Published online ahead of print June 20, 2008

Information Systems Research
Articles in Advance, pp. 1–20
ISSN 1047-7047 | EISSN 1526-5536

DOI 10.1287/isre.1070.0160
© 2008 INFORMS

User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach

John D'Arcy
Mendoza College of Business, University of Notre Dame, Notre Dame, Indiana 46556,
jdarcy1@nd.edu

Anat Hovav
Korea University Business School, Seoul 136-701 Korea, anatzh@korea.ac.kr

Dennis Galletta
Katz Graduate School of Business, University of Pittsburgh, Pittsburgh, Pennsylvania 15260,
galletta@katz.pitt.edu

Intentional insider misuse of information systems resources (i.e., IS misuse) represents a significant threat to organizations. For example, industry statistics suggest that between 50%–75% of security incidents originate from within an organization. Because of the large number of misuse incidents, it has become important to understand how to reduce such behavior. General deterrence theory suggests that certain controls can serve as deterrent mechanisms by increasing the perceived threat of punishment for IS misuse. This paper presents an extended deterrence theory model that combines work from criminology, social psychology, and information systems. The model posits that user awareness of security countermeasures directly influences the perceived certainty and severity of organizational sanctions associated with IS misuse, which leads to reduced IS misuse intention. The model is then tested on 269 computer users from eight different companies. The results suggest that three practices deter IS misuse: user awareness of security policies; security education, training, and awareness (SETA) programs; and computer monitoring. The results also suggest that perceived severity of sanctions is more effective in reducing IS misuse than certainty of sanctions. Further, there is evidence that the impact of sanction perceptions vary based on one's level of morality. Implications for the research and practice of IS security are discussed.

Key words: IS misuse; IS security; security countermeasures; general deterrence theory; security management; end-user security
History: Sandra Slaughter, Senior Editor; Sue Brown, Associate Editor. This paper was received on July 11, 2006, and was with the authors 7 months for 2 revisions. Published online in *Articles in Advance*.

Introduction

A United Nations (2005, p. xxiii) report describes "tens, if not hundreds of billions of dollars" of annual worldwide economic damage caused by compromises in information security. The latest survey from the Computer Security Institute (Richardson 2007) reported losses averaging $345,000 among the 39% of respondents able to estimate losses and willing to report them. Interestingly, research indicates that between 50%–75% of security incidents originate from within an organization (Ernst and Young 2003, InformationWeek 2005), often perpetrated by disgruntled employees (Standage 2002). Because only a fraction of security incidents are actually discovered (Hoffer and Straub 1989, Whitman 2003), the reported statistics likely underestimate the problem. Moreover, organizations are often reluctant to disclose such information, fearing negative publicity that could damage their image and/or stock price (Hoffer and Straub 1989, Richardson 2007).

The number of security breaches that involve internal misuse of IS resources highlight the importance of understanding how organizations can reduce such behavior. Information security researchers and practitioners recommend various countermeasures that can be used to combat IS misuse (Dhillon 1999, Parker 1998, Straub and Welke 1998). Based on the predictions of general deterrence theory (GDT), procedural and technical countermeasures can serve as deterrent mechanisms by increasing the perceived certainty and severity of punishment for IS misuse (Gibbs 1975, Straub and Welke 1998, Tittle 1980).

This study will introduce and empirically test an extended GDT model that posits that user awareness of security countermeasures (i.e., security policies, security education, training, and awareness (SETA) programs, computer monitoring) directly impacts user perceptions of the certainty and severity of sanctions associated with IS misuse, which in turn have a direct effect on IS misuse intention. The results suggest a modified version of GDT in the IS security context to advance our understanding of the underlying process through which security countermeasures impact users' intentions to misuse information systems. The results also have important implications for the practice of IS security management.

Literature Review

Organizational strategies for reducing systems risk generally fall into four distinct stages—deterrence, prevention, detection, and recovery (Forcht 1994, Straub and Welke 1998). Straub and Welke (1998) refer to these four stages collectively as the *Security Action Cycle*. Based on this model, effective IS security management should aim to maximize the number of deterred and prevented abusive acts and minimize those that are detected and punished (Theoharidou et al. 2005). The current study focuses on stage one of the Security Action Cycle—that is, deterrent strategies for reducing IS misuse. Deterring IS misuse can be accomplished with a mix of procedural and technical controls such as security policies, SETA programs, and monitoring software (e.g., Dhillon 1999, Parker 1998, Straub and Welke 1998).[1] Following Straub (1990), we use the term "security countermeasures" to collectively describe these controls.

Security policies contain detailed guidelines for the proper and improper use of organizational IS resources (Whitman et al. 2001). From a deterrence perspective, security policies rely on the same underlying mechanism as societal laws: providing knowledge of what constitutes unacceptable conduct increases the perceived threat of punishment for illicit behavior (Lee and Lee 2002). SETA programs have a similar deterrent effect, achieved through ongoing organizational efforts (e.g., security briefings or courses) that reinforce acceptable usage guidelines and emphasize the potential consequences for misuse. Computer monitoring includes tracking employees' Internet use, recording network activities, and performing security audits (Panko and Beh 2002, Urbaczewski and Jessup 2002). These surveillance activities are thought to deter IS misuse by increasing the perceived chances of detection and punishment for such behavior (Parker 1998, Straub and Nance 1990).

It should be noted that other commonly used security countermeasures (e.g., access controls) may also have deterrent value (Straub 1990, Lee et al. 2004). However, the literature considers such controls to be preventive mechanisms, and therefore they are not included in this study.

Empirical studies have assessed the effectiveness of a variety of security countermeasures. Most of these studies used GDT (or some variation of GDT) as a theoretical base. The rationale for GDT is that security countermeasures can serve as deterrent mechanisms by increasing perceptions of the certainty and severity of punishment for IS misuse, thereby reducing the incidence of such behavior. Despite the theoretical basis, deterrence-based research in IS has been inconclusive. Although some studies provide evidence that certain countermeasures help deter IS misuse (e.g., Gopal and Sanders 1997, Kankanhalli et al. 2003, Straub 1990), others suggest that such controls have little, if any, deterrent effect (Foltz 2000, Harrington 1996, Lee et al. 2004, Wiant 2003).

Straub (1990) surveyed IS personnel in 1,211 organizations and found that security policy statements and technical controls were associated with lower levels of computer abuse. Similarly, Kankanhalli et al. (2003) surveyed a group of IS managers and found that spending more time on security activities and using more advanced security software were associated with higher perceived security effectiveness. However,

[1] From the perspective of the Security Action Cycle (Straub and Welke 1998), computer monitoring is a form of detection. However, the model also includes a deterrence feedback loop through which detective controls can deter future IS misuse, as long as potential abusers become aware of such controls.

Wiant's (2003) survey of 140 IS managers found that organizational use of security policies was not associated with diminished quantity or severity of security incidents.

Studies that turned to the individual level for assessing the impact of security countermeasures have encountered similar equivocality. Gopal and Sanders (1997) found that policy statements prohibiting software piracy and warning of its legal consequences resulted in lower piracy intentions. Conversely, Foltz (2000) found that a university computer usage policy had no effect on IS misuse intentions and behaviors involving modifying, stealing, or destroying software and data. Harrington (1996) assessed the impact of codes of ethics on a variety of computer abuse judgments and intentions of IS employees. Results indicated that general codes of ethics had no effect on computer abuse judgments and intentions, while IS-specific codes of ethics had a slight effect on computer sabotage. Lee et al. (2004) found that security policies and systems had no impact on the computer abuse behaviors of a sample of Korean managers and MBA students.

Although these previous studies are highly informative and provide the groundwork for the current analysis, they do not quantify the existence of security countermeasures from the user's perspective. Because users and managers might have widely differing perceptions (Finch et al. 2003, Foltz 2000), our study focuses on the impact of *user awareness* of deterrent countermeasures on IS misuse intentions. By focusing on user awareness of security countermeasures, we aim to extend prior work and provide a more comprehensive lens for studying the impact of security on end-user behavior.

In addition, although security researchers and practitioners have long proclaimed the benefits of SETA programs (e.g., Parker 1998, Straub and Welke 1998, Hansche 2001), there is limited empirical research on their deterrent effects. Assessing the deterrent capabilities of SETA programs is particularly salient for practitioners because industry surveys indicate that such programs are becoming a strategic priority within many organizations (Berinato 2005, Deloitte 2005).

There is also a trend toward monitoring employee computer usage in the workplace. Recent surveys found that approximately 76% of organizations monitor their employees' e-mail and website usage (AMA 2005), while 63% conduct security audits (Richardson 2007). Within the IS security literature, active and visible security efforts in the form of computer monitoring and auditing are recommended approaches for deterring IS misuse based on the theoretical perspective of GDT (Kankanhalli et al. 2003, Straub 1990). However, while a significant body of research has examined the impact of control-based[2] computer monitoring on job-related variables such as attitudes (e.g., Furnell et al. 2000, Spitzmuller and Stanton 2006, Stanton and Weiss 2000), satisfaction (Alder et al. 2006, George 1996, Urbaczewski and Jessup 2002), trust (Alder et al. 2006), and security-conscious behaviors (Stanton et al. 2005), there is a dearth of empirical work that has assessed the deterrent effect of computer monitoring on end users' misuse intention.

The study also seeks to extend prior GDT-based assessments of security countermeasures by directly measuring GDT's two main constructs, perceived certainty and perceived severity of sanctions, thereby examining the underlying process through which security countermeasures impact an individual's intention to commit IS misuse. This represents an explicit test of GDT based on its original specification (e.g., Gibbs 1975).

Extended GDT Model

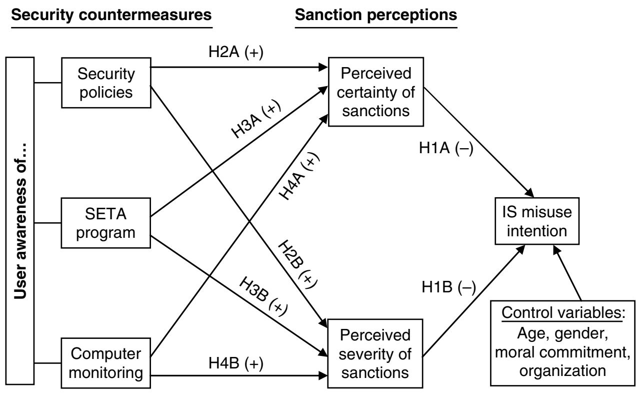
Our proposed theoretical model, shown in Figure 1, integrates user awareness of security countermeasures, sanction perceptions, and IS misuse intentions. The model expands on GDT by including security countermeasures as antecedents to perceived certainty and perceived severity of sanctions. That is, security countermeasures influence users' IS misuse intentions indirectly through their effects on sanction perceptions.

