CORE
Metadata, citation and similar papers at core.ac.uk
Provided by AIS Electronic Library (AISeL)

Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2004 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2004

The Role of Individual Characteristics on the Effectiveness of IS Security Countermeasures

John D'Arcy
Temple University

Anat Hovav
Temple University

Follow this and additional works at: http://aisel.aisnet.org/amcis2004

Recommended Citation
D'Arcy, John and Hovav, Anat, "The Role of Individual Characteristics on the Effectiveness of IS Security Countermeasures" (2004). *AMCIS 2004 Proceedings*. 176.
http://aisel.aisnet.org/amcis2004/176

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2004 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

The Role of Individual Characteristics on the Effectiveness of IS Security Countermeasures

John D'Arcy
Temple University
jdarcy@temple.edu

Anat Hovav
Temple University
anat.hovav@temple.edu

ABSTRACT

General deterrence theory suggests that deterrent security countermeasures (e.g., security policies, security awareness programs, security software) can be used to control IS misuse in organizations. However, empirical studies that have examined the effectiveness of such techniques have produced inconclusive results. A limitation of these studies is that they ignore the impacts of sanction perceptions and individual characteristics on IS misuse behavior. The purpose of this paper is to reconcile the discrepant findings of prior research by introducing a conceptual model that proposes a relationship between deterrent security countermeasures, sanction perceptions, individual characteristics, and IS misuse. The model includes the following propositions: (i) deterrent security countermeasures increase perceived certainty and severity of sanctions, which leads to lower IS misuse intention; (ii) the relationship between deterrent countermeasures and perceived certainty and severity of sanctions is moderated by an individual's computer self-efficacy, computer experience, gender, age, risk propensity, and employment context.

Keywords

IS security, computer abuse, IS misuse, general deterrence theory

INTRODUCTION

Employee misuse of information systems (IS) represents a very real and costly threat to organizations. The most recent CSI/FBI Computer Crime and Security Survey (Power, 2003) reports that 45% of industry and government respondents face IS security incidents due to the actions of legitimate users, with estimated losses as high as $100,000 per incident. This same group of respondents estimates over $11 million in losses due to insider abuse of network access. Further, the percentage of IS security incidents from inside the organization has risen steadily from 37% in 1999 to 45% in 2003. There is evidence that this trend is likely to continue in the future. The computer literacy of organizational staffs has increased over the years, creating sophisticated users of technology. An undesirable side effect of this increased sophistication is that users are becoming adept at committing various types of computer abuse (Straub and Nance, 1990).

While internal IS security incidents no longer outnumber externally initiated security incidents (Power, 2002), the insider threat remains the greatest single risk to organizations. Most security experts agree that more successful attacks come from inside the organization than from the outside and that insider attacks are potentially more costly (Schultz, 2002; Shaw, Ruby, and Post, 1998). Researchers have suggested that organizations engage in deterrent efforts in order to control IS misuse (Dhillon, 1999; Parker, 1981). Parker (1981) was an early advocate of procedural deterrents, such as guidelines and policy statements, in lowering IS misuse by white-collar amateurs. More recently, researchers have suggested that organizations adopt a mix of procedural (e.g., security policies, acceptable usage guidelines, security awareness programs) and technical (e.g., access controls, user ID/passwords, biometric controls) deterrent countermeasures. The general theory of deterrence from the field of criminology provides theoretical justification for the use of deterrent countermeasures as a means to limit the incidence of IS misuse in organizations. The theory argues that the use of deterrent countermeasures will increase individuals' perceptions of the likelihood and severity of punishment and therefore dissuade them from engaging in illegal and/or illicit computing behaviors.

Straub (1990) empirically tested the general deterrence theory and found that use of deterrent countermeasures (e.g., distributed policy statements that specify conditions for proper system use and security software) was associated with lower levels of IS misuse. However, research that has explored the impact of deterrent techniques on individual IS misuse behavior

has been inconclusive. A possible explanation for these equivocal results is that prior studies have not assessed the impact of deterrent countermeasures on individual perceptions of punishment certainty and severity, which, according to general deterrence theory, have a direct influence on abusive behavior intentions. Moreover, several individual characteristics that influence perceptions of punishment have not been considered.

