South Africa, pp. 133-144.

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

Straub, D. W. 1989. "Validating Instruments in MIS Research," *MIS Quarterly* (13:2), pp. 147-169.

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

Straub, D. W., Boudreau, M., and Gefen, D. 2004. "Validation Guidelines for IS Positivist Research," *Communications of the Association for Information Systems* (13:24), pp. 380-427.

Straub, D. W., Carlson, P. J., and Jones, E. H. 1993. "Deterring Cheating by Student Programmers: A Field Experiment in Computer Security," *Journal of Management Systems* (5:1), pp. 33-48.

Straub, D. W., and Karahanna, E. 1998. "Knowledge Worker Communications and Recipient Availability: Toward a Task Closure Explanation of Media Choice," *Organization Science* (9:2), pp. 160-175.

Straub, D. W., and Nance, W. D. 1990. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly* (14:1), pp. 45-62.

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

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

Tangney, J. P. 1995. "Shame and Guilt in Interpersonal Relationships," in *Self-Conscious Emotions: The Psychology of Shame, Guilt, Embarrassment, and Pride*, J. P. Tangney and K. Fischer (eds.), New York: Guilford, pp. 114-141.

Thurman, Q. C. 1984. "Deviance and the Neutralization of Moral Commitment: An Empirical Analysis," *Deviant Behavior* (5), pp. 291-304.

Thurman, Q. C., St. John, C., and Riggs, L. 1984. "Neutralization and Tax Evasion: How Effective Would a Moral Appeal Be in Improving Compliance to Tax Laws?," *Law & Policy* (6:3), pp. 309-327.

Tibbetts, S. G. 1997. "Shame and Rational Choice in Offending Decisions," *Criminal Justice and Behavior* (24:2), pp. 234-255.

Tittle, C. R. 1980. *Sanctions and Social Deviance: The Question of Deterrence*, New York: Praeger.

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

Tudor, J. K. 2000. *IS Security Architecture: An Integrated Approach to Security in the Organization*, Boca Raton, FL: CRC Press.

Vroom, C., and von Solms, R. 2004. "Towards Information Security Behavioural Compliance," *Computers and Security* (23:3), pp. 191-198.

Weber, J. 1992. "Scenarios in Business Ethics Research: Review, Critical Assessment, and Recommendations," *Business Ethics Quarterly* (2:2), pp. 137-160.

Wood, C. 1982. "Policies for Deterring Computer Abuse," *Computers and Security* (1:2), pp. 139-145.

About the Authors

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 holds a Ph.D. in Philosophy from the University of Joensuu, Finland, and a Ph.D. in Information Systems from the University of Oulu. His research interests include IS security, IS development, computer ethics, and philosophical aspects of IS. He has 30 published or forthcoming papers in journals such as *Journal of the Association for Information Systems, European Journal of Information Systems, Information & Organization, Information Systems Journal, Information & Management, DATA BASE, Communications of the ACM, IEEE Computer,* and *IEEE IT Professional.* He has served as a senior and associate editor for the International Conference on Information Systems as well as guest senior editor for the *MIS Quarterly* special issue on Information Systems Security in a Digital Economy. He is a member of the editorial boards of *European Journal of Information Systems, Journal of Organizational and End User Computing,* and *Journal of Information Systems Security.*

Anthony Vance is an assistant professor of Information Systems in the Information Systems Department at the Marriott School of Management, Brigham Young University. Previous to this position, he worked as a visiting research professor in the IS Research Centre in the Department of Information Processing Science at the University of Oulu, Finland. He earned his Ph.D. in Computer Information Systems from Georgia State Unviersity and the University of Paris– Dauphine. He received a B.S. in IS and a Master's of Information Systems Management (MISM), during which he was also enrolled in the IS Ph.D. preparation program, at the Marriott School of Management. Prior to his Ph.D. studies, Anthony worked as an IT security consultant for Deloitte. His work has been published in *Journal of Management Information Systems* and *European Journal of Information Systems.* His research interests are IS security, trust in IS, internal control, and international issues in information systems.