IS Misuse Intention

IS misuse intention is defined as an individual's intention to perform a behavior that is defined by the

[2] Monitoring research generally distinguishes between performance-based and control-based computer monitoring. Performance-based monitoring is used to measure employee productivity (e.g., tracking a data entry clerk's keystrokes). Control-based monitoring is used to gain compliance with organizational rules and regulations (Urbaczewski and Jessup 2002). Control-based computer monitoring is the focus of this paper.

Figure 1 The Extended GDT Model



organization as a misuse of IS resources (Magklaras and Furnell 2002). One's intention is thought to capture the motivational factors that affect a behavior (Ajzen 1988). The domain of IS misuse is quite varied, ranging from behaviors that are unethical and/or inappropriate (e.g., personal use of company e-mail) to those that are illegal (e.g., accessing confidential company information). This study attempts to examine a range of IS misuse behaviors in various contexts by introducing a set of scenarios of misuse. Specifically, we focus on four IS misuse intentions: sending an inappropriate e-mail, use of unlicensed (pirated) software, unauthorized access to computerized data, and unauthorized modification of computerized data.

- Survey results indicate that 68% of U.S. employees who use e-mail at work have sent or received inappropriate e-mail via their work account that could place their company at financial or legal risk (Fortiva 2005).[3]
- A report by the Business Software Alliance (BSA 2005) estimates that 35%–40% of business applications used globally are pirated copies.
- Unauthorized access to and modification of computerized data have been reported as two of the most common types of breaches in organizations (Berinato 2005, Richardson 2007).

Although these four behaviors do not enumerate all possible IS misuse types, we judged them as representative of typical IS misuse issues often encountered by organizations, including privacy, accuracy, property, and accessibility (Mason 1986). Moreover, all of these activities have been identified as serious threats to organizations (e.g., Harrington 1996, Whitman 2003).

Perceived Certainty and Severity of Sanctions

GDT predicts that the greater the certainty and severity of sanctions for an illicit act, the more individuals are deterred from that act (Gibbs 1975). In this study, *certainty of sanctions* refers to the probability of being punished, and *severity of sanctions* refers to the degree of punishment (Tittle 1980) associated with committing IS misuse.

Deterrence research has shown consistently that sanction fear predicts various criminal and deviant behaviors (Nagin and Pogarsky 2001, Tittle 1980). For example, perceived certainty of sanctions (PC) and perceived severity of sanctions (PS) were both negatively associated with the intention to engage in several socially deviant behaviors such as lying to one's spouse, sitting during the national anthem, and smoking marijuana, as well as deviant behavior in the workplace such as stealing from an employer and making personal use of an employer's equipment (e.g., Cole 1989, Hollinger and Clark 1983, Nagin and Pogarsky 2001, Tittle 1980). Although a large number of criminological studies have found PC to have a stronger deterrent effect than PS (see Paternoster 1987 and von Hirsch et al. 1999), a few studies found that the deterrent influence of PS is just as strong, if not stronger, than that of PC (Carnes and Englebrecht 1995, Freeman and Watson 2006, Klepper and Nagin 1989, Nagin and Pogarsky 2001). Within the IS domain, Skinner and Fream (1997) found that PS was more influential than PC on college students' intentions to illegally access other students' computer accounts. Based on these results, we do not predict the relative deterrent capacity provided by either PC or PS. Instead, we take a more conservative approach based on the original specification of GDT (e.g., Gibbs 1975) and hypothesize that both are inversely related

[3] Such risks include damages caused by e-mail-borne viruses and phishing scams. In addition, organizations can be held liable for employee distribution of offensive e-mail messages. Approximately 13% of U.S. employers have been charged with discrimination or sexual harassment stemming from e-mail misuse (AMA 2005). One noteworthy case involves Chevron Corporation, which was ordered to pay female employees $2.2 million to settle a sexual harassment lawsuit stemming from inappropriate e-mail circulated by male employees (Verespej 2000).

to IS misuse intention:

Hypothesis 1A (H1A). *Perceived certainty of sanctions is negatively associated with IS misuse intention.*

Hypothesis 1B (H1B). *Perceived severity of sanctions is negatively associated with IS misuse intention.*

Security Policies

Although various definitions and meanings have been used to describe security policies (Baskerville and Siponen 2002), we adopt a broad definition as "guiding statements of goals to be achieved" (Gaston 1996, p. 175) with regard to information security. At the operational level, a security policy defines rules and guidelines for the proper use of organizational IS resources (i.e., acceptable use guidelines) (Whitman et al. 2001). Consistent with several earlier IS deterrence studies (Lee et al. 2004, Straub and Nance 1990, Straub 1990), we consider security policies in this manner.

Prior research suggests that laws and legal sanctions can discourage members of a society from engaging in illicit behavior (e.g., Tittle 1980, von Hirsch et al. 1999). By definition, the term "law" includes prescribed actions and enforcement by a controlling authority. Deterrence is therefore achieved by providing knowledge of what constitutes unacceptable or illegal conduct, and then creating a fear of, or desire to avoid, negative consequences through perceived enforcement (Tittle 1980). Insofar as security policies are the equivalent of organizational laws (Whitman 2004), we expect that such policies rely on the same underlying mechanism in deterring IS misuse. They are expected to increase the perceived certainty of sanctions (Lee and Lee 2002) because they imply the existence of enforcement via organizational security activities (Whitman 2004). The acceptable usage rules and guidelines outlined in security policies also suggest that penalties will occur should the user choose not to adhere. Indeed, security policies can be the basis for litigation or internal measures that punish IS misuse behavior (Straub and Nance 1990, Whitman and Mattord 2005) and should therefore increase perceived severity of sanctions. Further justification for this effect comes from the protection motivation literature (e.g., Rogers 1983), where studies (e.g., MacMath and Prentice-Dunn 2005, Pechmann et al. 2003) found that information containing persuasive messages influence individuals' threat appraisal process, thereby increasing the perceived severity of consequences for risky (or potentially risky) behaviors. Finally, the absence of security policies can lead to a misunderstanding of acceptable system use (Straub 1990), and lead users to assume that IS misuse is not subject to enforcement and has little to no consequences. Hence, we hypothesize that:

Hypothesis 2A (H2A). *User awareness of IS security policies is positively associated with perceived certainty of sanctions.*

Hypothesis 2B (H2B). *User awareness of IS security policies is positively associated with perceived severity of sanctions.*

Security Education, Training, and Awareness (SETA) Program

The best way to ensure the viability of a security policy is to make sure users understand it and accept necessary precautions (Whitman et al. 2001). Information security researchers have argued that SETA programs are necessary to control IS misuse (Dhillon 1999, Parker 1998, Whitman 2004). SETA programs can take many forms, and focus on providing users with general knowledge of the information security environment, along with the skills necessary to perform any required security procedures (Lee and Lee 2002, Whitman et al. 2001). For example, a SETA program might review the organization's code of conduct and hold a discussion of moral dilemmas related to information security (Harrington 1996, Workman and Gathegi 2007). SETA programs can also be included within more general organizational training strategies that promote awareness of day-to-day physical security issues within the organization (Furnell et al. 2002).

Regardless of the form the SETA program takes, its foundation is based on the information security policy; SETA programs often use the security policy as the primary training tool (Peltier 2005). However, the scope of the SETA program extends beyond just "awareness of security policy" and often includes *ongoing* efforts to (1) convey knowledge about information risks in the organizational environment, (2) emphasize recent actions against employees for security policy violations, and (3) raise employee awareness of their responsibilities regarding organizational information resources (Straub and Welke 1998, Wybo and Straub 1989). These ongoing efforts might include a combination of security awareness e-mails and newsletters, briefings on the consequences of IS misuse, and periodic security refresher courses (Hansche 2001, von Solms and von Solms 2004).

Research has found that public awareness and informational campaigns can reduce certain illicit behaviors such as drunk driving (Ferguson et al. 1999, Nienstedt 1985), shoplifting (McNees et al. 1976, Sacco 1985), and workplace drug use (Quazi 1993). Such programs deter those behaviors by reviewing current laws and by emphasizing the likelihood of apprehension and the corresponding penalties for violating the law (Ferguson et al. 1999, Sacco 1985). In a similar vein, ongoing SETA efforts can deter misuse attempts by providing information about correct and incorrect usage of information systems, punishment associated with incorrect usage, and knowledge of organizational enforcement activities (Wybo and Straub 1989). As with security policies, SETA programs also enable organizations to hold employees accountable for IS misuse, permitting these organizations to punish deviant behavior (Whitman and Mattord 2005). Straub and Welke (1998, p. 445) assert that a major reason for initiating a SETA program is to "convince potential abusers that the company is serious about security and will not take intentional breaches of this security lightly," thereby stressing the perceived certainty and severity of sanctions for IS misuse. Hence, we hypothesize:

Hypothesis 3A (H3A). *User awareness of SETA programs is positively associated with perceived certainty of sanctions.*

Hypothesis 3B (H3B). *User awareness of SETA programs is positively associated with perceived severity of sanctions.*

Computer Monitoring

Computer monitoring is often used by organizations to gain compliance with rules and regulations (Urbaczewski and Jessup 2002). Within the IS context, examples include tracking employees' Internet use, recording network activities, and performing security audits (Panko and Beh 2002, Urbaczewski and Jessup 2002). Deterrence studies from criminology and sociology suggest that monitoring and surveillance increase perceived certainty of sanctions (e.g., Alm and McKee 2006, Ferguson et al. 1999, Kinsey 1992, Wentzel 2004). There is also evidence that such techniques increase perceived sanction severity. Kinsey (1992) found that prior exposure to IRS auditing practices was positively associated with perceived severity of tax evasion penalties. Other studies reported a positive relationship between IRS audits and tax compliance (e.g., Dubin et al. 1990, Witte and Woodbury 1985), which is consistent with the notion that monitoring increases sanction perceptions.

