Journal of Business Ethics
DOI 10.1007/s10551-008-9909-7

Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures

John D'Arcy
Anat Hovav

ABSTRACT. Research from the fields of criminology and social psychology suggests that the deterrent effect of security countermeasures is not uniform across individuals. In this study, we examine whether certain individual characteristics (i.e., computer self-efficacy) or work arrangement (i.e., virtual status) moderate the influence of security policies, security education, training, and awareness (SETA) program, and computer monitoring on information systems misuse. The results suggest that computer savvy individuals are less deterred by SETA programs and computer monitoring, while these countermeasures are also less influential (from a deterrence perspective) on employees that spend more working days outside the office. Implications for both the research and practice of information security are discussed.

KEY WORDS: information systems security, deterrence theory, computer ethics, information security management, computer self-efficacy, differential deterrence hypothesis, virtual work

Introduction

It is acknowledged within the information security research community that insiders represent one of the most significant threats to the security of organizational information assets (e.g., Dhillon, 1999; Whitman, 2003). In this study, we define an insider as "a person that has legitimately been given the capability of accessing one or many components of the IT infrastructure" (Magklaras et al., 2006, p. 362). The insider threat is evidenced in industry surveys that report between one-half and three-quarters of all security incidents originate from within the organization (Ernst and Young, 2003; InformationWeek, 2005). Considering that a large percentage of security breaches go undetected (Hoffer and Straub, 1989), it is likely that these figures underestimate the actual level of insider information systems (IS) misuse.

Information security specialists recommend a combination of procedural and technical countermeasures as a strategy for combating IS misuse. Procedural countermeasures include security policy statements, acceptable usage guidelines, and security education, training, and awareness (SETA) programs. Technical countermeasures include authentication technologies and filtering and monitoring software. Following Straub (1990), we use the term "security countermeasures" to collectively describe these procedural and technical controls. General deterrence theory (GDT) provides theoretical justification for the use of security countermeasures as mechanisms to reduce IS misuse. The theory posits that "disincentives" or sanctions dissuade potential offenders from illicit behavior and as the certainty and severity of sanctions increase, the level of illicit behavior should decrease (Tittle, 1980). Within the context of IS security, GDT suggests that security countermeasures can limit the incidence of IS misuse by convincing potential offenders that there is too high a certainty of getting caught and punished severely (Straub, 1990).

A number of studies have used GDT as a theoretical perspective in examining the effectiveness of various security countermeasures. This research includes empirical investigations of the relationships between security countermeasures and aggregate misuse levels (Kankanhalli et al., 2003; Straub, 1990; Wiant, 2003), as well as the impact of security countermeasures on specific misuse behaviors such as software piracy, modifying, stealing, or destroying data, and computer sabotage (e.g., D'Arcy and

Hovav, 2007; Foltz, 2000; Gopal and Sanders, 1997; Harrington, 1996; Lee et al., 2004). Taken as a whole, the results of these studies have been largely inconclusive. As such, several authors (e.g., Banerjee et al., 1998; Gattiker and Kelley, 1999; Harrington, 1996) have called for further research to better understand what factors influence the effectiveness of security countermeasures.

A potential explanation for the equivocal results of prior studies is the omission of certain individual factors that influence sanction perceptions. The differential deterrence hypothesis (Mann et al., 2003) suggests that the impact of security countermeasures will not be uniform across all persons due to individual and situational differences that influence perceived strength of sanctions. Hence, it is possible that certain security countermeasures that deter some people may be perceived as only a minor threat by others. The purpose of the current study is to investigate this issue by exploring the impact of two likely influences on sanction perceptions in an IS context: computer self-efficacy and virtual status (i.e., the degree to which an employee operates from traditional offices or from dispersed locations via telecommunication equipment; Wiesenfeld et al., 1999). Specifically, we examine whether computer self-efficacy and virtual status moderate the influence of security policies, SETA programs, and computer monitoring on IS misuse intention. While extant research suggests that computer self-efficacy and virtual status may influence security countermeasure effectiveness (e.g., Heath and Tversky, 1991; Kruegar and Dickson, 1994; Williams, 1992; Zimbardo, 1969), neither variable has been included in prior empirical investigations of the topic. Further, an understanding of the influence of virtual status on the effectiveness of security countermeasures is of increasing importance to modern organizations, given the rise in telecommuting and other virtual work arrangements. Recent estimates indicate that by 2011, over 75% of the U.S. workforce will spend at least a portion of their workweek in virtual mode (IDC Research, 2007).

Research model and hypotheses

The study's research model is presented in Figure 1. The model is grounded in GDT and posits that (1) user awareness of security policies, SETA program, and computer monitoring directly influence IS misuse intention, and (2) that the relationships between these three countermeasures and IS misuse intention are moderated by computer self-efficacy and virtual status. Note that our model contains *user awareness* of security policies, SETA program, and computer monitoring, as opposed to objective measures of these variables. This is for two main reasons. First, the impact of security countermeasures as deterrence mechanisms ultimately depends on the actions and awareness of end users, and therefore it is important to understand the impact of these controls from the user perspective. Second, research suggests that end users are not fully aware of the existence of many security countermeasures within their organizations (Finch et al., 2003; Foltz, 2000). The following sections elaborate on the constructs in the research model and the proposed relationships among them.