The purpose of this paper is to reconcile the discrepant findings of prior IS deterrence research by introducing a conceptual model that proposes a relationship between deterrent security countermeasures, sanction perceptions, individual characteristics, and IS misuse behavior. In particular, the paper includes the following propositions: *(i) deterrent security countermeasures increase perceived certainty and severity of sanctions associated with IS misuse, which leads to lower IS misuse intentions; (ii) the relationship between deterrent countermeasures and perceived certainty and severity of sanctions is moderated by an individual's computer self-efficacy, computer experience, gender, age, risk propensity, and employment context.* The proposed model provides a better understanding of the impact of security countermeasures on IS misuse and should also assist managers in determining appropriate uses for IS security countermeasures.

The remainder of the paper is organized as follows. The next section provides a definition of IS misuse. This is followed by a review of prior studies that have assessed the impact of security countermeasures on IS misuse and potential explanations for the inconclusive results of previous research. Next, the paper's model and propositions are presented. The final section includes implications of the proposed model for researchers and practitioners as well as possible methodological approaches for empirical testing.

DEFINITION OF IS MISUSE

IS misuse can be a very subjective term, ranging from behaviors that are unethical and/or inappropriate (e.g., inappropriate use of e-mail and Internet privileges) to those that are illegal (e.g., stealing company information). Examples of IS misuse include theft or modification of computer programs, embezzlement or modification of data, unauthorized use of computer services, purposeful interruption of computer services, inadequate control of media, unauthorized access to passwords, and destruction of data by computer viruses (Foltz, 2000; Straub, 1990). This paper adopts a broad definition of IS misuse as "the intentional misuse of computer systems by users who are authorized to access those systems and networks" (Schultz, 2002, p. 526). This definition can include behaviors that are considered illegal, inappropriate, and unethical in the context of IS (Leonard and Cronan, 2001).

LITERATURE REVIEW

Prior studies have used the lens of general deterrence theory (GDT) from the field of criminology to assess the effectiveness of various security countermeasures in lowering IS misuse. GDT predicts that "disincentives" or sanctions dissuade potential offenders from illegal behavior and that as the certainty and severity of sanctions increase, the level of illegal behaviors should decrease (Gibbs, 1975). Within the realm of IS, GDT predicts that use of deterrent security countermeasures (e.g., security policies and guidelines, security awareness programs, preventative security software) will lower IS misuse by convincing potential abusers that there is too high a certainty of getting caught and punished severely (Straub and Welke, 1998).

Straub (1990) used a GDT-based theoretical framework to empirically test the effectiveness of deterrent and preventative security countermeasures in lowering computer misuse. Survey responses from IS personnel in 1,211 randomly selected organizations indicated that higher levels of deterrent (e.g., number of information sources, number of security staff hours per week) and preventative (e.g., screen access to a system to admit authorized users only and use of security software) security controls were associated with lower levels of misuse. In addition, use of more comprehensive preventative security software was found to be associated with greater ability to identify perpetrators of abuse and to discover more serious computer misuse incidents (Nance and Straub, 1988). Kankanhalli, Teo, Tan, and Wei (2003) also tested the effectiveness of deterrent and preventative measures on IS security effectiveness. Consistent with GDT, the researchers found that greater organizational deterrent efforts (in the form of man-hours expended on IS security purposes) and preventative efforts (in the form of more advanced security software) were associated with higher perceived IS security effectiveness.