Extending these findings to the IS context suggests that monitoring and surveillance activities can reduce IS misuse by increasing the perceived certainty and severity of sanctions for such behavior (Parker 1998, Straub and Nance 1990). Monitoring employee computing activities is an active security measure that increases the organization's ability to detect IS misuse, thus increasing the perceived certainty *and frequency* of sanctions. Moreover, monitoring techniques enable the detection of more serious and deliberate misuse incidents that are likely subject to severe punishment. Exposure to others who have been punished as an example should therefore increase users' perceived severity of sanctions. Further, monitoring practices signal the computing activities management views as most important and which violations will likely receive the most punishment. Users can interpret the devotion of resources to monitoring as a warning of severe punishment for violations. Therefore, it can be expected that if a user is made aware of monitoring practices, their perceptions of being caught and subsequently punished for IS misuse will be increased. Hence, we hypothesize:

Hypothesis 4A (H4A). *User awareness of computer monitoring practices is positively associated with perceived certainty of sanctions.*

Hypothesis 4B (H4B). *User awareness of computer monitoring practices is positively associated with perceived severity of sanctions.*

Control Variables

Research suggests additional variables that should be included because of their potential influence on IS misuse intention. Three variables that have been shown to predict various forms of IS misuse are age, gender, and morality (e.g., Gattiker and Kelley 1999, Leonard and Cronan 2001, Leonard et al. 2004). This study seeks to assess the impact of sanction perceptions on IS misuse intention beyond these known predictors. Therefore, age, gender, and moral commitment are included as control variables on the relationships between perceived certainty and severity of sanctions and IS misuse intention. Including moral commitment as a control is particularly important because prior research suggests that the influence of sanction perceptions may diminish once moral considerations are taken into account (Paternoster 1987, Wentzel 2004). Hence, our model provides for a more stringent test of the effects of perceived certainty and severity of sanctions on IS misuse intention. Following Banerjee et al. (1998), organization is also included as a control variable to account for potential differences in IS misuse intention among users in different organizations.

Methodology

To test the relationships implied by the research model and the research hypotheses, this field study used a survey instrument for data collection. The first part of the survey was designed to capture respondents' perceptions of the certainty (PC) and severity (PS) of organizational sanctions for engaging in IS misuse, their moral commitment (MC), and their IS misuse intention (INT). The second part measured respondent awareness of security policies, SETA programs, and computer monitoring, as well as the other variables in the research model.

The PC, PS, MC, and INT constructs were measured using four misuse scenarios. Scenarios were chosen because they are considered nonintrusive, provide an unintimidating way to respond to sensitive issues (Nagin and Pogarsky 2001), and result in improved internal validity (Harrington 1996, Kerlinger 1986). The four scenarios included in the survey are: (1) sending an inappropriate e-mail message—developed for this study; (2) use of unlicensed (pirated) software—modified from Christensen and Eining (1994) and Pierce and Henry (2000); (3) unauthorized access to computerized data—modified from Paradice (1990) and Pierce and Henry (2000); and (4) unauthorized modification of computerized data—modified from Paradice (1990).

Guidelines from the literature (e.g., Finch 1987) were utilized in creating/modifying the scenarios. Specifically, we selected scenarios that would appear plausible to the respondents and avoided descriptions of disastrous IS misuse events to improve respondents' ability to project themselves into the scenarios. The scenarios were pretested on a group of 26 employed professionals taking evening MBA classes at a large mid-Atlantic U.S. university. Their feedback indicated a general consensus that the scenarios were realistic and that participants had little difficulty placing themselves in the hypothetical position of the scenario characters. The feedback also resulted in minor wording changes to some of the scenarios to remove ambiguities.

For each of the scenarios, respondents replied to questions measuring PC, PS, MC, and INT for the particular misuse behavior depicted in the scenario (see Appendix A for the scenarios and accompanying survey items).[4] INT was measured using a two-item scale consisting of one original item and one item adapted from Leonard and Cronan (2001). MC was

[4] An anonymous reviewer suggested that respondents may have shifted perspectives when responding to the INT, PC, and PS items because the PC and PS items ask participants to consider their own place of employment, while this is not stated explicitly for the INT items. While recognizing that such a shift is possible, we believe it is more likely that respondents maintained a consistent perspective for the INT, PC, and PS items—that is, they considered all of these items within the context of their own workplace. First, the survey introduction stated that the scenarios depict common computing behaviors within an organizational setting. Hence, it seems reasonable that when respondents projected their IS misuse behaviors through the INT items, they projected them with their own work context in mind. Second, our approach of having participants play the role in the scenario while measuring the antecedent variables from the organizational perspective is consistent with other scenario-based IS studies (e.g., Banerjee et al. 1998). It is also similar to the Bachman et al. (1992) study of male college student sexual offenders in which participants estimated the probability they would act as the scenario male did, while also estimating the likelihood that this character would be caught and punished by the respondent's university. Finally, the variance explained by the combination of PC and PS constructs in the current study (discussed in the "Analysis and Results" section) is consistent with a number of deterrence studies (see Paternoster 1987 for review) that utilized these same constructs. This consistency supports our conceptualization of the INT, PC, and PS constructs and the notion that participants maintained a single contextual perspective (i.e., their own workplace) when responding to these items.

measured with a single item adapted from Lin et al. (1999)[5] that gauged respondents' moral judgment of the scenario behavior. Scales for PC and PS were each adapted from Peace et al. (2003). Because the goal of this study was to examine generalized patterns of IS misuse rather than specific behaviors depicted in each scenario, we created composite measures of PC, PS, MC, and INT by summing the responses to these items across the four misuse scenarios. Therefore, our measures of PC, PS, MC, and INT represent general indices of these variables. Silberman (1976) provides a theoretical rationale for using composite measures by suggesting that we may be able to predict generalized patterns of deviance better than specific deviant acts. This approach has also been used in prior deterrence studies outside of the IS discipline (e.g., Grasmick and Bryjak 1980, Hollinger and Clark 1983, Silberman 1976) and in prior studies of IS misuse (Banerjee et al. 1998, Skinner and Fream 1997).

The IS security literature was examined for validated measures involving user awareness or perceptions of security countermeasures. However, existing measures (e.g., Lee et al. 2004, Straub 1990) are either operationalized at the organizational level or are written from the perspective of IS security administrators. Hence, original scales (see Appendix B) that measure users' awareness of security policies, SETA programs, and computer monitoring within their organizations were developed for this study. A preliminary version of the full survey instrument was tested for clarity and validity using a panel of six MIS faculty members and a pilot sample of 54 computer-using professionals. Based on the feedback gathered and analysis of the pilot data, some of the items were slightly modified prior to final survey administration.

Sample and Procedure

An e-mail invitation to complete the online survey was sent to 805 employed professionals, of which 304 responded, for an initial response rate of 38%. Incomplete or otherwise unusable entries were discarded from the data set, leaving 269 usable responses (33%). A summary of the demographic characteristics of respondents is provided in Table 1.

Table 1 Demographic Characteristics of Respondents

	Survey participants ($n = 269$)	
Gender		
Male	167	62.1%
Female	102	37.9%
Age		
18–24	16	5.9%
25–34	92	34.2%
35–44	88	32.7%
45–54	57	21.2%
55 and over	16	5.9%
Position		
Managerial	61	22.7%
Technical	105	39.0%
Professional staff	88	32.7%
Administrative	15	5.6%
Industry		
Advertising/Marketing	14	5.2%
Aerospace	61	22.7%
Financial services	57	21.2%
Information technology	73	27.1%
Manufacturing	51	19.0%
Other	13	4.8%
Company size (no. of employees)		
Less than 100	48	17.8%
100–499	0	0.0%
500–999	4	1.5%
1,000–2,499	73	27.1%
2,500–9,999	0	0.0%
More than 9,999	144	53.5%
Computer use at work (hrs./day)		
Range	3–12	
Mean	7.47	
Std. deviation	1.57	

The pool of survey participants was obtained from eight companies located across the United States. Initially, 12 U.S.-based companies were identified from personal and research institute contacts as possible participants in the study. Either the CEO or the CIO within each company received a letter explaining the purpose of the research and inquiring about the firm's willingness to participate. The organizations were offered a report of the study's findings as an incentive to participate. Eight companies agreed to participate, three companies declined due to time constraints, and one company did not respond. Each of the participating companies provided a contact person with whom the researchers worked to facilitate survey administration. The contact persons were instructed to select a sample of employees from various user departments to receive the survey.

[5] The moral commitment measure is a summation (composite) of individuals' responses over four scenarios, so some level of generality is captured in this measure (Cronbach's alpha = 0.64).

To test for nonresponse bias, we compared the participating and nonparticipating companies' business type (coded as 1 = public; 2 = private), industry (coded as 1 = manufacturing; 2 = service; 3 = other), revenue, and number of employees. Results of *t*-tests for revenue and number of employees were not significant, and Fisher's exact tests showed no significant relationships for either business type or industry. We also tested for nonresponse bias among individuals by comparing responses of early and late respondents (Armstrong and Overton 1977). Early respondents were those who responded within one week. The two samples were compared on all study variables and on age, gender, position, and organizational tenure. All *t*-test comparisons between the means of the early and late respondents showed no significant differences except for age[6] (early = 2.8, late = 3.1; $p = 0.032$), which suggests a slight bias toward younger employees as early respondents.

Analysis and Results

Partial Least Squares Analysis

Because several new or modified scales were utilized in this study, we first assessed the measures using an independent sample of 238 evening MBA students from two mid-Atlantic U.S. universities. Exploratory factor analysis was conducted on the reflective scales and the formative scales were analyzed using techniques discussed later in this section. The results were largely consistent with those of the confirmatory analysis (reported in Tables 2–4) and therefore are not included here for purposes of brevity. PLS-Graph 3.00 was used for confirmatory analysis of the measurement items and for hypotheses testing. PLS was selected for two main reasons. First, PLS does not impose normality requirements on the data. Formal tests indicated that item responses were not all normally distributed in this study (see Appendix C). Second, PLS can handle both reflective and formative scales, both of which are used in this study. Indicators of a formative scale represent different dimensions of a construct, whereas reflective indicators represent a single, underlying concept (Diamantopoulos and Winklhofer 2001, Jarvis et al. 2003).

Following criteria specified in Jarvis et al. (2003), we modeled security policies, SETA, and computer monitoring as formative based on the reasoning that certain indicators can occur independently of the others within these constructs. For example, in terms of computer monitoring, user awareness of e-mail monitoring may not be related to awareness of the organization's monitoring of unauthorized software usage. The same logic can be applied to the indicators of the security policies and SETA constructs. All other scales in the study were modeled as reflective. Following the recommended two-stage procedure (Anderson and Gerbing 1988), we assessed the measurement model first, followed by the structural relationships.