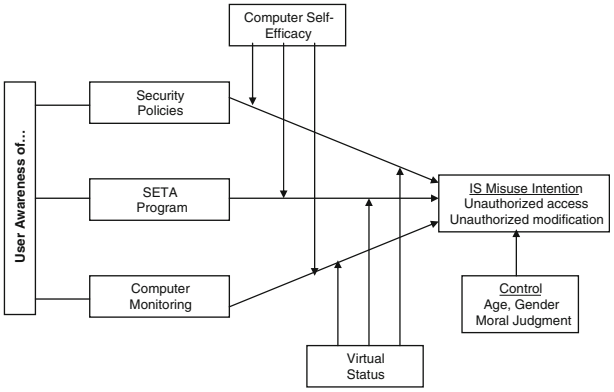

Figure 1. The research model.

IS misuse intention

IS misuse intention is defined as an individual's intention to perform a behavior that is defined by the organization as a misuse of IS resources (Magklaras et al., 2006). One's intention is thought to capture the motivational factors that affect a behavior (Azjen, 1988) and there is a significant body of research supporting intention as a strong predictor of actual behavior (e.g., Sheppard et al., 1988). The current study focuses on two IS misuse intentions: unauthorized access to computerized data and unauthorized modification of computerized

data. Both of these are common types of security breaches in organizations (Richardson, 2007). Moreover, a ranking of IS misuse categories conducted with a panel of experts identified both unauthorized access to and modifications of computerized data as severe threats to organizational information security (D'Arcy and Hovav, 2007).

Security countermeasures: security policies, SETA program, and computer monitoring

Criminological research suggests that active and visible deterrent efforts can convince potential abusers of the certainty and severity of punishment and, based on the predictions of GDT, these increased punishment perceptions will deter illicit behavior (e.g., Tittle, 1980). Straub (1990) identified security polices, SETA programs, and computer monitoring as examples of countermeasures that organizations can employ to deter IS misuse. The direct effects of these countermeasures on unauthorized access and unauthorized modification intentions are reported in D'Arcy and Hovav (2007). Therefore, for purposes of brevity we do not restate these relationships as hypotheses in this paper.

Additional influences on sanction perceptions: computer self-efficacy and virtual status

Deterrence researchers have suggested that the deterrent effect of various sanction practices differs radically from individual to individual and from social group to social group (Bachman et al., 1992; Tittle, 1980). This argument is captured within the differential deterrence hypothesis, which posits that the impact of formal sanctions is not uniform across all persons due to individual and situational differences (Mann et al., 2003). Such differences are thought to influence sanction perceptions, which in turn have a direct effect on behavior (Tittle, 1980). Existing research from the fields of criminology and social psychology supports the differential deterrence hypothesis as 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/or projected deviant and criminal behavior (e.g., Hollinger and Clark, 1983; Weaver and Carroll, 1985). There is also support for the differential deterrence hypothesis within the IS literature. Harrington (1996) found that an individual personality trait, responsibility denial, influenced the effectiveness of IS codes of ethics in deterring computer abuse behaviors. A review of the IS security, criminology, and risk behavior literature identified computer self-efficacy and virtual status as additional variables that may impact the deterrent effectiveness of security countermeasures due to their influence on sanction perceptions.

Computer self-efficacy is defined as "individuals' judgment of their computer-related skills in diverse situations" (Compeau and Higgins, 1995, p. 192). The construct has generally been used to refer to one's overall confidence in their ability to use computers. Research that has examined risky decision making among various groups suggests that there is a significant relationship between perceptions of self-efficacy and risk-taking behavior. Wyatt (1990) studied several risky behaviors (e.g., gambling) among college students and found that self-efficacy was the principle variable influencing risk-taking behavior. Heath and Tversky (1991) conducted a series of experiments that suggested that people take significantly more risks in situations in which they feel competent. Research by Kruegar and Dickson (1994) suggests that self-efficacy influences risk-taking behavior through opportunity recognition. The researchers 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, these findings suggest that individuals with higher computer self-efficacy have lower perceptions of threats pertaining to IS misuse. Thus, it can be expected that higher computer self-efficacy users will be less deterred by security countermeasures. This leads to following hypotheses:

H1: Computer self-efficacy will negatively influence the relationship between user awareness of security countermeasures and IS misuse intention.

Virtual status refers to the degree of work that an employee performs within traditional offices or

from dispersed locations via telecommunications equipment (Wiesenfeld et al., 1999). A common arrangement in which employees work virtually is telecommuting. Other forms of virtual work include mobile or remote working arrangements. While organizations cite increased productivity and cost reductions as benefits of virtual work programs (Potter, 2003), a potential drawback is that virtual workers may experience social isolation since they are often separated, both temporally and spatially, from other organizational members (Pearlson and Saunders, 2001). Studies have reported that virtual workers felt excluded from decision making and less visible in their organizations (Mann et al., 2000; Watad and DiSanzo, 2000). The deterrence literature provides evidence that feelings of social isolation can lead to perceptions of decreased sanction costs. Williams (1992) found that increased isolation from community resources of social control (i.e., police agencies) was associated with lower perceived costs of arrest for various forms of violence against one's spouse. Williams (1992) concluded that the influence of social isolation was significant since "if people believe their affairs are detached from the jurisdiction of police, then they will perceive themselves as immune to the attention and actions of police agencies" (p. 624). Applying this same argument to the domain of IS misuse suggests that virtual workers, due to the increased temporal and spatial isolation that is associated with their work, will perceive lower sanction costs for misusing IS resources and therefore will be less deterred by security countermeasures.