In contrast to organizational-level studies, studies that have tested the effectiveness of deterrent countermeasures on individual IS misuse behavior have produced mixed results. Straub, Carlson, and Jones (1993) conducted a field study to examine the impact of deterrent efforts in preventing student cheating on out-of-class computer programming assignments. Results showed that deterrent efforts (e.g., dissemination of definition of computer abuse and rules governing punishment) combined with public warnings of sanctions were effective in deterring cheating behavior. Foltz (2000) assessed the before and after effects of a university computer usage policy and found that the policy had no effect on IS misuse intentions and behaviors involving modifying, stealing, or destroying software and data. Harrington (1996) assessed the influence of codes of ethics on computer abuse intentions among IS employees and found that codes had a deterrent effect only for those individuals that were high in a psychological trait called responsibility denial. Thus, Harrington's results suggest that the impacts of deterrents are contingent on individual characteristics.

In summary, while prior organizational-level studies provide strong evidence of the effectiveness of deterrent countermeasures in lowering IS misuse, research that has explored the impact of deterrent techniques on individual IS misuse behavior has been inconclusive.

A limitation of prior IS deterrence studies is that they have failed to assess the impact of deterrent countermeasures on individual perceptions of punishment certainty and severity, which, according to general deterrence theory, have a direct influence on abusive behavior intentions. The deterrence literature argues that it is the perceptions of sanctions rather than the sanctions themselves that lead to deterrence (Gibb, 1975; Tittle, 1980). The impact of sanctions or sanctioning practices on criminal behavior works through perceived certainty and perceived severity of sanctions. Objective properties of sanctions influence perceived certainty and severity of sanction, which in turn affect behavior (Richards and Tittle, 1981). This suggests that the impact of deterrent security countermeasures on IS misuse behavior is dependent upon the countermeasures' ability to influence an individual's perception of sanction risk (e.g., getting caught and getting punished). Straub (1990) and Kankanhalli et al. (2003) both recognize the importance of sanction perceptions in their studies. However, neither study includes measures of sanction perceptions as variables. Straub (1990) contends that objective measures of deterrents and preventatives serve as surrogates for perceived certainty and severity of sanctions since "deterrent security activities represent how potential abusers perceive risk" (Straub, 1990, p. 258). Similarly, Kankanhalli et al. (2003) assert that "deterrent efforts correspond to certainty of sanctions because the amount of such efforts directly affects the probability that IS abusers will be caught" (p. 141). However, the deterrence literature suggests that objective measures may not serve as adequate surrogates for perceived certainty and severity of sanctions since perceptions of sanction characteristics can vary independently of objective sanction characteristics (Gibbs, 1975; Tittle, 1980). Therefore, individual perceptions of the threats imposed by deterrent security countermeasures may not be directly proportional to the actual level of countermeasures employed in an organization. The model presented in this paper accounts for sanction perceptions by including perceived certainty and severity of sanctions as links between deterrent security countermeasures and IS misuse intentions.

Another concern of prior IS deterrence studies is that they have not accounted for the impact of individual characteristics on the relationship between security countermeasures and IS misuse. With the exception of Harrington (1996), prior IS deterrence studies have implicitly assumed that the impact of deterrent countermeasures is the same for all individuals. Existing research suggests that this may be a false assumption, as sanctions have been shown to have different deterrence values for persons with different perspectives on the law, morality, and/or the threat of punishment itself (Silberman, 1976). Variables such as age, gender, risk propensity, expertise, socioeconomic status, race, geographic mobility, and labor force status have all been shown to influence perceptions of sanctions and projected deviant and criminal behavior (Hollinger and Clark, 1989; Tittle, 1980; Weaver and Carroll, 1989). Deterrence researchers have called for a greater emphasis on understanding the factors that influence sanction perceptions in order to identify the conditions under which sanctions are likely to be important influences on behavior (Nagin and Pogarsky, 2001). Peace, Galletta, and Thong (2003) also suggest the need for further research to understand what influences sanction perceptions in the context of IS. The model presented in this paper includes the moderating impacts of computer self-efficacy, computer experience, gender, age, risk propensity, and employee context on the effectiveness of deterrent security countermeasures.