Measurement Model

The adequacy of the reflective scales was assessed through conventional tests of convergent validity, discriminant validity, and reliability. For convergent validity, all factor loadings should exceed 0.7 and average variance extracted (AVE) for each construct should exceed 0.5 (Fornell and Larcker 1981, Gefen and Straub 2005). As seen in Table 2, both criteria are met and therefore convergent validity is satisfactory. For discriminant validity, the square root of the AVE for each construct should be larger than the interconstruct correlations, and items should load more strongly on their corresponding construct than on other constructs (i.e., loadings should be higher than cross-loadings) (Gefen and Straub 2005). As shown in Table 3, the square root of AVE for each construct exceeds the correlations between that and all other constructs. The results in Table 3 also show that all items load more highly on their own construct than on other constructs. Hence, the criteria for

Table 2 Loadings, Cross-Loadings, and AVEs for Reflective Scales

Construct	Items	IS misuse intention	Perceived certainty	Perceived severity	AVE
IS misuse intention (INT)	INT1	**0.967**	−0.259	−0.318	0.93
	INT2	**0.964**	−0.246	−0.310	
Perceived certainty (PC)	PC1	−0.262	**0.969**	0.616	0.94
	PC2	−0.246	**0.971**	0.532	
Perceived severity (PS)	PS1	−0.304	0.578	**0.966**	0.93
	PS2	−0.324	0.565	**0.965**	

Notes. Procedures from Gefen and Straub (2005) were used to calculate the cross-loadings. Boldface numbers are the item loadings on the constructs.

[6] Age was coded as follows: 1 = 18–24; 2 = 25–34; 3 = 35–44; 4 = 45–54; 5 = 55 and over.

Table 3 **Reliability and Interconstruct Correlations for Reflective Scales**

Construct	Composite reliability	IS misuse intention	Perceived certainty	Perceived severity
IS misuse intention (INT)	0.97	**0.96**		
Perceived certainty (PC)	0.96	−0.26*	**0.97**	
Perceived severity (PS)	0.96	−0.33*	0.59*	**0.96**

Note. Boldface items are the square root of the average variance extracted (AVE).

*Significant at the 0.01 level.

discriminant validity are met. Reliability was assessed using composite reliability, a measure of internal consistency included in the PLS output. As shown in Table 3, the composite reliabilities of all constructs are above the recommended 0.70 threshold (Fornell and Larcker 1981).

Formative scales are not subject to the same validity and reliability criteria as described above (Diamantopoulos and Winklhofer 2001, Jarvis et al. 2003). Reliability testing is irrelevant because the measures of a formative construct are not necessarily correlated. However, item weights can be examined to identify their relevant importance in forming each construct (Chin 1998). As seen in Appendix B, all item weights are significant at the 0.10 level or better, except P5, SETA2, and M2. Although it has been suggested that nonsignificant items should be removed from formative scales, methodologists also caution that eliminating any item may change the construct meaning and adversely affect content validity (Diamantopoulos and Winklhofer 2001, Jarvis et al. 2003). With this in mind, we carefully analyzed items P5, SETA2, and M2. Item P5 could be construed a number of ways[7] (e.g., whether the employee is allowed to take the computer home, browse the Web, etc.), and therefore may not fit within the scope of our security policies definition. Items SETA2 and M2 are captured in a more general sense elsewhere in their respective constructs, and therefore removing these items did not seem to alter the constructs' meanings. We also ran structural models both with and without items P5, SETA2, and M2 and the direction and significance of the path coefficients remained the same. Hence, items P5, SETA2, and M2 were excluded from the remaining analyses.

Techniques from prior IS studies were used to assess the convergent and discriminant validity of the formative scales (Glenn et al. 2006, Loch et al. 2003, Patnayakuni et al. 2006). First, following Loch et al. (2003), we created a "weighted" score for each item by multiplying its value by its PLS weight. The weighted scores were then summed to create a composite score for each formative construct. Subsequently, each weighted item was correlated against the composite score for each construct. In essence, each item's correlation with its intended construct represents a "loading," whereas its correlations with other constructs represent the "cross-loadings" (Patnayakuni et al. 2006). The results of the correlation analysis revealed that all measures of the same construct (i.e., intermeasure correlations) are significantly correlated ($p < 0.01$), thus providing evidence of convergent validity (Loch et al. 2003). Also, as shown in Table 4, each item's correlation with its own construct is higher than its correlations with other constructs. Hence, there is evidence of discriminant validity. It is worth noting, however, that certain items within the security policies and SETA program scales are highly correlated. Thus, while the discriminant validity criteria suggest that our newly developed security policies and SETA program scales measure distinct constructs, future research should continue to refine

Table 4 **Item-to-Construct Correlation vs. Correlations with Other Constructs**

Construct	Items	Security policies	SETA program	Computer monitoring
Security policies (P)	P1	**0.810**	0.482	0.432
	P2	**0.879**	0.613	0.485
	P3	**0.813**	0.535	0.498
	P4	**0.830**	0.698	0.449
SETA program (SETA)	SETA1	0.433	**0.771**	0.391
	SETA3	0.612	**0.790**	0.495
	SETA4	0.715	**0.930**	0.510
	SETA5	0.563	**0.811**	0.504
Computer monitoring (M)	M1	0.474	0.507	**0.850**
	M3	0.403	0.333	**0.690**
	M4	0.349	0.390	**0.731**
	M5	0.484	0.427	**0.693**
	M6	0.354	0.348	**0.710**

Notes. All intermeasure and item-to-construct correlations are significant at the 0.01 level. Boldface numbers are the item-to-construct correlations.

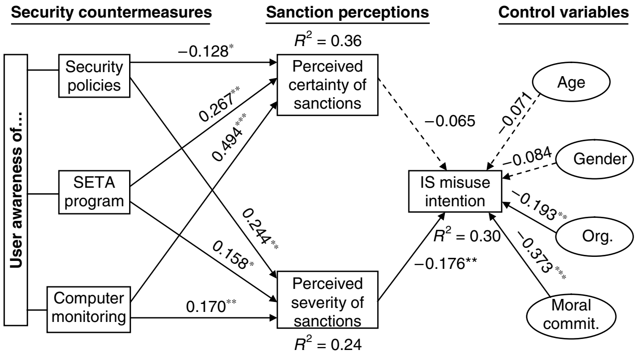
[7] We are grateful to an anonymous reviewer for pointing this out.

these measures to better distinguish between the two constructs.

We also tested for multicollinearity within the formative scales. Whereas multicollinearity is desirable for reflective scales, excessive collinearity within formative scales can make the construct less stable (Jarvis et al. 2003). Following Glenn et al. (2006), we ran a series of regression models with each item serving as the dependent variable and the other items designated as independent variables. All the variance inflation factors (VIF) in the regression models were less than 2.3, which is well below the usual cutoff level of 10.0 and within a more conservative cutoff level of 5.0 (Hair et al. 1998). Hence, multicollinearity problems were not found in the formative scales.

Finally, we assessed the extent of common method variance (CMV) with two tests. First, we performed Harmon's one factor test (Podsakoff et al. 2003) by including all reflective items in a principal components factor analysis. The results revealed three factors with no single factor accounting for a majority of variance, suggesting no substantial CMV among the reflective scales. Second, we performed Lindell and Whitney's (2001) technique in which a theoretically unrelated construct (called the *marker variable*) is used to adjust correlations among the study variables to account for CMV. Because we did not intentionally include an unrelated measure in our study (due to survey length), a weakly related construct—computer self-efficacy[8]—was chosen and its average correlation with the principal study variables ($r = 0.11$) was used as the CMV estimate. Following Malhotra et al. (2006), we developed a CMV-adjusted correlation matrix and examined the CMV-adjusted structural relationships in our research model. The CMV-adjusted structural model was estimated using LISREL 8.5.[9] With the exception of the path from PS to INT (which dropped from $p < 0.01$ to $p < 0.05$), the direction and significance of the paths remained unchanged from those in Figure 2. Further, the explained variance for the PC, PS, and INT variables remained relatively stable, at 30%, 21%, and 33%, respectively. Taken together, the above tests provide reasonable evidence that CMV was not substantial in this study.

Figure 2 **Results of PLS Structural Model Analysis**



Note. Paths in dashes are not significant ($p > 0.10$).
$^{*}p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$.

Structural Model

The hypotheses were tested by examining the structural model. The test of the structural model includes estimating the path coefficients, which indicate the strength of the relationships between the independent and dependent variables, and the R^2 value (the variance explained by the independent variables) (Chin 1998). A bootstrapping resampling procedure (500 samples) was used to determine the significance of the paths within the structural model. Results of the analysis are shown in Figure 2 and summarized in Table 5.

As seen in Figure 2, the R^2 values for all endogenous constructs exceed 10%, implying a satisfactory and substantive model (Falk and Miller 1992). The three security countermeasures explain 36%[10] of the variance in PC and 24% of the variance in PS. The

[8] Computer self-efficacy was included in the survey but not used in the research model. The construct was measured with six items (Cronbach's alpha = 0.87) taken from Compeau and Higgins's (1995) 10-item scale.

[9] LISREL was used for this analysis because PLS-Graph requires a raw data file (not correlation matrix) for input. We acknowledge that direct comparisons between our PLS and LISREL structural model analyses are not appropriate due to underlying differences in the two statistical techniques. However, the separate results do provide evidence that CMV was not a serious issue in this study. It should also be noted that the security policies, SETA program, and computer monitoring constructs were modeled as reflective in the CMV-adjusted structural model because formative measures can cause identification problems in LISREL (Chin 1998).

[10] Considering that the significant negative correlation between security policies and PC has no theoretical basis, we reran the model without the path from security policies to PC. The R^2 for PC dropped slightly to 0.35.