Additional evidence that security countermeasures may be less effective against virtual workers comes from deindividuation theory. According to deindividuation theory, when individuals are not seen or paid attention to, they do not feel scrutinized (Zimbardo, 1969). The result is reduced inner constraints based on guilt, shame, fear, and commitment and increasing behavior that is uninhibited and antinormative. Deindividuation theory has been used by IS researchers to describe the sense of anonymity that individuals experience when using information technology (Loch and Conger, 1996). Research suggests that virtual workers may experience the psychological state of deindividuation as a result of being temporally and spatially dispersed from other organizational members. For example, Watad and DiSanzo (2000) reported that virtual workers expressed concern about "being out of sight, and out of mind" of their employing organizations. In addition, as mentioned above, virtual workers may experience psychological separation from other organizational members through social isolation. Feelings of isolation can contribute to a deindividuated state in which virtual workers feel increasingly anonymous and unaccounted for, resulting in decreased perceptions of fear associated with deviant behavior. Considering that security countermeasures rely on increased punishment perceptions to achieve deterrence, the preceding discussion suggests that such controls will have less influence on virtual workers. This leads to the following hypotheses:

H2: Virtual status will negatively influence the relationship between user awareness of security countermeasures and IS misuse intention.

Control variables

Prior research that has examined IS misuse and the general area of criminal and deviant behavior suggests age, gender, and morality are additional variables that should be included because of their potential influence on IS misuse intention. For example, empirical results have shown that younger, male employees are more likely to engage in deviant workplace behavior such as stealing from their employer (Hollinger and Clark, 1983; Tittle, 1980), as well as perform numerous unethical behaviors involving the use of computers (i.e., software piracy, unauthorized access) (e.g., Gattiker and Kelley, 1999; Loch and Conger, 1996). There is also strong empirical support for the role of moral considerations in predicting IS misuse. Silberman (1976) found a negative correlation between moral propensity and several criminal and deviant behaviors such as petty theft, shoplifting, and vandalism. Within the IS literature, Sacco and Zureik (1990) found that beliefs about ethics had a significant impact on computer misuse. Other IS studies have shown a relationship between moral judgments of IS misuse and willingness to engage in such behavior (Kreie and Cronan, 1998; Lee et al., 2004; Leonard and Cronan, 2001). Researchers have also found that

ethical judgments of IS misuse differ depending on the behavior in question (Harrington, 1996; Kreie and Cronan, 1998). For this reason, we focus on moral judgment of the act, as opposed to general level of morality of the individual. It should also be noted that while we recognize the importance of age, gender, and moral judgment in particular, in explaining IS misuse, the current study seeks to assess the hypothesized relationships beyond the influence of these known predictors. Hence, age, gender, and moral judgment are designated as control variables in the analysis.

Methodology

The survey

A survey instrument was designed to capture respondents' intentions regarding two IS misuse scenarios (i.e., unauthorized access and unauthorized modification) and to measure the other variables in the research model. The specific scenarios are presented in the Appendix. For each scenario, respondents were presented with two questions that assessed the likelihood that they would act as the person did in the scenario. This IS misuse intention scale consisted of one original item and one item adapted from Leonard and Cronan (2001). An additional item, adapted from Lin et al. (1999), was included after each scenario to assess moral judgment of the act. Original scales (available in D'Arcy and Hovav, 2007) measuring user awareness of security policies, SETA program, and computer monitoring were presented in a separate section, followed by computer self-efficacy, virtual status, and demographic items. Computer self-efficacy was measured with six items adapted from Compeau and Higgins's (1995) original 10-item scale. This six-item scale is also used in Chau (2001), where it exhibited strong psychometric properties. Virtual status was measured using three open-ended questions that ask respondents to indicate how many days per week they spend in the office, home, and mobile work modes, respectively (Wiesenfeld et al., 1999). From the data, a virtual status variable that captures the number of days that an employee spends working outside the office was generated. Higher scores indicate a greater number of working days outside the office and thus a higher virtual status.

Sample

Survey responses were collected from two groups of participants: employed professionals taking evening MBA classes at two mid-Atlantic U.S. universities and employees in eight organizations located across the U.S. For the MBA sample, 356 questionnaires were distributed and 238 usable responses were obtained (67% response rate). For the industry sample, a total of 805 employees received an invitation to complete the survey, and 269 usable responses were obtained (38% response rate). Results of the instrument validation were largely consistent across the two sample groups,[1] and therefore the data were pooled into a combined sample (n = 507) to increase statistical power and facilitate brevity of results reporting. The combined sample consisted of almost two-thirds (65%) males, and about half of respondents (52%) were in the 25–34 age group. Respondents held managerial (25%), technical (30%), professional (39%), and administrative (6%) positions and worked in various industries including manufacturing (32%), finance/insurance (22%), software (17%), healthcare (10%), advertising/marketing (7%), education (6%), and retail (6%). Company size ranged from small to large, with a sizable portion (44%) having 10,000 or more employees.