PROPOSED MODEL

Using the framework of GDT, this paper presents a model that explores the impact of deterrent security countermeasures on sanction perceptions, which in turn predict IS misuse behavior intentions. The model also considers individual characteristics that moderate the relationship between deterrent countermeasures and sanction perceptions. The complete model is illustrated in Figure 1 and the proposed relationships are discussed in the following sections.

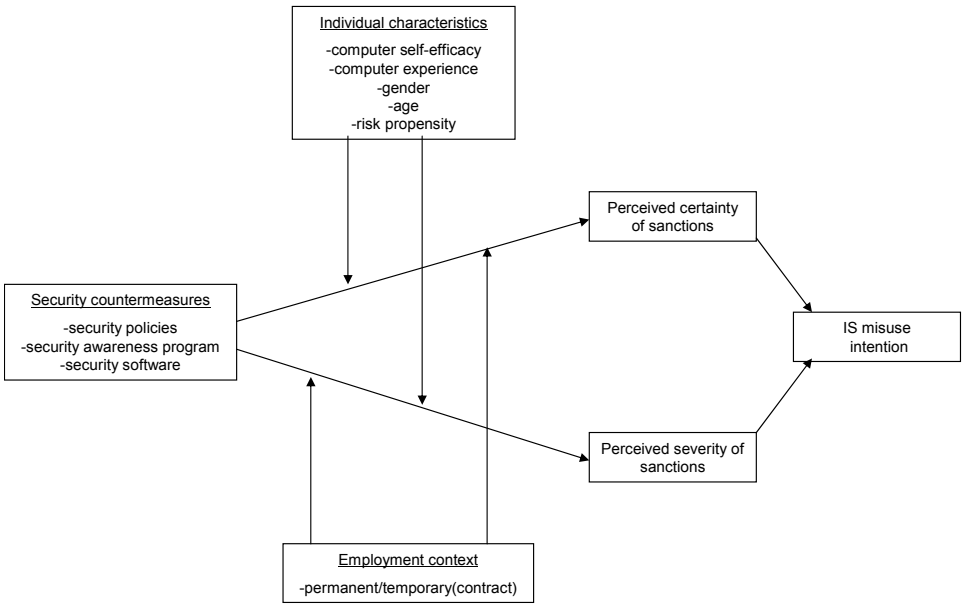

Figure 1. A Model Linking Deterrent Security Countermeasures to IS Misuse Intention

A prominent finding from over 30 years of deterrence research is that sanction fear has consistently been able to predict various criminal and deviant behaviors (Nagin and Pogarsky, 2001; Tittle, 1980). Sanction fear is typically measured using two primary constructs: certainty of sanction and severity of sanction. The certainty of sanction refers to the probability of being punished, and the severity of sanction refers to the degree of punishment (Gibbs, 1975). Tittle (1980) found that sanction fear was negatively associated with intention to engage in several socially deviant behaviors (e.g., lying to one's spouse, sitting during the national anthem, smoking marijuana) as well as deviant behavior in the workplace (e.g., making personal use of an employer's equipment). Hollinger and Clark (1983) found that employees who perceived lower certainty and severity of organizational sanctions were more likely to steal from their employers. IS misuse is typically characterized as an amateur, white-collar crime or antisocial behavior (Parker, 1981; Straub, 1990). Therefore, both perceived certainty and severity of sanctions should be inversely related to IS misuse behavior:

P1: Perceived certainty and severity of sanctions are both negatively associated with IS misuse behavior.

Deterrence research posits that objective properties of sanctions influence perceived severity and certainty of sanction, which in turn affect behavior (Richards and Tittle, 1981). In terms of IS security, this suggests that active and visible deterrent efforts can convince potential abusers of the certainty and severity of punishment. Straub (1990) identifies security policies, security awareness programs, and security systems as examples of countermeasures that organizations can employ to control IS misuse. Security policies are meant to deter IS misuse by clearly defining unacceptable or illegal conduct, thereby increasing the perceived threat of punishment (Lee and Lee, 2002). Security awareness programs convey knowledge about risks in the organizational environment and emphasize actions taken by the firm, including policies and sanctions for

violations. A major reason for such programs is to convince potential abusers that the company is serious about securing its systems and will not treat intentional breaches of security lightly (Straub and Welke, 1998). Thus, security awareness programs stress both the certainty and severity of sanctioning. Security systems (e.g., access controls, user ID/passwords) directly impact misuse behavior by preventing access to information resources. However, Straub and Welke (1998) argue that security software also has a deterrent effect on future misuse by convincing potential offenders of the certainty and severity of punishment. Therefore, the following is proposed:

P2: Deterrent security countermeasures (e.g., security policies, security awareness programs, and security software) are positively associated with both perceived certainty and severity of sanctions.

Prior research suggests that the relationship between security countermeasures and sanction perceptions is moderated by individual characteristics (Tittle, 1980; Harrington, 1996). Based on a review of the IS security, criminology, and risk behavior literatures, individual factors that should logically influence the degree to which security countermeasures influence sanction perceptions are discussed below.

Research that has examined risky decision making among various groups suggests that there is a positive relationship between perceptions of self-efficacy and risk-taking behavior (Dulebohn, 2002; Wyatt, 1990). Laboratory research by Kruegar and Dickinson (1994) suggests that self-efficacy influences risk taking behavior through opportunity recognition. They found that an increase in self-efficacy increases perceptions of opportunity and decreases perceptions of threat and that changing opportunities of threat perceptions changes risk taking behavior. Given that IS misuse is a risky behavior, the preceding discussion suggests that individuals with high self-efficacy have lower perceptions of threats pertaining to IS misuse and therefore are less likely to be deterred by security countermeasures. However, IS misuse is unique in that the ability to perform such behaviors requires some level of computer skills. Therefore, this model includes computer self-efficacy instead of general self-efficacy since the behaviors being studied involve the use of IS resources. Computer self-efficacy is defined as "individuals' judgment of their computer-related skills in diverse situations" (Compeau and Higgins, 1995, p. 192). The above discussion suggests the following proposition:

P3: Computer self-efficacy moderates the effect of deterrent security countermeasures on both perceived certainty and severity of sanctions. Compared with individuals with low computer self-efficacy, individuals with high computer self-efficacy will perceive less certainty and severity of sanctions in response to deterrent security countermeasures.

In addition to perceptions of computer-related skills, there is also suggestive evidence that actual levels of computing skills impact threat perceptions and therefore influence the effectiveness of security countermeasures in controlling IS misuse. Loch and Conger (1996) found that an individual's level of computer literacy was a significant influence on ethical decision-making involving the use of computers. Weaver and Carroll (1985) studied behaviors of experienced and novice shoplifters and found that perceptions of the likelihood of sanctions were much stronger for novices. Novice shoplifters were generally more fearful of punishment and more easily deterred. Experienced shoplifters perceived greater opportunities for shoplifting and were less deterred by retailer tactics such as mirrors, cameras, and visible sales personnel. Together, these results suggest that deterrent security countermeasures are less likely to increase sanction perceptions for IS misuse among highly trained or experienced computer users. This leads to the following proposition:

P4: Computer experience moderates the effect of deterrent security countermeasures on both perceived certainty and severity of sanctions. Compared with individuals with less computer experience, individuals with more computer experience will perceive less certainty and severity of sanctions in response to deterrent security countermeasures.

The deterrence literature has consistently shown that the impact of sanctions is weaker on men than women (Tittle, 1980). Richards and Tittle (1981) surveyed respondents on the probability that they would be arrested if they were to commit six crimes ranging from minor theft (worth about $5) to assault (physically harming someone on purpose) and found that the perceived risk of arrest was lower among men for all six offenses. Hollinger and Clark (1983) found that men were more

likely to steal from their employers. Within the IS literature, empirical results have shown that men are more likely to commit software piracy (Kreie and Cronan, 1998) and engage in numerous unethical behaviors involving the use of computers (Gattiker and Kelley, 1999; Leonard and Cronan, 2001; Loch and Conger, 1996). Considered together, the above findings suggest that men perceive less risk in committing IS misuse and therefore are less likely than women to perceive certainty and severity of sanctions in response to deterrent security countermeasures.