Table 5 Summary of Hypotheses Tests

Hyp. no.	Hypothesis (direction)	Path coefficient	*T*-value	Significance (one-tailed)	Supported?
H1A	PC → INT (−)	−0.065	1.085	n.s.	No
H1B	PS → INT (−)	−0.176	2.511	$p < 0.01$	Yes
H2A	P → PC (+)	−0.128	1.646	$p < 0.05$	No
H2B	P → PS (+)	0.244	2.887	$p < 0.01$	Yes
H3A	SETA → PC (+)	0.267	3.463	$p < 0.01$	Yes
H3B	SETA → PS (+)	0.158	1.931	$p < 0.05$	Yes
H4A	M → PC (+)	0.494	7.989	$p < 0.001$	Yes
H4B	M → PS (+)	0.170	2.646	$p < 0.01$	Yes
Control variables	Org. → INT	−0.193	3.693	$p < 0.01$	—
	MC → INT	−0.373	5.609	$p < 0.001$	—
	Age → INT	−0.071	1.367	n.s.	—
	Gender → INT	−0.084	1.581	n.s.	—

Notes. PC = Perceived certainty; PS = Perceived severity; INT = IS misuse intention; P = Security policies; SETA = SETA program; M = Computer monitoring; Org. = Organization; MC = Moral commitment.

combination of PC, PS, and the control variables explain 30% of the variance in IS misuse intention. PC and PS alone explain 11% of intention variance, while MC contributes an additional 14%.

Consistent with H1B, PS has a significant negative effect on INT ($\beta = -0.176$, $p < 0.01$). The relationship between PC and INT is directionally consistent with H1A, but not significant ($\beta = -0.065$, $p > 0.10$).[11] Consistent with Hypotheses H3A and H4A, both user awareness of SETA program ($\beta = 0.267$, $p < 0.01$) and computer monitoring ($\beta = 0.494$, $p < 0.001$) have significant direct effects on PC. User awareness of security policies is significantly associated with PC, but the direction of this path is opposite to expectations. Hence, H2A is not supported. Consistent with Hypotheses H2B, H3B, and H4B, user awareness of security policies ($\beta = 0.244$, $p < 0.01$), SETA program ($\beta = 0.158$, $p < 0.05$), and monitoring practices ($\beta = 0.170$, $p < 0.01$) each has a significant direct effect on PS.

As an additional step, we ran a PLS model with PC and PS removed to determine if the data supported the posited full mediation of the effects of the security countermeasures on IS misuse intention by PC and PS. Of the three security countermeasures, only security policies had a significant direct path to INT ($p < 0.05$). These results point to the relevance of PC and PS as mediators of the effects of SETA program and computer monitoring on IS misuse intention.

Post Hoc Analysis

The nonsignificant relationship between PC and INT is contrary to the predictions of GDT. Therefore, we revisited the deterrence literature in search of a potential explanation for this unexpected result. Several deterrence theorists (e.g., Bachman et al. 1992, MacCoun 1993, Silberman 1976) have argued that the deterrent effects of PC and PS depend on moral considerations. The rationale is that those individuals with strong moral inhibitions are already effectively restrained from deviant behavior and therefore the threat of punishment is irrelevant, or at least much weaker. Other, less morally-inhibited individuals, however, are more influenced by the threat of punishment. There is some empirical evidence supporting the notion that "morality" (measured as either perceived morality of an act or general level of morality of the individual) moderates the impact of punishment threats (Bachman et al. 1992, Strelan and Boeckmann 2007, Workman and Gathegi 2006). However, it should also be noted that at least a few studies have found no evidence of this moderating effect (Grasmick and Green 1981, Klepper and Nagin 1989, Paternoster 1989).

For this study, we tested whether moral commitment (MC) moderates the influence of PC and PS on INT by adding two latent interaction variables ($PC * MC$ and $PS * MC$) to the main effects variables in Figure 2. These two variables were created by multiplying the indicators for PC and PS, respectively, by the MC indicator (as per Chin et al. 2003). The results indicate that both $PC * MC$ ($\beta = 0.123$, $p < 0.10$) and

[11] As shown in Appendices C and D, the distribution of the INT variable was skewed (mean = 7.87; standard deviation = 3.62), with a large proportion of respondents in the lower end (low IS misuse intention). A skewed distribution of the dependent variable is common in unethical/deviant behavior studies (e.g., Bachman et al. 1992, Hollinger and Clark 1983). To address this issue, and further test H1 and H2, we dichotomized the INT variables (with two different cutoff points) and redid the analyses. For the first dichotomization, we coded the INT variables as 0 for scores of 4 (the lowest value on the scale of 4–28; it represents those with little or no probability of engaging in the scenario behaviors) and 1 for all other scores. For the second dichotomization, we coded the INT variables as 0 for scores below the median (median = 7.0 for both INT1 and INT2) and 1 for scores above the median. The direction and significance of the path coefficients remained unchanged from those in Figure 2 in both analyses and therefore we left INT as a continuous variable.

Table 6 **Results for High and Low Moral Commitment Subgroups**

	Path coefficients	
Paths	High moral commitment	Low moral commitment
PC → INT	−0.233*	0.043
PS → INT	0.103	−0.379**
R^2 of INT	0.27	0.18

*$p < 0.05$, **$p < 0.01$.

PS ∗ MC ($\beta = -0.201$, $p < 0.01$) were associated with INT, suggesting that MC moderates the impact of both PC and PS on INT. To further explore this effect, we split the sample into two groups based on the median of MC: higher moral commitment (i.e., viewed the scenario behaviors as "less" morally acceptable) and lower moral commitment (i.e., viewed the scenario behaviors as "more" morally acceptable).[12] Separate PLS models were run for each subgroup.

The results shown in Table 6 indicate that for the higher MC group, PC has a significant effect on INT ($\beta = -0.233$, $p < 0.05$) but not for the lower MC group. Conversely, for the lower MC group, PS has a significant effect on INT ($\beta = -0.379$, $p < 0.01$) but not for the higher MC group. Statistical tests using the approach suggested by Keil et al. (2000) showed that the differences in the PC to INT and PS to INT path coefficients from the two groups were significant at the 0.05 level. Thus, in the context of IS misuse, perceptions of being caught seem to be more of a deterrent for individuals with stronger moral inhibitions, whereas perceptions of punishment severity are a greater deterrent for less morally-inhibited people. These results are discussed further in the next section.

Discussion

The overall results indicate that controlling for age, gender, moral commitment, and organization, perceived severity of sanctions has a direct, negative effect on IS misuse intention but perceived certainty of sanctions does not. The results suggest a modification to GDT in the context of IS security. From a substantive perspective, IS misuse appears to be much more strongly influenced by PS than PC. This finding contradicts a large number of prior deterrence studies in the fields of sociology and criminology, which reported that the impact of PC was much greater than that of PS (Paternoster 1987, von Hirsch et al. 1999). It is, however, consistent with Skinner and Fream's (1997) deterrence-based study within the IS domain.

A post hoc analysis showed that moral commitment has interesting, previously unseen interaction effects for both PC and PS. The results suggest that PC has a greater influence than PS on IS misuse intention for respondents who exhibit high levels of moral commitment, while PS has more influence than PC on IS misuse intention for those with low levels of moral commitment. Although the former is consistent with several studies (Bachman et al. 1992, Strelan and Boeckmann 2006, Workman and Gathegi 2007), to our knowledge the latter has not been reported in previous work.

These findings have interesting potential explanations. We speculate that IS misuse is considered to be less serious than other types of infractions, given that the most visible "victim" is a computer system, with only indirect effects on people. Evidence of this assertion can be found by examining the relatively light sentences demanded by courts in cases of computer crime (e.g., Harrington 1996, Workman and Gathegi 2007). People of high moral commitment might be very sensitive to certainty of sanctions because, no matter what the penalty, they would find it unpleasant even to be accused of a socially undesirable act. On the other hand, people of low moral commitment would be more concerned about the penalty that would be assessed due to their behavior.

Analysis of the research model indicates that PC and PS are key intervening variables linking security countermeasures to IS misuse intention. Thus, with the exception of the direct effect of security policies, the effects of the security countermeasures on IS

[12] The median for MC was 7.0. Considering that the possible range for this variable is between 4 and 28, the two subgroups can essentially be thought of as (1) those that are extremely morally opposed to the scenario behaviors, and (2) those that are less strong in their moral convictions about the behaviors. We also checked the distribution of the INT variable within the subgroups. The distribution of INT within the high morality subgroup was positively skewed. However, over 60% of INT scores were within the 5 to 20 range (i.e., above the minimum score of 4). Hence, there was sufficient variance to make the analysis meaningful. The INT scores within the low morality subgroup were normally distributed. Finally, we ran PLS models for each subgroup with INT dichotomized based on its median. The direction and significance of the path coefficients did not change from those in Table 6.

misuse, as discussed below, are indirect through perceived certainty and severity of sanctions.

Security Policy

The significant direct and indirect effects of security policies on IS misuse intention suggest that when users are aware that security policies exist, they are less likely to engage in IS misuse. The effectiveness of policy awareness on perceptions of punishment severity is important because our results suggest that perceived punishment severity is a strong deterrent to IS misuse.

The unexpected negative relationship between security policies and perceived certainty of sanctions deserves some attention because it suggests that awareness of security policies does not increase users' perceptions of the likelihood of getting caught for IS misuse. A possible explanation is that as users become more aware of security policy, they might also become more educated about information technology in general and realize the difficulties in detecting misuse incidents. It is known that a small percentage of computer security incidents are actually discovered (Whitman 2004). It may also be that many IS security policies focus on defining appropriate computing behaviors with little emphasis on organizational methods for detecting security incidents. Further, users may view deployment of security policies as a minimalist approach to security in general because such policies often consist of a simple form or procedure that is rarely looked at or updated (Forrester Research 2007, Lee and Lee 2002). Security policies do, however, provide a basis for punishment and therefore still increase users' perceived severity of sanctions.

From a methodological perspective, the testing method (i.e., use of scenarios) and the language of the particular scenarios used in this study may have contributed to the unexpected result. We considered using a formal manipulation check but determined that such a check could have sensitized participants, leading to overstated results. Although we conducted careful content reviews with an independent audience in place of such a check, it is difficult to determine precisely the extent to which respondents were able to engage the scenarios and thus relate the scenario behaviors to their own organizations' security policies. On the other hand, the significant relationship between security policies and perceived severity of sanctions suggests that this was not an issue. It is also possible that the distribution of the security policy variable (see Appendix C), which revealed that most respondents were aware of security policies in their organizations, might have affected our results. In retrospect, this distribution is not surprising considering that most organizations have some type of security policy in place (Lee and Lee 2002) and many organizations make employees aware of that policy at least to minimize legal exposure. Although the current study focused on existence of security policies, measuring security policies in terms of their salient characteristics (e.g., specific content, level of enforcement, frequency of updates) may provide greater variability in the response distribution and thus enable a better assessment of the relationship between security policies and perceived certainty of sanctions.