Analysis and results

Partial least squares (PLS-Graph 3.00) was used to analyze the data. The main reason for selecting PLS was to utilize the PLS product indicator approach for measuring interaction (Chin et al., 2003[2]). A secondary reason is that PLS does not impose normality requirements on the data (Chin, 1998). Formal tests indicated that item responses were not normally distributed in this study, as is often the case in survey-based research (Ping, 2004). Following standard procedure (Anderson and Gerbing, 1988), we first assessed the measurement model, followed by the structural relationships.

Measurement model

The measurement model was assessed through tests of convergent validity, discriminant validity, and reliability. For convergent validity, all factor loadings should exceed 0.70 and average variance extracted (AVE) for each construct should exceed 0.50 (Fornell and Larcker, 1981). As shown in Table I, both criteria were met for all constructs.

For discriminant validity, the square root of the AVE for each construct should be greater than the inter-construct 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 Tables I and II, these conditions were met for all constructs. Finally, the reliabilities of all constructs were above the recommended 0.70 threshold (Fornell and Larcker, 1981), as shown in the composite reliability column of Table II.

Structural model

The hypotheses were tested by examining six structural models. A main effects model, a model with computer self-efficacy (CSE) interaction variables added, and a model with virtual status (VS) interaction variables added were each tested with INT 1 (unauthorized access intention) serving as the dependent variable. Further, the same three models were tested with INT 2 (unauthorized modification intention) serving as the dependent variable. A bootstrapping procedure (500 resamples) was used to determine the significance of the paths within the structural models.

TABLE I

Loadings, cross-loadings, and AVEs for multi-item constructs

Construct	Item code	INT1	INT2	P	SETA	M	CSE	AVE
Unauthorized access (INT1)	INT1_1	**0.96**	0.24	0.18	0.22	0.10	0.05	0.95
	INT1_2	**0.98**	0.29	0.20	0.25	0.13	0.04	
Unauthorized mod (INT2)	INT2_1	0.25	**0.93**	0.10	0.03	0.02	0.07	0.87
	INT2_2	0.25	**0.93**	0.08	0.01	0.03	0.17	
Security policies (P)	P1	0.18	0.10	**0.87**	0.53	0.51	0.03	0.73
	P2	0.15	0.11	**0.89**	0.60	0.51	0.11	
	P3	0.17	0.05	**0.79**	0.59	0.51	0.01	
	P4	0.16	0.05	**0.86**	0.64	0.57	0.03	
SETA program (SETA)	SETA1	0.17	0.01	0.46	**0.77**	0.38	0.05	0.71
	SETA2	0.25	0.03	0.58	**0.87**	0.48	0.03	
	SETA3	0.19	0.02	0.67	**0.88**	0.48	0.01	
	SETA4	0.20	0.03	0.59	**0.86**	0.50	0.04	
Computer monitoring (M)	M1	0.13	0.01	0.49	0.52	**0.72**	0.06	0.63
	M2	0.05	0.02	0.60	0.43	**0.84**	0.01	
	M3	0.06	0.04	0.49	0.39	**0.81**	0.09	
	M4	0.13	0.07	0.40	0.45	**0.81**	0.13	
	M5	0.12	0.04	0.45	0.39	**0.80**	0.04	
Computer self-efficacy (CSE)	CSE1	0.00	0.09	0.02	0.04	0.04	**0.76**	0.66
	CSE2	0.00	0.13	0.04	0.01	0.06	**0.79**	
	CSE3	0.02	0.11	0.01	0.05	0.02	**0.86**	
	CSE4	0.03	0.10	0.07	0.02	0.07	**0.84**	
	CSE5	0.08	0.08	0.04	0.06	0.06	**0.84**	
	CSE6	0.07	0.09	0.08	0.02	0.05	**0.81**	

Boldface numbers are loadings (correlations) of indicators to their own construct; other numbers are cross-loadings.

TABLE II

Reliability and inter-construct correlations

Construct	Composite reliability	Inter-construct correlations					
		INT1	INT2	P	SETA	M	CSE
INT1	0.97	**0.97**					
INT2	0.93	0.27	**0.93**				
P	0.91	−0.08	−0.09	**0.85**			
SETA	0.90	−0.24	−0.02	0.68	**0.84**		
M	0.89	−0.12	−0.13	0.61	0.55	**0.79**	
CSE	0.92	0.04	−0.12	0.05	0.18	0.09	**0.81**

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

The latent interaction terms were developed following procedures described in Chin et al. (2003). First, all indicators reflecting the predictor (i.e., security policies, SETA program, computer monitoring) and moderator constructs (i.e., computer self-efficacy and virtual status) were standardized using SPSS 15.0. Further, product indicators were developed by creating all possible products from the two sets of indicators for each predictor–moderator combination. These product indicators were used to represent the latent interaction variables in the structural models. For example, the five measures reflecting the SETA construct (a predictor variable) and the six measures reflecting the CSE construct (a moderator variable) were cross-multiplied to create 30 items that represented the interaction construct SETA*CSE. This same procedure was followed for each combination of the security countermeasure and moderator variables. The results of the structural model analyses are presented in Table III.