P5: Gender moderates the effect of deterrent security countermeasures on both perceived certainty and severity of sanctions. Compared with women, men will perceive less certainty and severity of sanctions in response to deterrent security countermeasures.

Another individual characteristic that has been consistently shown to influence sanction perceptions is age. Tittle (1980) found that age was inversely related to deviance intentions in seventeen of the eighteen behaviors he studied. Dulebohn (2002) found a negative association between age and risk tolerance in selecting investment options in an employee-sponsored retirement plan. Hollinger and Clark (1983) found that perceptions of the certainty and severity of punishment for stealing from an employer were much lower among younger (under 25) employees. The IS literature also suggests that age impacts sanction perceptions. Young employees have been shown more likely to pirate software and engage in unethical computing behavior (Gattiker and Kelley, 1999). These results suggest that younger employees perceive less risk of sanctions for committing IS misuse and that the impact of security countermeasures on sanction perceptions is inversely related to age.

P6: Age moderates the effect of deterrent security countermeasures on both perceived certainty and severity of sanctions. Compared with older people, younger people will perceive less certainty and severity of sanctions in response to deterrent security countermeasures.

Zimring and Hawkins (1973) maintain that those who have a high propensity toward risk will be less deterred than those who avoid risks. Risk propensity can be defined as the tendency of a decision maker to take risky actions (Sitkin and Pablo, 1992). It is an enduring and persistent individual trait that is consistent across various situations, although some researchers argue that it can change over time as a result of experience (Sitkin and Weingart, 1995). If an individual has a high risk-taking propensity, (s)he may tend to underestimate the risks involved in a situation. Conversely, an individual with a low risk-taking propensity will weigh negative outcomes more highly, leading to heightened perception of risk. Sitkin and Weingart (1995) found a positive relationship between risk propensity and risky decision making among student subjects in a laboratory experiment. In the context of IS misuse, this literature suggests that individuals with higher risk propensities will perceive less sanction risk from security countermeasures than those that have lower risk propensities. This leads to the following proposition:

P7: Risk propensity moderates the effect of deterrent security countermeasures on both perceived certainty and severity of sanctions. Compared with individuals with low risk propensity, high risk propensity individuals will perceive less certainty and severity of sanctions in response to deterrent security countermeasures

Prior deterrence studies have shown a relationship between employment context and deviant behaviors. Tittle (1980) found increased proneness toward deviant behavior among part-time employees of an organization and also found that individuals who moved more often were more likely to engage in occupational specific deviance (e.g., making personal use of an employer's equipment). These results suggest that employment context may have a significant impact on sanction perceptions associated with IS misuse. The number of temporary (contract) workers that comprise organizational staffs continues to rise, especially as a result of outsourcing arrangements (Winter and Gill, 2001). Temporary (contract) workers are employed by a third party and not by the businesses in which they are performing their work. Therefore, it seems plausible that temporary workers would perceive fewer sanction risks for committing IS misuse. Moreover, temporary workers are highly transient, which Tittle (1980) suggests leads to freer behavior and less conformity with organizational norms. Ang and Slaughter (2000) studied the differences between permanent and temporary contract workers on software development teams and found that contract workers were perceived by their supervisors as less loyal, obedient, and trustworthy. Thus, it is proposed that:

P8: Employment context moderates the effect of deterrent security countermeasures on both perceived certainty and severity of sanctions. Compared with individuals who are permanent employees of an organization, temporary (contract) workers will perceive less certainty and severity of sanctions in response to deterrent security countermeasures.