Security Education, Training, and Awareness (SETA) Programs

The results on the impact of SETA programs are particularly noteworthy. Security researchers and best-practice advocates have long proclaimed the benefits of security education and training initiatives, but little empirical evidence supported these claims. This study provides evidence that user awareness of SETA programs can help reduce IS misuse due to their ability to increase perceptions of the certainty and severity of punishment for such behavior. The results empirically support the notion that SETA programs have a deterrent effect by reminding users that they are likely to be caught, and if they are caught they will be punished accordingly.

Computer Monitoring

Users' awareness of computer monitoring was shown to have a significant effect on users' perceived certainty and severity of sanctions, providing empirical support for the assertion that "policing" activities, such as efforts from security administrators to monitor computing activities and audit the use of IS assets can help deter IS misuse. The influence of monitoring practices on perceived certainty of sanctions was stronger than any of the other security countermeasures, suggesting that computer monitoring is a useful mechanism for convincing users that misuse activities will be detected. In addition, the significant effect of monitoring on perceived severity of sanctions indicates that monitoring is an effective countermeasure for reducing misuse intentions.

Organization

The control variable organization was examined further by testing the effect of organization (coded as a dummy variable) on PC and PS along with the three countermeasure variables. Organization did not have a significant effect on either PC or PS, suggesting that the influence of users' awareness of the security countermeasures on sanction perceptions is consistent across the eight organizations in our sample. However, organization was significant as a control variable on the relationships between PC and PS and IS misuse intention. Consistent with prior research (e.g., Banerjee et al. 1998), this suggests that IS misuse intention might vary based on organizational characteristics. Examples might include security culture, ethical climate, punishment history, and top management commitment to security. Future research should examine the influences of various organizational characteristics on both IS misuse intention and the effectiveness of security countermeasures.

Contributions

This study contributes to both research and practice in IS security. First, by examining the underlying process by which security countermeasures impact IS misuse, this research emphasizes the importance of perceived severity of sanctions on IS misuse intention. As expected, we found that users' awareness of security policies, SETA programs, and computer monitoring are each effective (to varying degrees) in increasing perceptions of sanctions associated with IS misuse. However, contrary to a number of deterrence studies in the criminological literature, our results suggest that perceived severity of sanctions has a significant direct effect on IS misuse intention, while perceived certainty of sanctions has an indirect effect through moral commitment. Thus, it appears that GDT in the context of IS misuse differs from prior interpretations of the theory.

Although the overall model seems to indicate that perceived severity of sanctions has the only desired direct effect on IS misuse intention, the post hoc analysis provides another contribution of this study. Taking moral commitment (MC) into consideration will be likely to provide more precise explanatory power to GDT models in a computer crime context, given that high MC individuals seem to be more sensitive to PC and low MC individuals seem to be more sensitive to PS.

It also seems that while GDT has some predictive power, the theory by itself does not provide a complete understanding of IS misuse. Corroborating our results with prior studies that found that informal sanctions (e.g., guilt, social stigma, peer involvement) have a strong effect on deviant behaviors, as well as research by Peace et al. (2003) that found that attitudinal variables help predict software piracy, additional factors beyond deterrence constructs are likely to provide insight into the antecedents of IS misuse.

Implications for Practice

The results of this study provide evidence that awareness of security policies, SETA programs, and computer monitoring each have some effect in deterring IS misuse—for security policies deterrence is achieved by increasing perceived severity of punishment, whereas for SETA programs and computer monitoring deterrence is achieved by increasing both perceived certainty and severity of punishment. Security policies, SETA programs, and computer monitoring are mechanisms over which the organization has direct control. Unfortunately, various other factors that have been shown to predict IS misuse are often more difficult for managers to control. For example, in the current study the control variable moral commitment was found to have a highly significant relationship with IS misuse intention. While theoretically interesting, this finding may have lesser practical value; each individual has a unique set of moral values (Kohlberg 1976), making it difficult for an organization to shape the morality levels of its user population. Thus, the deterrent effects of security policies, SETA programs, and computer monitoring are encouraging for practitioners.

Our findings are also significant in light of prior research that suggests that managers were not convinced that security efforts could deter IS misuse (Hoffer and Straub 1989, Straub and Welke 1998).

Instead, they considered IS security a preventive function—designed to restrict abusive activities. This study's results provide empirical evidence of the deterrent value of security countermeasures, which can help further substantiate organizational investments in these controls.

The post hoc analysis provides practitioners with a richer call to action. Because PC appears more important than PS for persons of high moral commitment, and that PS is more important than PC for persons of low moral commitment, organizations should focus on both the certainty and severity of punishment when designing SETA programs.

The observed effects of a SETA program on perceived certainty and severity of punishment and indirectly on IS misuse intention also have implications for the allocation of security budgets. In an industry survey, over 70% of organizations indicated that they use technologies such as virus detection software and firewalls to protect information systems, while only 28% reported that they have ongoing SETA programs in place (InformationWeek 2005). Our results suggest that organizations should consider allocating a greater portion of their budgets to security awareness education and training efforts. Moreover, our findings empirically confirm the prescriptive recommendations of security practitioners (e.g., Hansche 2001, Parker 1998) about the benefits of SETA programs.

Limitations and Future Research

Like most empirical research, this study has limitations that should be taken into account. The first limitation is the single source for both dependent and independent variables, which could introduce common method bias. Although formal tests revealed no evidence of substantial common method variance in this study, the research would be strengthened by a longitudinal design with a lag between collection of the dependent and independent variables, or by experimental studies that manipulate deterrent mechanisms and measure actual user behavior.

A second limitation is the use of IS misuse intention instead of actual behaviors. Despite the support in the literature for using intention as a predictor of actual behavior, there is no guarantee that individuals would behave as they have indicated. Future research should reexamine the model in a context where actual IS misuse can be measured to add additional credibility to the model.

Third, the measurement of IS misuse in this study is limited to the specific hypothetical scenarios chosen. Although the scenarios cover a wide range of security issues, they do not include every type of IS misuse. Future research should test the explanatory power of our model on a larger number of IS misuse behaviors. Additional analysis by scenario (e.g., Leonard and Cronan 2001, Leonard et al. 2004) could also test for differences in the impact of the security countermeasures on individual IS misuse behaviors. Experiments could also be conducted that use manipulation checks to ensure that respondents have adopted the scenarios to the context of their own workplace.

Finally, all eight organizations that participated in the study are based in the United States. Given international cultural and legal differences, it is possible that users in other countries might have different reactions to security countermeasures within their organizations and to IS misuse in general. Future research should validate the model in distinctly different national cultures outside of the United States.

Conclusion

This study makes significant progress toward explaining the relationships between security countermeasures, sanction perceptions, and IS misuse. The results suggest that user awareness of security policies, SETA programs, and computer monitoring each have some deterrent effect on IS misuse intention, and this effect is achieved indirectly through perceived certainty and/or severity of sanctions. There is also evidence that the influences of sanction perceptions vary based on one's level of morality. From a theoretical perspective, the research introduces an extended version of GDT and confirms its applicability to the IS security domain. This study also adds to previous deterrence-based assessments of security countermeasures by measuring GDT's two main constructs (perceived certainty and severity of sanctions) directly. Several avenues for future research remain and it is hoped that this study will stimulate others to extend this line of research.

Acknowledgments

This work was supported in part by a research grant from the State Farm Companies Foundation. The authors thank the senior editor, the associate editor, and three anonymous reviewers for constructive feedback and general guidance throughout the review process and the Temple University Institute for Business and Information Technology for facilitating data collection for this project. Special thanks to Hang Li at the University of Notre Dame for his valuable assistance with the LISREL analysis.

Appendix A. IS Misuse Scenarios and PC, PS, MC, and INT Items

Scenario 1: Taylor received an e-mail from a friend that contained a series of jokes. Many of the jokes poked fun at the stereotypes that people often associate with different ethnic groups. Taylor found the jokes very funny and decided to send the e-mail to several co-workers.

Scenario 2: By chance, Alex found the password that allowed him to access the restricted computer system that contained the salary information of all employees within his company. Around the same time, Alex was preparing to ask for a raise. Before meeting with his boss, Alex accessed the computer system and viewed the salaries of others in similar jobs. Alex used this information to determine how much of a salary increase to ask for.

Scenario 3: Jordan is given a personal computer (PC) at work. However, the new PC is missing a piece of software that Jordan believes would make her more effective on the job. Jordan requests that the company purchase the software but her request is denied. To solve the problem, Jordan obtains an unlicensed copy of the software from a friend outside of the company and installs the software on her PC at work.

Scenario 4: Chris prepares payroll records for his company's employees and therefore has access to the computer timekeeping and payroll systems. Periodically, Chris would increase the hours-worked records of certain employees with whom he was friends by "rounding up" their total hours for the week (forexample, Chris would change 39.5 hours worked to 40 hours worked).

Following each scenario, respondents were presented with the following questions. The item wordings were slightly modified to fit each scenario and all items were measured on seven-point scales using the endpoints shown below.

INT1 If you were Taylor, what is the likelihood that you would have sent the e-mail? (very unlikely .... very likely)

INT2 I could see myself sending the e-mail if I were in Taylor's situation: (strongly disagree .... strongly agree)

MC It was morally acceptable for Taylor to send the e-mail: (strongly disagree .... strongly agree)

For the next four questions, imagine that the preceding scenario took place in *your* place of work:

PS1 If caught sending the e-mail, Taylor would be severely reprimanded: (strongly disagree .... strongly agree)

PC1 Taylor would probably be caught, eventually, after sending the e-mail: (strongly disagree .... strongly agree)

PS2 If caught sending the e-mail, Taylor's punishment would be: (not severe at all .... very severe)

Appendix A. Continued

PC2 The likelihood the organization would discover that Taylor sent the e-mail is: (very low .... very high)

Notes. Individual items were summed across the four scenarios to create composite scores. For example,

$$\begin{aligned} \text{INT1} &= \text{INT1(scenario 1)} + \text{INT1(scenario 2)} \\ &\quad + \text{INT1(scenario 3)} + \text{INT1(scenario 4)}, \\ \text{INT2} &= \text{INT2(scenario 1)} + \text{INT2(scenario 2)} \\ &\quad + \text{INT2(scenario 3)} + \text{INT2(scenario 4)}. \end{aligned}$$

The composite values for INT1 and INT2 were then used in the PLS analysis. The same procedure was followed for the PC, PS, and MC constructs.