The results show partial support for the direct effects of the security countermeasures on IS misuse

TABLE III

Results for structural models (path coefficients and R^2)

	Unauthorized access (INT1)			Unauthorized modification (INT2)		
	Model 1	Model 2	Model 3	Model 1	Model 2	Model 3
Security policies (P)	0.04	0.04	0.04	−0.14**	−0.12*	−0.14**
SETA program (SETA)	−0.16**	−0.14**	−0.16**	0.03	0.04	0.04
Monitoring (M)	−0.03	−0.02	−0.03	−0.17**	−0.15**	−0.16**
Age	−0.09*	−0.09*	−0.09*	−0.13**	−0.13**	−0.14**
Gender	−0.01	−0.01	−0.00	−0.05	−0.04	−0.05
Moral judgment	0.48**	0.49**	0.47**	0.35**	0.35**	0.35**
Computer self-efficacy (CSE)		0.06			−0.03	
CSE*P		−0.02			−0.03	
CSE*SETA		−0.13***			−0.07	
CSE*M		−0.14*			−0.12*	
Virtual status (VS)			−0.02			−0.03
VS*P			−0.04			0.06
VS*SETA			−0.11***			0.07
VS*M			−0.05			−0.10***
R^2 of INT	0.30	0.33	0.32	0.19	0.21	0.21

*$p < 0.05$; **$p < 0.01$; ***$p < 0.10$ (one-tailed test).

intention. Awareness of security policies and computer monitoring is negatively associated with unauthorized modification intention, but not with unauthorized access intention. SETA program is negatively associated with unauthorized access intention, but not unauthorized modification intention. As mentioned, a discussion of these main effect results is included in D'Arcy and Hovav (2007). Therefore, we focus primarily on the hypothesized moderating effects for the remainder of this paper.

In terms of interpreting the moderating effects, the path coefficient for the interaction construct CSE*SETA, for example, would indicate how a change in the level of CSE would change the influence of SETA on IS misuse intention. This same interpretation applies to the other interaction constructs in Table III. Overall, the results provide some support for the moderating influences of computer self-efficacy (CSE) and virtual status (VS). CSE has a significant negative effect on both the relationships between computer monitoring and unauthorized access intention and computer monitoring and unauthorized modification intention. However, from a practical standpoint, the moderating effect of CSE on the relationship between computer monitoring and unauthorized access intention has little relevance, since the direct effect of computer monitoring is not significant for this behavior. CSE does have a marginally significant negative effect on the relationship between SETA program and unauthorized access intention. Taken as a whole, the results provide partial support for H1.

In terms of virtual status, VS has a marginally significant negative effect on both the relationships between SETA program and unauthorized access intention and computer monitoring and unauthorized modification intention. Thus, there is partial support for H2.

As an additional analysis, we examined the means of the security policy, SETA program, and computer monitoring constructs between virtual and non-virtual workers. We were interested in whether virtual workers are more/less aware of the existence of security countermeasures in their organizations. Following Wiesenfeld et al. (1999), we coded individuals working at least 1 day per week outside of the office as virtual workers; all others were coded as non-virtual workers. The sample consisted of 67 virtual workers and 440 non-virtual workers.

TABLE IV

Security countermeasure construct means for virtual and non-virtual workers

Subgroup	Security policies	SETA program	Monitoring*
Non-virtual workers	5.36	4.28	4.47
Virtual workers	5.07	4.16	4.08

*Difference between these subgroups is significant ($p < 0.05$).

Among the virtual workers, the mean number of working days outside the office was close to half a week (2.2 days). As shown in Table IV, awareness of each countermeasure is lower for the virtual worker subgroup. However, the only statistically significant difference between the groups is for awareness of computer monitoring ($p < 0.05$).

Discussion

The purpose of this study was to examine whether certain individual characteristics (i.e., computer self-efficacy) or work arrangements (i.e., virtual status) moderate the influence of security policies, SETA program, and computer monitoring on IS misuse. The moderator variables – computer self-efficacy and virtual status – were chosen based on theoretical considerations and past research. The results provide some evidence that the deterrent effectiveness of SETA programs and computer monitoring is not uniform across all individuals. However, the impact of security policies appears consistent regardless of computer self-efficacy and virtual status.

CSE was shown to have a negative effect on the relationship between SETA and unauthorized access intention. Thus, it appears that SETA programs have less deterrent effect on computer savvy individuals when it comes to this type of misuse. The results also suggest that CSE does not moderate the impact of SETA on unauthorized modification, nor does SETA have a direct effect on this behavior. Unauthorized modification is generally known to be illegal and therefore users that engage in this misuse likely have a strong instrumental intent. This intent may be so strong that incremental deterrent effect of

a SETA program (above that of security policies) is weak, regardless of one's perceived computing skills.