DISCUSSION AND CONCLUSION

This paper advances a model of the effect of deterrent security countermeasures on IS misuse behavior. It is argued that this effect is mediated by perceptions of the certainty and severity of sanctions for committing IS misuse. In addition, computer self-efficacy, computer experience, gender, age, risk propensity, and employment context are proposed to moderate the relationship between deterrent security countermeasures and sanction perceptions. The model is based on the idea that sanction perceptions and individual variables explain, in part, the inconclusive results reported in previous IS deterrence studies.

This research contributes to the IS security literature by incorporating several individual variables into the relationship between deterrent security countermeasures and IS misuse behavior. These variables have not been considered in prior studies. In addition, the proposed model provides guidance to managers on the specific conditions where deterrent security countermeasures may or may not be effective. This research is needed, as Straub and Welke (1998) found that managers are generally not aware of the deterrent techniques available for controlling IS misuse.

The next step is to test the propositions presented in this paper. Tittle (1980) suggests the use of survey questions that ask for future IS misuse intentions since asking for future intentions establishes time precedence and helps in establishing causal order. However, direct questions about engaging/not engaging in IS misuse may not be appropriate due to the sensitive nature of the behaviors in question. A more suitable option may be the use of scenarios involving different forms of IS misuse. Scenarios have the advantage of providing a less intimidating way to respond to sensitive issues and offer realistic situations that place the subject in a decision-making role (Gattiker and Kelley, 1999). Moreover, scenarios avoid the subject's tendency to try to gain experimenter approval and so are commonly used in deterrence research (Harrington, 1996). Controlled laboratory experiments, field studies, and simulations offer additional methodological approaches for empirical testing.

REFERENCES

1. Ang, S., and Slaughter, S.A. (2001) Work Outcomes and Job Design for Contract Versus Permanent Information Systems Professionals on Software Development Teams, *MIS Quarterly*, 25, 3, 321-350.
2. Compeau, D.R., and Higgins, C.A. (1995) Computer Self-Efficacy: Development of a Measure and Initial Test, *MIS Quarterly*, 19, 2, 189-211.
3. Dhillon, G. (1999) Managing and Controlling Computer Misuse, *Information Management & Computer Security*, 7, 4, 171-175.
4. Dulebohn, J.H. (2002) An Investigation of the Determinants of Investment Risk Behavior in Employer-Sponsored Retirement Plans, *Journal of Management*, 28, 1, 3-26.
5. Foltz, C.B. (2000) The Impact of Deterrent Countermeasures Upon Individual Intent to Commit Misuse: A Behavioral Approach, Unpublished Doctoral Dissertation, University of Arkansas.
6. Gattiker, U.E., and Kelley, H. (1999) Morality and Computers: Attitudes and Differences in Moral Judgments, *Information Systems Research*, 10, 3, 233-254.
7. Gibbs, J.P. (1975) Crime, Punishment, and Deterrence, Elsevier, New York.
8. Harrington, S.J. (1996) The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions, *MIS Quarterly*, 20, 3, 257-278.
9. Hollinger, R.C., and Clark, J.P. (1983) Deterrence in the Workplace: Perceived Certainty, Perceived Severity, and Employee Theft, *Social Forces*, 62, 2, 398-418.