Appendix B. Security Countermeasure Items

Item	Weight
P1: My organization has specific guidelines that describe acceptable use of e-mail.	0.23†
P2: My organization has established rules of behavior for use of computer resources.	0.29*
P3: My organization has a formal policy that forbids employees from accessing computer systems that they are not authorized to use.	0.27*
P4: My organization has specific guidelines that describe acceptable use of computer passwords.	0.26*
P5: My organization has specific guidelines that govern what employees are allowed to do with their computers.	0.17
SETA1: My organization provides training to help employees improve their awareness of computer and information security issues.	0.27*
SETA2: My organization provides employees with education on computer software copyright laws.	0.09
SETA3: In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way.	0.16†
SETA4: My organization educates employees on their computer security responsibilities.	0.56*
SETA5: In my organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use.	0.29*
M1: I believe that my organization monitors any modification or altering of computerized data by employees.	0.55*
M2: I believe that employee computing activities are monitored by my organization.	0.12
M3: I believe that my organization monitors computing activities to ensure that employees are performing only explicitly authorized tasks.	0.21*
M4: I believe that my organization reviews logs of employees' computing activities on a regular basis.	0.23*
M5: I believe that my organization conducts periodic audits to detect the use of unauthorized software on its computers.	0.27*
M6: I believe that my organization actively monitors the content of employees' e-mail messages.	0.31*

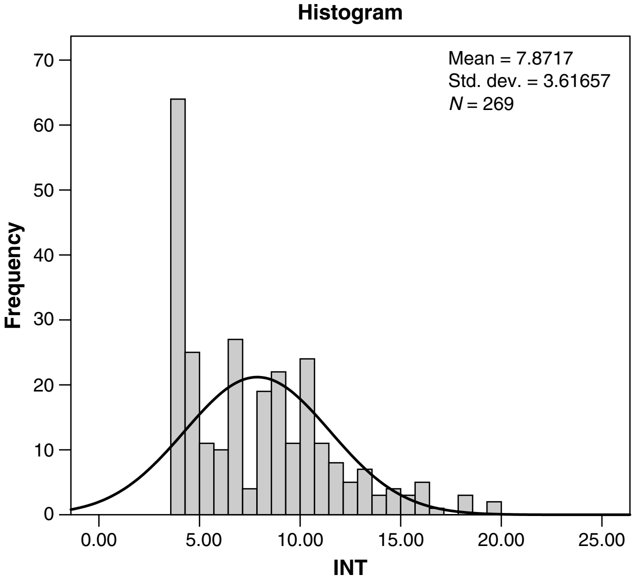
Notes. All items were measured using seven-point response scales ("strongly disagree" to "strongly agree").
$^\dagger p < 0.10$; $^* p < 0.05$.

Appendix C. Construct Descriptive Statistics and Tests for Normality

					Skewness		Kurtosis	
Construct	Min.	Max.	Mean	Std. dev.	Statistic	*Z*-score	Statistic	*Z*-score
INT	4.00	20.00	7.87	3.62	0.90	**6.01**	0.39	1.32
PC	5.00	28.00	17.71	4.80	0.09	0.59	−0.26	−0.89
PS	8.00	28.00	19.95	4.18	−0.34	**−2.30**	−0.18	−0.63
P	1.00	7.00	5.58	1.29	−1.28	**−8.61**	1.68	**5.66**
SETA	1.00	7.00	4.33	1.52	−0.12	−0.83	−0.81	**−2.73**
M	1.33	7.00	4.59	1.28	−0.33	**−2.18**	−0.34	−1.14

Note. Bold *z*-scores indicate a significant ($p < 0.025$) departure from normality for skewness or kurtosis.

Appendix D. Histogram for IS Misuse Intention Variable (Scale Mean)



References

Ajzen, I. 1988. *Attitudes, Personality, and Behavior*. Dorsey Press, Chicago.

Alder, G. S., T. W. Noel, M. L. Ambrose. 2006. Clarifying the effects of Internet monitoring on job attitudes: The mediating role of employee trust. *Inform. Management* **43**(7) 894–903.

Alm, J., M. McKee. 2006. Audit certainty, audit productivity, and taxpayer compliance. *National Tax J.* **59**(4) 801–816.

AMA. 2005. 2005 Electronic monitoring and surveillance survey. American Management Association, New York.

Anderson, J. C., D. W. Gerbing. 1988. Structural equation modeling in practice: A review and recommended two-step approach. *Psych. Bull.* **103**(3) 411–423.

Armstrong, J. S., T. S. Overton. 1977. Estimating nonresponse bias in mail surveys. *J. Marketing Res.* (14) 396–402.

Bachman, R., R. Paternoster, S. Ward. 1992. The rationality of sexual offending: Testing a deterrence/rational choice conception of sexual assault. *Law Soc. Rev.* **26**(2) 343–372.

Banerjee, D., T. P. Cronan, T. W. Jones. 1998. Modeling IT ethics: A study in situational ethics. *MIS Quart.* **22**(1) 31–60.

Baskerville, R., M. Siponen. 2002. An information security meta-policy for emergent organizations. *Logist. Inform. Management* **15**(5/6) 337–346.

Berinato, S. 2005. The global state of information security 2005. *CIO Magazine* **15**(September) 60–72.

BSA. 2005. Second annual BSA and IDC global software piracy study. Business Software Alliance, Washington, D.C.

Carnes, G. A., T. D. Englebrecht. 1995. An investigation of the effect of detection risk perceptions, penalty sanctions, and income visibility on tax compliance. *J. Amer. Taxation Assoc.* **17**(1) 26–41.

Chin, W. 1998. The partial least squares approach to structural equation modeling. G. A. Marcoulides, ed. *Modern Methods For Business Research*. Lawrence Erlbaum Associates, Mahwah, NJ, 295–336.

Chin, W., B. L. Marcolin, P. R. Newsted. 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. *Inform. Systems Res.* **14**(2) 189–217.

Christensen, A., M. M. Eining. 1994. Instructional case: Software piracy—Who does it impact? *Issues Accounting Ed.* **9**(1) 151–159.

Cole, C. A. 1989. Deterrence and consumer fraud. *J. Retailing* **65**(1) 107–120.

Compeau, D. R., C. A. Higgins. 1995. Computer self-efficacy: Development of a measure and initial test. *MIS Quart.* **19**(2) 189–211.

Deloitte. 2005. *Global Security Survey*. New York.

Dhillon, G. 1999. Managing and controlling computer misuse. *Inform. Management Comput. Security* **7**(4) 171–175.

Diamantopoulos, A., H. M. Winklhofer. 2001. Index construction with formative indicators: An alternative to scale development. *J. Marketing Res.* (38) 269–277.

Dubin, J. A., M. J. Graetz, L. L. Wilde. 1990. The effect of audit rates on the federal individual income tax, 1977–1986. *National Tax J.* **43**(4) 395–409.

Ernst and Young. 2003. *Global Information Security Survey*. New York.

Falk, R. F., N. B. Miller. 1992. *A Primer for Soft Modeling*. University of Akron Press, Akron, OH.

Ferguson, M., M. Sheehan, J. Davey, B. Watson. 1999. *Drink Driving Rehabilitation: The Present Context—A Road Safety Research Report*. Centre for Accident Research and Road Safety, Brisbane, Australia. Available online at: http://www.atsb.gov.au/publications/1999/pdf/Alc_Rehab_2.pdf.

Finch, J. 1987. The vignette technique in survey research. *Sociology* **21**(1) 105–114.

Finch, J. H., S. M. Furnell, P. S. Dowland. 2003. Assessing IT security culture: System administrator and end-user. *Proc. ISOneWorld Conf.*, Las Vegas, NV, 16–20.

Foltz, C. B. 2000. The impact of deterrent countermeasures upon individual intent to commit misuse: A behavioral approach. Unpublished doctoral dissertation, University of Arkansas, Fayetteville.

Forcht, K. A. 1994. *Computer Security Management*. Boyd & Fraser, Danvers, MA.

Fornell, C., D. F. Larcker. 1981. Evaluating structural equation models with unobservable variables and measurement error. *J. Marketing Res.* **18**(1) 39–50.

Forrester Research. 2007. *The State of Data Security in North America*. Cambridge, MA.

Fotiva, Inc. 2005. Risky business: New survey shows almost 70 percent of e-mail-using employees have sent or received e-mail that may pose a threat to businesses. Available online at: http://www.harrisinteractive.com/news/newsletters/clientnews/Fortiva2005.pdf.

Freeman, J., B. Watson. 2006. An application of Stafford and Warr's reconceptualisation of deterrence to a group of recidivist drink drivers. *Accident Anal. Prevention* (38) 462–471.

Furnell, S. M., M. Gennatou, P. S. Dowland. 2002. A prototype tool for information security awareness and training. *Logist. Inform. Management* **15**(5/6) 352–357.

Furnell, S. M., P. S. Dowland, H. M. Illingworth, P. L. Reynolds. 2000. Authentication and supervision: A survey of user attitudes. *Comput. Security* **19**(6) 529–539.

Gaston, S. J. 1996. *Information Security: Strategies for Successful Management*. CICA Publishing, Toronto.

Gattiker, U. E., H. Kelley. 1999. Morality and computers: Attitudes and differences in moral judgments. *Inform. Systems Res.* **10**(3) 233–254.

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

George, J. F. 1996. Computer-based monitoring: Common perceptions and empirical results. *MIS Quart.* **20**(4) 459–480.

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

Glenn, D., G. J. Browne, J. C. Wetherbe. 2006. Why do Internet users stick with a specific web site? A relationship perspective. *Internat. J. Electronic Commerce* **10**(4) 105–141.

Gopal, R. D., G. L. Sanders. 1997. Preventative and deterrent controls for software piracy. *J. Management Inform. Systems* **13**(4) 29–47.

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

Grasmick, H. G., D. E. Green. 1981. Deterrence and the morally committed. *Sociol. Quart.* (22) 1–14.

Hair, J. F., R. E. Anderson, R. L. Tatham, W. C. Black. 1998. *Multivariate Data Analysis*. Prentice Hall, Englewood Cliffs, NJ.

Hansche, S. 2001. Designing a security awareness program: Part 1. *Inform. Systems Security* **9**(6) 14–22.

Harrington, S. J. 1996. The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quart.* **20**(3) 257–278.

Hoffer, J. A., D. W. Straub. 1989. The 9 to 5 underground: Are you policing computer crimes? *Sloan Management Rev.* **30**(4) 35–43.

Hollinger, R. C., J. P. Clark. 1983. Deterrence in the workplace: Perceived certainty, perceived severity, and employee theft. *Soc. Forces* **62**(2) 398–418.