The results regarding the moderating effect of CSE on computer monitoring suggest that computer savvy individuals feel that they can overcome the monitoring capabilities of their organizations and that they are less likely to be caught when engaging in unauthorized modification. More sophisticated users may also realize that security personnel cannot actively ''watch'' all computing activities, even though such activities are automatically logged and recorded by monitoring technologies.

In terms of the VS interaction effects, our results suggest that SETA programs are less effective in deterring unauthorized access for employees that spend more working days outside the office. However, virtual work arrangement does not seem to influence the impact of SETA on unauthorized modification. Similar to our previous explanation, it may be that SETA programs cannot influence the strong intent that is associated with unauthorized modification activities, regardless of a user's virtual status. Our results also suggest that virtual workers do not regard computer monitoring as significant a deterrent toward unauthorized modification as non-virtual workers. This may be because employees perceive that monitoring is confined to organizational boundaries and that once an employee is out of the office, it is more difficult for the organization to monitor his/her computing activities. However, the non-significant impact of VS on the relationship between monitoring and unauthorized access suggests that this explanation may only apply to the most severe types of IS misuse. It is also possible that employees associate monitoring more with data modifications than with access. Employees might not realize that organizations can monitor access even when there is no change to existing information. This assertion is supported by the non-significant direct affect of monitoring on unauthorized access intention. Future research is needed to address this issue more thoroughly.

It is also interesting that user awareness of each of the countermeasures was lower among virtual workers compared to non-virtual workers. This suggests that virtual workers do not perceive the existence of these procedural and technical security controls as strongly as traditional employees. The significant difference in monitoring awareness between the two groups may also explain why virtual status had a limited moderating effect on the impact of computer monitoring.

Finally, while not directly related to our hypotheses, a key finding from the study is that moral judgment had the strongest impact on IS misuse intention for both behaviors. This is not surprising in light of prior work that has shown a strong relationship between morality and various forms of deviant and unethical behavior, including IS misuse. Our results indicate that judgment of whether the behavior is right or wrong has a stronger influence than security policies, SETA program, and computer monitoring in terms of an individual's willingness to engage in IS misuse. These findings suggest avenues for future research, several of which are discussed in the following section.

Contributions, limitations, and future research

This research offers contributions to both research and practice. From a research perspective, the study provides one of the few tests of the differential deterrence hypothesis in the realm of IS security. Previous studies have largely assumed that the impact of security countermeasures is uniform across individuals. By accounting for the moderating influences of computer self-efficacy and virtual status, the current study contributes to an improved understanding of the relationships between security countermeasures and IS misuse. Moreover, by providing evidence that the deterrent effect of certain countermeasures varies due to individual and situational factors, the study helps explain the equivocal findings of prior work (i.e., monitoring is less effective for computer savvy users when it comes to unauthorized modification).

From an information security management perspective, the results indicate that the effectiveness of SETA programs can be improved by tailoring such programs to certain groups of employees. For example, computer knowledge appears to reduce the deterrent effect of SETA for certain misuse behaviors. Thus, security education and training programs should take into consideration the employee's level of computer understanding. Similarly, the moderating effect of computer self-efficacy on monitoring

suggests that users with more computer knowledge believe that they can "cheat" the system and avoid the implications of monitoring technologies. Thus, when implementing such technologies, organizations need to convey to computer savvy users that they are not immune.

The results also indicate that virtual workers are less deterred by SETA programs and computer monitoring for certain misuse behaviors. Therefore, organizations should create specialized security programs for workers that spend more working days outside the office. Such workers need to understand that organizational security measures apply equally whether in or out of the physical boundaries of the office. Moreover, as evident in Table IV, organizations need to dedicate more resources toward making virtual workers aware of existing security countermeasures. This is especially important as more organizations adopt virtual structures, outsource portions of their knowledge work, and implement telecommuting programs.

Like most empirical research, this study has limitations that should be taken into account. These limitations point to important issues for further research. One limitation is the relatively small number of virtual workers in relation to the total sample. This may have contributed to the marginally significant ($p < 0.10$) virtual status interaction effects and the non-significance of several other relationships involving virtual status. However, the virtual workers in our sample worked on average close to half of their workweek outside the office, which suggests that some degree of "virtualness" was captured within this group. Nonetheless, additional research using a larger number of virtual workers is needed to further validate our findings.

Another limitation is the overall amount of variance explained by the security countermeasure and moderator variables in our model. While our results suggest that these variables influence IS misuse decisions, other factors also contribute toward this behavior. Combining the current research model with additional theoretical perspectives may provide further insight into the relationships between security countermeasures and IS misuse. One potentially fruitful area is the integration of morality and security countermeasures. Given the strong influence of moral judgment in explaining IS misuse, future research could investigate the antecedents of moral judgment in the current model, including the impact of security countermeasures. A study by Tenbrunsel and Messick (1999) found that strength of surveillance and sanctioning systems influence ethical judgments by changing individuals' perception of a decision problem from an ethical one to that of a business decision. Additionally, Silberman (1976) suggests that societal laws and regulations can influence moral judgment through a socialization process in which the controls become internalized as self-regulatory mechanisms. It would be interesting to investigate whether this dynamic occurs in the context of IS security. In other words, can certain security countermeasures be used to shape moral judgments of IS misuse?