10. Kankanhalli, A., Teo, H.-H., Tan, B.C.Y., and Wei, K.-K. (2003) An Integrative Study of Information Systems Security Effectiveness, *International Journal of Information Management*, 23, 2, 139-154.
11. Kreie, J., and Cronan, T.P. (1998) How Men and Women View Ethics, *Communications of the ACM*, 41, 9, 70-76.
12. Kruegar, N.J., and Dickson, P.R. (1994) How Believing in Ourselves Increases Risk Taking: Perceived Self-Efficacy and Opportunity Recognition, *Decision Sciences*, 25, 3, 385-400.
13. Lee, J., and Lee, Y. (2002) A Holistic Model of Computer Abuse Within Organizations, *Information Management & Computer Security*, 10, 2, 57-63.
14. Leonard, L.N.K., and Cronan, T.P. (2001) Illegal, Inappropriate, and Unethical Behavior in an Information Technology Context: A Study to Explain Influences, *Journal of the Association for Information Systems*, 1, 1-31.
15. Loch, K.D., and Conger, S. (1996) Evaluating Ethical Decision Making and Computer Use, *Communications of the ACM*, 39, 7, 74-83.
16. Nagin, D.S., and Pogarsky, G. (2001) Integrating Celerity, Impulsivity, and Extralegal Sanction Threats Into a Model of General Deterrence and Evidence, *Criminology*, 39, 4, 865-891.
17. Nance, W.D., and Straub, D.W. (1988) An Investigation Into the Use and Usefulness of Security Software in Detecting Computer Abuse, *Proceedings of the Ninth International Conference on Information Systems*, Minneapolis, MN.
18. Parker, D.B. (1981) Computer Security Management, Reston Publishers, Reston, VA.
19. Peace, A.G., Galletta, D.F., and Thong, J.Y.L. (2003) Software Piracy in the Workplace: A Model and Empirical Test, *Journal of Management Information Systems*, 20, 1, 153-177.
20. Power, R. (2002) 2002 CSI/FBI Computer Crime and Security Survey, *Computer Security Issues and Trends*, 8, 1, 1-28.
21. Power, R. (2003) 2003 CSI/FBI Computer Crime and Security Survey, *Computer Security Issues and Trends*, 9, 1, 1-22.
22. Richards, P., and Tittle, C.R. (1981) Gender and Perceived Chances of Arrest, *Social Forces*, 59, 4, 1182-1199.
23. Schultz, E.E. (2002) A Framework for Understanding and Predicting Insider Attacks, *Computers & Security*, 21, 6, 526-531.
24. Shaw, E.S., Ruby, K.G., and Post, J.M. (1998) The Insider Threat to Information Systems: The Psychology of the Dangerous Insider, *Security Awareness Bulletin*, 2, 1-10.
25. Silberman, M. (1976) Toward a Theory of Criminal Deterrence, *American Sociological Review*, 41, 3, 442-461.
26. Sitkin, S.B., and Pablo, A.L. (1992) Reconceptualizing the Determinants of Risk Behavior, *Academy of Management Review*, 17, 1, pp 9-38.
27. Sitkin, S.B., and Weingart, L.R. (1995) Determinants of Risky Decision-Making Behavior: A Test of the Mediating Role of Risk Perceptions and Propensity, *Academy of Management Journal*, 38, 6, 1573-1592.
28. Straub, D.W. (1990) Effective IS Security: An Empirical Study, *Information Systems Research*, 1, 3, 255-276.
29. Straub, D.W., Carlson, P.J., and Jones, E.H. (1993) Deterring Cheating by Student Programmers: A Field Experiment in Computer Security, *Journal of Management Systems*, 5, 1, 33-48.
30. Straub, D.W., and Nance, W.D. (1990) Discovering and Disciplining Computer Abuse in Organizations: A Field Study, *MIS Quarterly*, 14, 1, 45-60.
31. Straub, D.W., and Welke, R.J. (1998) Coping With Systems Risk: Security Planning Models for Management Decision Making, *MIS Quarterly*, 22, 4, 441-469.
32. Tittle, C.R. (1980) Sanctions and Social Deviance: The Question of Deterrence, Praeger, New York.
33. Weaver, F.M., and Carroll, J.S. (1985) Crime Perceptions in a Natural Setting by Expert and Novice Shoplifters, *Social Psychology Quarterly*, 48, 4, 349-359.
34. Winter, S.J., and Gill, G.T. (2001) OfficeTech: A New Paradigm in Office Services?, *Journal of Information Technology*, 16, 1, 23-32.
35. Wyatt, G. (1990) Risk-Taking and Risk-Avoiding Behavior: The Impact of Some Dispositional and Situational Variables, *The Journal of Psychology*, 124, 4, 437-447.
36. Zimring, F.E., and Hawkins, G. (1973) Deterrence: The Legal in Crime Control, The University of Chicago Press, Chicago.