InformationWeek. 2005. U.S. Information Security Research Report 2005. United Business Media, London.

Jarvis, C. B., P. M. Mackenzie, P. M. Podsakoff. 2003. A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *J. Consumer Res.* **30**(2) 199–218.

Kankanhalli, A., H.-H. Teo, B. C. Y. Tan, K.-K. Wei. 2003. An integrative study of information systems security effectiveness. *Internat. J. Inform. Management* **23**(2) 139–154.

Keil, M., B. Tan, K. K. Wei, V. Saarinen, V. Tuunainen, A. Wassenaar. 2000. A cross-cultural study of escalation of commitment in software projects. *MIS Quart.* **24**(2) 299–325.

Kerlinger, F. N. 1986. *Foundations of Behavioral Research*, 3rd ed. Holt, Rinehart & Winston, New York.

Kinsey, K. A. 1992. Deterrence and alienation effects of IRS enforcement: An analysis of survey data. J. Slemrod, ed. *Why People Pay Taxes*. University of Michigan Press, Ann Arbor, 259–285.

Klepper, S., D. Nagin. 1989. The deterrent effect of perceived certainty and severity of punishment revisited. *Criminology* **27**(4) 721–746.

Kohlberg, L. 1976. Moral stages and moralization: The cognitive-developmental approach. T. Lickona, ed. *Moral Development and Behavior*. Holt, Rinehart, and Winston, New York, 31–53.

Lee, J., Y. Lee. 2002. A holistic model of computer abuse within organizations. *Inform. Management Comput. Security* **10**(2) 57–63.

Lee, S. M., S.-G. Lee, S. Yoo. 2004. An integrative model of computer abuse based on social control and general deterrence theories. *Inform. Management* **41**(6) 707–718.

Leonard, L. N. K., T. P. Cronan. 2001. Illegal, inappropriate, and unethical behavior in an information technology context: A study to explain influences. *J. Assoc. Inform. Systems* **1**(12) 1–31.

Leonard, L. N. K., T. P. Cronan, J. Kreie. 2004. What influences IT ethical behavior intentions—Planned behavior, reasoned action, perceived importance, individual characteristics? *Inform. Management* **42**(1) 143–158.

Lin, T.-C., M.-H. Hsu, F.-Y. Kuo, P.-C. Sun. 1999. An intention model-based study of software piracy. *Proc. 32nd Hawaii Internat. Conf. System Sci.*, IEEE Computer Society, Maui, HI.

Lindell, M. K., D. J. Whitney. 2001. Accounting for common method variance in cross-sectional research designs. *J. Appl. Psych.* **86**(1) 114–121.

Loch, K. D., D. Straub, S. Kamel. 2003. Diffusing the Internet in the Arab world: The role of social norms and techological culturation. *IEEE Trans. Engrg. Management* **50**(1) 45–63.

MacCoun, R. J. 1993. Drugs and the law: A psychological analysis of drug prohibition. *Psych. Bull.* **113**(3) 497–512.

MacMath, B., S. Prentice-Dunn. 2005. Protection motivation theory and skin cancer risk: The role of individual differences in response to persuasive appeals. *J. Appl. Soc. Psych.* **35**(3) 621–643.

Magklaras, G. B., S. M. Furnell. 2002. Insider threat prediction tool: Evaluating the probability of IT misuse. *Comput. Security* **21**(1) 62–73.

Malhotra, N. K., S. S. Kim, A. Patil. 2006. Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research. *Management Sci.* **52**(12) 1865–1883.

Mason, R. 1986. Four ethical issues of the information age. *MIS Quart.* **10**(1) 4–12.

McNees, M. P., D. S. Egli, R. S. Marshall, J. F. Schnelle, T. R. Risley. 1976. Shoplifting prevention: Providing information through signs. *J. Appl. Behav. Anal.* **9**(4) 399–405.

Nagin, D. S., G. Pogarsky. 2001. Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence and evidence. *Criminology* **39**(4) 865–891.

Nienstedt, B. C. 1985. Testing deterrence: The effects of a DWI law and publicity campaigns. Unpublished doctoral dissertation, Arizona State University, Tempe.

Panko, R. R., H. G. Beh. 2002. Monitoring for pornography and sexual harassment. *Comm. ACM* **45**(1) 84–87.

Paradice, D. B. 1990. Ethical attitudes of entry-level MIS personnel. *Inform. Management* **18**(3) 143–151.

Parker, D. B. 1998. *Fighting Computer Crime*. John Wiley & Sons, New York.

Paternoster, R. 1987. The deterrent effect of the perceived certainty and severity of punishment: A review of the evidence and issues. *Justice Quart.* **4**(2) 173–217.

Paternoster, R. 1989. Decision to participate in and desist from four types of common delinquency: Deterrence and the rational choice perspective. *Law Soc. Rev.* **23**(1) 7–40.

Patnayakuni, R., A. Rai, N. Seth. 2006. Relational antecedents of information flow integration for supply chain coordination. *J. Management Inform. Systems* **23**(1) 13–49.

Peace, A. G., D. F. Galletta, J. Y. L. Thong. 2003. Software piracy in the workplace: A model and empirical test. *J. Management Inform. Systems* **20**(1) 153–177.

Pechmann, C., G. Zhao, M. Goldberg, E. Reibling. 2003. What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes. *J. Marketing* **67**(2) 1–18.

Peltier, T. R. 2005. Implementing an information security awareness program. *Inform. Systems Security* **14**(2) 37–49.

Pierce, M. A., J. W. Henry. 2000. Judgments about computer ethics: Do individual, co-worker, and company judgments differ? *J. Bus. Ethics* **28**(4) 307–322.

Podsakoff, P. M., S. B. Mackenzie, J. Y. Lee, N. P. Podsakoff. 2003. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *J. Appl. Psych.* **88**(5) 879–903.

Quazi, M. M. 1993. Effective drug-free workplace plan uses worker testing as a deterrent. *Occupational Health Safety* **62**(6) 26–31.

Richardson, R. 2007. *CSI/FBI Computer Crime and Security Survey*. Computer Security Institute, San Francisco.

Rogers, R. 1983. Cognitive and physiological processes in fear-based attitude change: A revised theory of protection motivation. J. Cacioppo, R. Petty, eds. *Social Psychophysiology: A Sourcebook*. Guilford, New York, 153–176.

Sacco, V. F. 1985. Shoplifting prevention: The role of communication-based intervention strategies. *Canadian J. Criminology* **27**(1) 15–29.

Silberman, M. 1976. Toward a theory of criminal deterrence. *Amer. Sociol. Rev.* **41**(3) 442–461.

Skinner, W. F., A. M. Fream. 1997. A social learning theory analysis of computer crime among college students. *J. Res. Crime Delinquency* **34**(4) 495–518.

Spitzmuller, C., J. M. Stanton. 2006. Examining employee compliance with organizational surveillance and monitoring. *J. Occupational Organ. Psych.* (79) 245–272.

Standage, T. 2002. The weakest link. *Economist* **365**(8296) 11–16.

Stanton, J. M., E. M. Weiss. 2000. Electronic monitoring in their own words: An exploratory study of employees' experiences with new types of surveillance. *Comput. Human Behav.* **16**(4) 423–440.

Stanton, J. M., K. R. Stam, P. R. Mastrangelo, J. Jolton. 2005. An analysis of end user security behaviors. *Comput. Security* **24**(2) 124–133.

Straub, D. W. 1990. Effective IS security: An empirical study. *Inform. Systems Res.* **1**(3) 255–276.

Straub, D. W., W. D. Nance. 1990. Discovering and disciplining computer abuse in organizations: A field study. *MIS Quart.* **14**(1) 45–60.

Straub, D. W., R. J. Welke. 1998. Coping with systems risk: Security planning models for management decision making. *MIS Quart.* **22**(4) 441–469.

Strelan, P., R. J. Boeckmann. 2006. Why drug testing in elite sport does not work: Perceptual deterrence theory and the role of personal moral beliefs. *J. Appl. Soc. Psych.* **36**(12) 2909–2934.

Theoharidou, M., S. Kokolakis, M. Karyda, E. Kiountouzis. 2005. The insider threat to information systems and the effectiveness of ISO17799. *Comput. Security* **24**(6) 472–484.

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

United Nations. 2005. Conference on Trade and Development, Information Economy Report. Geneva, Switzerland. http://www.unctad.org/en/docs/sdteecb20051overview_en.pdf.

Urbaczewski, A., L. M. Jessup. 2002. Does electronic monitoring of employee Internet usage work? *Comm. ACM* **45**(1) 80–83.

Verespej, M. A. 2000. Inappropriate Internet surfing. *Indust. Week* **29**(3) 59–64.

von Hirsch, A., A. E. Bottoms, E. Burney, P. O. Wikstrom. 1999. *Criminal Deterrence and Sentence Severity: An Analysis of Recent Research*, Oxford Publishing, Oxford, UK.

von Solms, R., B. von Solms. 2004. From policies to culture. *Comput. Security* **23**(4) 275–279.

Wentzel, M. 2004. The social side of sanctions: Personal and social norms as moderators of deterrence. *Law Human Behav.* **28**(5) 547–567.

Whitman, M. E. 2003. Enemy at the gate: Threats to information security. *Comm. ACM* **46**(8) 91–95.

Whitman, M. E. 2004. In defense of the realm: Understanding the threats to information security. *Internat. J. Inform. Management* **24**(1) 43–57.

Whitman, M. E., H. Mattord. 2005. *Principles of Information Security*. Course Technology, Boston.

Whitman, M. E., A. M. Townsend, R. J. Alberts. 2001. Information systems security and the need for policy. M. Khosrowpour, ed. *Information Security Management: Global Challenges in the New Millennium*. Idea Group Publishing, Hershey, PA, 9–18.

Wiant, T. L. 2003. Policy and its impact on medical record security. Unpublished doctoral dissertation, University of Kentucky, Lexington.

Witte, D., D. Woodbury. 1985. The effect of tax laws and tax administration on tax compliance: The case of the U.S. individual income tax. *National Tax J.* **38**(1) 1–13.

Workman, M., J. Gathegi. 2007. Punishment and ethics deterrents: A study of insider security contravention. *J. Amer. Soc. Inform. Sci. Tech.* **58**(2) 212–222.

Wybo, M. D., D. W. Straub. 1989. Protecting organizational information resources. *Inform. Resources Management J.* **2**(4) 1–15.