A further exploration of the current research model could also investigate whether moral judgments of IS misuse differ for virtual workers and for those with varying levels of computer self-efficacy. Examining these interaction effects may provide more precise results in terms of the impact of computer self-efficacy and virtual status on IS misuse intention. An additional question that arises is whether high CSE individuals and virtual workers actually perceive lower sanction costs (as our results would suggest) and whether such perceptions are justified. If high CSE individuals underestimate the risk of sanction, then they are more likely to be susceptible to decision biases such as positive illusions and overconfidence, which in turn could lead to greater occurrence of "insecure" computing behaviors. Future research could explore potential decision biases among high CSE and virtual workers and the impact of such biases on sanction perceptions within these groups.

Conclusion

This study examined whether computer self-efficacy and virtual status influence the deterrent effectiveness of security policies, SETA program, and computer monitoring. Our results provide some evidence that computer savvy users are less deterred by SETA programs and computer monitoring. The results also suggest that SETA programs and monitoring are less influential (from a deterrence

perspective) on users that spend more working days outside the office. While our results were not entirely consistent across both misuse behaviors examined, they do suggest that organizations need to consider different security approaches for different groups of computer users. The findings also underscore the importance of moral judgments in predicting IS misuse, as well as suggest avenues for future research in this area.

Notes

[1] Results of the instrument validation testing for the separate groups are available from the first author.

[2] Chin et al. (2003) provide a discussion and empirical evidence of the advantages of the PLS product indicator approach for measuring interaction effects versus alternative methods such as regression.

Acknowledgments

The authors thank the State Farm Companies Foundation for providing partial funding for this research. Earlier versions of this paper were presented at the *Fifth Ethical Dimensions in Business Conference* at the University of Notre Dame (November 29, 2007) and the *Pre-ICIS Workshop on Information Security and Privacy* (Milwaukee, WI, December 10, 2006). The paper also benefited from discussions with participants of the University of Notre Dame Management Department Seminar Series.

Appendix – IS misuse scenarios

Unauthorized access scenario

By chance, Alex found the password that allowed him to access the restricted computer system that contained the salary information of 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.

Unauthorized modification scenario

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 (for example, Chris would change 39.5 h worked to 40 h worked).

References

Anderson, J. C. and D. W. Gerbing: 1988, 'Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach', *Psychological Bulletin* **103**(3), 411–423.

Azjen, I.: 1988, *Attitudes, Personality, and Behavior* (Dorsey Press, Chicago, IL).

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

Banerjee, D., T. P. Cronan and T. W. Jones: 1998, 'Modeling IT Ethics: A Study in Situational Ethics', *MIS Quarterly* **22**(1), 31–60.

Chau, P. Y. K.: 2001, 'Influence of Computer Attitude and Self-Efficacy on IT Usage Behavior', *Journal of End User Computing* **13**(1), 26–33.

Chin, W.: 1998, 'The Partial Least Squares Approach to Structural Equation Modeling', in G. A. Marcoulides (ed.), *Modern Methods for Business Research* (Lawrence Erlbaum Associates, Mahwah, NJ), pp. 295–336.

Chin, W., B. L. Marcolin and 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', *Information Systems Research* **14**(2), 189–217.

Compeau, D. R. and C. A. Higgins: 1995, 'Computer Self-Efficacy: Development of a Measure and Initial Test', *MIS Quarterly* **19**(2), 189–211.

D'Arcy, J. and A. Hovav: 2007, 'Towards a Best Fit Between Organizational Security Countermeasures and Information Systems Misuse Behaviors', *Journal of Information System Security* **3**(2), 3–30.

Dhillon, G.: 1999, 'Managing and Controlling Computer Misuse', *Information Management & Computer Security* **7**(4), 171–175.

Ernst and Young: 2003, *Global Information Security Survey 2003* (New York, NY).

Finch, J. H., S. M. Furnell and P. S. Dowland: 2003, 'Assessing IT Security Culture: System Administrator and End-User', Proceedings of the ISOneWorld Conference, Las Vegas, NV.

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, AK.

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

Gattiker, U. E. and H. Kelley: 1999, 'Morality and Computers: Attitudes and Differences in Moral Judgments', *Information Systems Research* **10**(3), 233–254.

Gefen, D. and D. Straub: 2005, 'A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example', *Communications of the AIS* **16**(5), 91–109.

Gopal, R. D. and G. L. Sanders: 1997, 'Preventative and Deterrent Controls for Software Piracy', *Journal of Management Information Systems* **13**(4), 29–47.

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.

Heath, C. and A. Tversky: 1991, 'Preference and Belief: Ambiguity and Competence in Choice Under Uncertainty', *Journal of Risk and Uncertainty* **4**, 5–28.

Hoffer, J. A. and D. Straub: 1989, 'The 9 to 5 Underground: Are You Policing Computer Crimes?', *Sloan Management Review* **30**(4), 35–43.

Hollinger, R. C. and T. P. Clark: 1983, 'Deterrence in the Workplace: Perceived Certainty, Perceived Severity, and Employee Theft', *Social Forces* **62**(2), 398–418.

IDC Research: 2007, 'Worldwide Mobile Worker: 2007–2011 Forecast and Analysis', http://www.idc.com/getdoc.jsp?containerId=prUS21037208.

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

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

Kreie, J. and T. P. Cronan: 1998, 'How Men and Women View Ethics', *Communications of the ACM* **41**(9), 70–76.

Kruegar, N. J. and P. R. Dickson: 1994, 'How Believing in Ourselves Increases Risk Taking: Perceived Self-Efficacy and Opportunity Recognition', *Decision Sciences* **25**(3), 385–400.

Lee, S. M., S. G. Lee and S. Yoo: 2004, 'An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories', *Information and Management* **41**(6), 707–718.

Leonard, L. N. K. and T. P. Cronan: 2001, 'Illegal, Inappropriate, and Unethical Behavior in an Information Technology Context: A Study to Explain Influences', *Journal of the Association for Information Systems* **1**(12), 1–30.

Lin, T.-C., M. H. Hsu, F. Y. Kuo and P. C. Sun: 1999, 'An Intention Model-Based Study of Software Piracy', Proceedings of the 32nd Hawaii International Conference on System Sciences, Maui, Hawaii.

Loch, K. D. and S. Conger: 1996, 'Evaluating Ethical Decision Making and Computer Use', *Communications of the ACM* **39**(7), 74–83.

Magklaras, G. B., S. M. Furnell and P. J. Brooke: 2006, 'Towards an Insider Threat Prediction Specification Language', *Information Management & Computer Security* **14**(4), 361–381.

Mann, R. E., G. Smart, E. M. Stoduto, E. Adlaf, D. Vingilis, R. Beirness, R. Lamble and M. Ashbridge: 2003, 'The Effects of Drinking-Driving Laws: A Test of the Differential Deterrence Hypothesis', *Addiction* **98**(11), 1531–1536.

Mann, S., R. Varey and W. Button: 2000, 'An Exploration of the Emotional Impact of Teleworking via Computer-Mediated Communication', *Journal of Managerial Psychology* **15**(7), 668–690.

Pearlson, K. E. and C. S. Saunders: 2001, 'There's No Place Like Home: Managing Telecommuting Paradoxes', *Academy of Management Executive* **15**(2), 117–128.

Ping, R. A.: 2004, '*Testing Latent Variable Models with Survey Data*', 2nd Edition. www.wright.edu/~robert.ping/lv1/toc1.htm).

Potter, E. E.: 2003, 'Telecommuting: The Future of Work, Corporate Culture, and American Society', *Journal of Labor Research* **24**(1), 73–84.

Richardson, R.: 2007, *CSI Computer Crime and Security Survey* (Computer Security Institute, San Francisco, CA).

Sacco, V. F. and E. Zureik: 1990, 'Correlates of Computer Misuse: Data from a Self-Reporting Sample', *Behaviour & Information Technology* **9**(5), 353–369.

Sheppard, B., H. J. Hartwick and P. R. Warshaw: 1988, 'The Theory of Reasoned Action: A Meta-Analysis of Past Research with Recommendations for Modifications and Future Research', *Journal of Consumer Research* **15**, 325–343.

Silberman, M.: 1976, 'Towards a Theory of Criminal Deterrence', *American Sociological Review* **41**(3), 442–461.

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

Tenbrunsel, A. E. and D. M. Messick: 1999, 'Sanctioning Systems, Decision Frames, and Cooperation', *Administrative Science Quarterly* **44**(4), 684–707.

Tittle, C. R.: 1980, *Sanctions and Social Deviance: The Question of Deterrence* (Praeger, NY).

Watad, M. M. and F. J. DiSanzo: 2000, 'Case Study: The Synergism of Telecommuting and Office Automation', *Sloan Management Review* **41**(2), 85–97.

Weaver, F. M. and J. S. Carroll: 1985, 'Crime Perceptions in a Natural Setting by Expert and Novice Shoplifters', *Social Psychology Quarterly* **48**(4), 349–359.

Whitman, M. E.: 2003, 'Enemy at the Gate: Threats to Information Security', *Communications of the ACM* **46**(8), 91–95.

Wiant, T. L.: 2003, 'Policy and Its Impact on Medical Record Security', Unpublished Doctoral Dissertation, University of Kentucky, Lexington, KY.

Wiesenfeld, B. M., S. Raghuram and R. Garud: 1999, 'Communication Patterns as Determinants of Organizational Identification in a Virtual Organization', *Organization Science* **10**(6), 777–790.

Williams, K.: 1992, 'Social Sources of Marital Violence and Deterrence: Testing an Integrated Theory of Assaults Between Partners', *Journal of Marriage and Family* **54**(3), 620–629.

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.

Zimbardo, P. G.: 1969, 'The Human Choice: Individuation, Reason, and Order Versus Deindividuation, Impulse, and Chaos', in W. J. Arnold and D. Levine (eds.), *Nebraska Symposium on Motivation* (University of Nebraska Press, Lincoln, NE).

John D'Arcy
Department of Management,
University of Notre Dame,
Notre Dame, IN 46556, U.S.A.
E-mail: jdarcy1@nd.edu

Anat Hovav
Korea University Business School,
Anam-Dong, Seongbuk-Gu, Seoul 136-701, Korea
E-mail: anatzh@korea.ac.kr